AEROSPACE RECOMMENDED PRACTICE

ARP4761™	REV. A
Issued 1996-12 Revised 2023-12 Superseding ARP4761	

(R) Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment

RATIONALE

This SAE Aerospace Recommended Practice (ARP) provides updated and expanded guidelines for accomplishing the safety assessment process on civil aircraft, systems, and equipment.

PREFACE

Since the original publication of ARP4761, the civil aviation industry safety assessment process has evolved. Many practices that were in their infancy when the original document was published are now well established and have more defined processes. For example, the Aircraft Functional Hazard Assessment (AFHA) which was at that time starting to become common practice is now a standard element of the safety assessment process. The AFHA process and legacy methods have been updated, and the Preliminary Aircraft Safety Assessment (PASA), Aircraft Safety Assessment (ASA), and new safety analysis methods have been added in Revision A. In addition to the breakout of the aircraft-level processes, the Definitions section has undergone significant updates and Section 3 has been restructured, including major updates to the figures. This update represents the current industry best practices and is intended to help those developing new or modifying existing civil aircraft, systems, or equipment to have success in developing safe aircraft for the future. Terms no longer used in this document or cases where their dictionary definition applies have been deleted from the definitions.

TABLE OF CONTENTS

1. SCOPE 4
1.1 Purpose 4
1.2 Intended Users 4
1.3 How to Use This Document 4

2. REFERENCES 5
2.1 Applicable Documents 5
2.1.1 SAE Publications 5
2.1.2 U.S. Government Publications 6
2.1.3 FAA Publications 6
2.1.4 EASA Publications 6
2.1.5 RTCA Publications 7
2.1.6 EUROCAE Publications 7
2.1.7 Other References 7
2.2 Definitions 8
2.3 Acronyms 12

SAENORM.COM : Click to view the full PDF of arp4761a

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2023 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: **http://www.sae.org**

For more information on this standard, visit
https://www.sae.org/standards/content/ARP4761A/

3. SAFETY ASSESSMENT PROCESS 14
3.1 Safety Assessment Process Overview 14
3.1.1 Safety Assessment Process Activities and Interactions 16
3.1.2 Safety Analysis Methods 17
3.2 Aircraft Functional Hazard Assessment (AFHA) 20
3.3 Preliminary Aircraft Safety Assessment (PASA) 20
3.4 System Functional Hazard Assessment (SFHA) 20
3.5 Preliminary System Safety Assessment (PSSA) 21
3.6 System Safety Assessment (SSA) 21
3.7 Aircraft Safety Assessment (ASA) 22
3.8 Determining Depth of Analysis for Failure Conditions 22
3.9 Function Development Assurance Level (FDAL) and Item Development Assurance Level (IDAL) Assignment 22
3.10 Considerations of Human Error in the Safety Assessment Process 22

4. SAFETY ANALYSIS METHODS 23
4.1 Fault Tree Analysis/Dependence Diagram/Markov Analysis/Model-Based Safety Analysis 23
4.1.1 Applications of the FTA, DD, MA, and MBSA 23
4.2 Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects Summary (FMES) 25
4.3 Cascading Effects Analysis (CEA) 25
4.4 Zonal Safety Analysis (ZSA) 25
4.5 Particular Risk Analysis (PRA) 26
4.6 Common Mode Analysis (CMA) 26

5. SAFETY-RELATED MAINTENANCE TASKS AND INTERVALS 26
5.1 Certification Maintenance Requirements 26
5.2 Maintenance Steering Group 27

6. MASTER MINIMUM EQUIPMENT LIST (MMEL) 27

7. TIME-LIMITED DISPATCH (TLD) 27

8. IN-SERVICE SAFETY ASSESSMENT 28

9. NOTES 28
9.1 Contribution Acknowledgement 28
9.2 Contribution Acknowledgement 29
9.3 Revision Indicator 29

APPENDIX A AIRCRAFT FUNCTIONAL HAZARD ASSESSMENT (AFHA) 30

APPENDIX B PRELIMINARY AIRCRAFT SAFETY ASSESSMENT (PASA) 49

APPENDIX C SYSTEM FUNCTIONAL HAZARD ASSESSMENT (SFHA) 65

APPENDIX D PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA) 84

APPENDIX E SYSTEM SAFETY ASSESSMENT (SSA) 97

APPENDIX F AIRCRAFT SAFETY ASSESSMENT (ASA) 104

APPENDIX G FAULT TREE ANALYSIS (FTA) 112

APPENDIX H DEPENDENCE DIAGRAM (DD) 167

APPENDIX I MARKOV ANALYSIS (MA) 172

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX J FAILURE MODES AND EFFECTS ANALYSIS (FMEA) 242

APPENDIX K ZONAL SAFETY ANALYSIS (ZSA) 256

APPENDIX L PARTICULAR RISK ANALYSIS (PRA) 266

APPENDIX M COMMON MODE ANALYSIS (CMA) 274

APPENDIX N MODEL-BASED SAFETY ANALYSIS (MBSA) 290

APPENDIX O CASCADING EFFECTS ANALYSIS (CEA) 321

APPENDIX P FUNCTION AND ITEM DEVELOPMENT ASSURANCE ASSIGNMENT (FDAL/IDAL) 330

APPENDIX Q CONTIGUOUS SAFETY ASSESSMENT PROCESS EXAMPLE 351

Figure 1 Overview of safety assessment process 16
Figure 2 Safety assessment process interaction with a typical development process 18
Figure 3 General safety assessment process 19

SAENORM.COM : Click to view the full PDF of arp4761a

1. SCOPE

ARP4761A and its EUROCAE counterpart, ED-135, present guidelines for performing safety assessments of civil aircraft, systems, and equipment. They may be used when addressing compliance with certification requirements (e.g., 14 CFR/CS Parts 23, 25, 27, and 29 and 14 CFR Parts 33, 35, CS-E, and CS-P). ARP4761A/ED-135 may also be used to assist a company in meeting its own internal safety assessment standards. While the safety assessment processes described are primarily associated with civil aircraft, systems, and equipment, these processes may be used in many other applications. The guidelines herein identify a systematic safety assessment process, but other processes may be equally effective.

The processes described herein are usually applicable to the new designs or to existing designs that are affected by changes to design or functions. In the case of the implementation of existing design(s) in a derivative application, complementary means such as service experience in a similar application may be used in the safety assessment.

ARP4761A/ED-135 does not address safety assessment of in-service products but does include references to those processes. ARP5150A and ARP5151A contain processes for conducting in-service safety assessments.

This document does not include information on security threat considerations.

1.1 Purpose

This document presents guidelines for conducting an industry accepted safety assessment process consisting of the Aircraft Functional Hazard Assessment (AFHA), Preliminary Aircraft Safety Assessment (PASA), System Functional Hazard Assessment (SFHA), Preliminary System Safety Assessment (PSSA), System Safety Assessment (SSA), and Aircraft Safety Assessment (ASA) processes.

This document also presents information on the safety analysis methods that may be used to conduct the safety assessment process. These methods include Fault Tree Analysis (FTA), Dependence Diagram (DD), Markov Analysis (MA), Model-Based Safety Analysis (MBSA), Failure Modes and Effects Analysis/Summary (FMEA/FMES), Cascading Effects Analysis (CEA), Zonal Safety Analysis (ZSA), Particular Risk Analysis (PRA), and Common Mode Analysis (CMA).

1.2 Intended Users

The intended users of this document include, but are not limited to, aircraft, engine, and propeller manufacturers, system integrators, equipment suppliers, and certification authorities who are involved with the safety assessment of civil aircraft and associated systems and equipment.

1.3 How to Use This Document

The guidelines provided in this document are intended to be used in conjunction with other applicable documents (e.g., ARP4754B/ED-79B, RTCA DO-178C/ED-12C, RTCA DO-254/ED-80, and RTCA DO-297/ED-124), and also with the associated certification regulations and advisory material. These regulations/advisory materials include 14 CFR/CS Parts 23, 25, 27, and 29 (sections 1309, 1709, 2510, and other system safety requirements such as sections 671, 783, 901, 903, and 933, as applicable) and 14 CFR Parts 33 and 35, CS-E, and CS-P. Since the terminology used herein is directly aligned with ARP4754B/ED-79B, the application of ARP4761A/ED-135 in support of other development processes may require an understanding of the concepts in ARP4754B/ED-79B.

All the processes described in this document may not be applicable to all projects. The depth each process goes to in this document is an example and the level presented here may not be applicable to all projects. The safety program plan (or similar planning document) should draw from the list of processes depicted in this document, and describe how, and to what depth they will be used. The size and scope of the final process presented in this document may not be appropriate for the type and complexity of the product or STC activity. At a high level, the applicant is strongly encouraged to have the safety program plan (or similar planning document) include the depth to which each process will be applied, and where the results will show that the safety requirements are met. For information on planning documents, refer to ARP4754B/ED-79B. This document defines an overall safety assessment process and provides recommendations of process outputs. It identifies activities, methods, and inputs that may be used in the performance of safety assessments for civil aircraft and their associated systems and equipment. It is recognized that the safety process for a given program will be accomplished at multiple levels by multiple stakeholders.

SAENORM.COM : Click to view the full PDF of arp4761a

General guidelines in evaluating the safety aspects of an aircraft, system, or equipment are provided in Section 3; the recommended processes and analytical methods, and the relationship between these, are introduced therein. Section 4 expands on some of these analytical methods. Section 5 provides information on the use of the analytical methods in this document by the manufacturer in determining maintenance tasks and intervals that provide for safe operation of the aircraft. Section 6 describes the relationship between the safety assessment process and the Master Minimum Equipment List (MMEL). Section 7 provides information on the Time Limited Dispatch (TLD) concept for Full-Authority Digital Engine Control (FADEC) systems which may be helpful in developing similar aircraft design solutions. Section 8 provides information on associated in-service safety assessment.

Users who need further information on a specific process or method may obtain detailed information from Appendices A through P. Appendix Q provides a contiguous example of the safety assessment process for a hypothetical system. This example illustrates the relationships between the processes and methods in creating the overall safety evaluation of an aircraft or system as it develops through the design cycle.

NOTE: The appendices are not standalone documents, but are intended to be used in conjunction with the information contained in this document's main body. The user is cautioned not to use the appendices independent of the document main body. Further, the contiguous example contained in Appendix Q should not be used without making reference to the document main body and corresponding appendices.

Examples presented in this document, including documentation examples, are intended only as illustrations. The examples should not be interpreted as an addition to or an amplification of any recommendation.

Throughout this document and appendices, reference is made to using FTA. It should be understood by the reader that other quantitative analysis methods—such as DD, MA, or MBSA—may be selected to accomplish the same purpose, depending on the circumstances and the types of data desired.

ARP5580 contains information about FMEA, but ARP4761A/ED-135 takes precedence for purposes of civil aircraft safety assessment.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

AIR6219	Development of Atmospheric Neutron Single Event Effects Analysis for Use in Safety Assessments
ARP4754B	Guidelines for Development of Civil Aircraft and Systems
ARP5107C	Guidelines for Time-Limited Dispatch (TLD) Analysis for Electronic Engine Control Systems
ARP5150A	Safety Assessment of Transport Airplanes in Commercial Service
ARP5151A	Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service

SAENORM.COM : Click to view the full PDF of arp4761a

2.1.2 U.S. Government Publications

Copies of these documents are available online at https://quicksearch.dla.mil.

MIL-HDBK-217F Reliability Prediction of Electronic Equipment

MIL-HDBK-338B Electronic Reliability Design Handbook

2.1.3 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

14 CFR 23.2510 Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes, Subpart F - Equipment; Equipment, Systems, and Installations

14 CFR 25.1309 Airworthiness Standards: Transport Category Airplanes, Subpart F - Equipment; Equipment, Systems, and Installations (refer to AC 25.1309-1A)

14 CFR 27.1309 Airworthiness Standards: Normal Category Rotorcraft, Subpart F - Equipment; Equipment, Systems, and Installations

14 CFR 29.1309 Airworthiness Standards: Transport Category Rotorcraft, Subpart F - Equipment; Equipment, Systems, and Installations

14 CFR 25.1709 Airworthiness Standards: Transport Category Airplanes, Subpart H - Electrical Wiring Interconnection Systems (EWIS) - System Safety, EWIS

14 CFR 33 Airworthiness Standards: Aircraft Engines

14 CFR 35 Airworthiness Standards: Propellers

AC 20-155A Industry Documents to Support Aircraft Lightning Protection Certification

AC 20-158A The Certification of Aircraft Electrical and Electronic Systems for Operation in the High-Intensity Radiated Fields (HIRF) Environment

AC 25-19A Certification Maintenance Requirements

AC 25.1309-1A System Design and Analysis*

*Note that, through the Equivalent Level of Safety (ELOS) process, the FAA may grant an applicant the use of the AC 25.1309 Draft ARSENAL which accompanies an ELOS finding on 14 CFR 25.1301 and 25.1309 that the Aviation Rulemaking Advisory Committee (ARAC) recommended in June 2002 ARAC report TAEsdaT2-5241996 (includes AC/AMJ 25.1309 Draft ARSENAL revised System Design and Analysis).

2.1.4 EASA Publications

Available from European Union Aviation Safety Agency, Konrad-Adenauer-Ufer 3, D-50668 Cologne, Germany, Tel: +49 221 8999 000, www.easa.europa.eu.

CS 23.2510 Certification Specifications for Normal-Category Aeroplanes, Subpart F - Equipment; Equipment, systems and installations

CS 25.1309 Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, Subpart F - Equipment; Equipment, systems and installations

CS 27.1309 Certification Specifications and Acceptable Means of Compliance for Small Rotorcraft, Subpart F - Equipment; Equipment, systems and installations

SAENORM.COM : Click to view the full PDF of arp4761a

CS 29.1309 Certification Specifications and Acceptable Means of Compliance for Large Rotorcraft, Subpart F - Equipment; Equipment, systems and installations

CS 25.1709 Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, Subpart H, System Safety, EWIS

CS-E Certification Specifications and Acceptable Means of Compliance for Engines

CS-MMEL Master Minimum Equipment List

CS-P Certification Specification for Propellers

AMC 25.1309 Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, Subpart F - System Design and Analysis (contained within CS 25)

AMC 25-19 Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, Certification Maintenance Requirements (contained within CS 25)

2.1.5 RTCA Publications

Available from RTCA, Inc., 1150 18th Street, NW, Suite 910, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

DO-178B Software Considerations in Airborne Systems and Equipment Certification

DO-178C Software Considerations in Airborne Systems and Equipment Certification

DO-254 Design Assurance Guidance for Airborne Electronic Hardware

DO-297 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

2.1.6 EUROCAE Publications

Available from EUROCAE Secretariat, 9-23 Rue Paul Lafargue, 93200 Saint-Denis, France, Tel: +33 1 40 92 79 30, https://www.eurocae.net/.

ED-12B Software Considerations in Airborne Systems and Equipment Certification

ED-12C Software Considerations in Airborne Systems and Equipment Certification

ED-79B Guidelines for Development of Civil Aircraft and Systems

ED-80 Design Assurance Guidance for Airborne Electronic Hardware

ED-124 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

ER-008 Development of Atmospheric Neutron Single Event Effects Analysis for use in Safety Assessments

2.1.7 Other References

MSG-3 Operator/Manufacturer Scheduled Maintenance Development

NUREG-0492 Fault Tree Handbook, U.S. Nuclear Regulatory Commission

SAENORM.COM : Click to view the full PDF of arp4761a

2.2 Definitions

NOTE: The shared definitions in ARP4754B/ED-79B, ARP5150A, ARP5151A, and those in this document and ED-135 have been coordinated for consistency.

ANALYSIS: A detailed examination based on decomposition into simple elements.

ASSESSMENT: An evaluation process which may include one or more types of analysis and experience.

ASSUMPTION: Statements, principles and/or premises offered without proof.

ASSURANCE: The planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements (DO-178C/ED-12C, ARP4754B/ED-79B).

“AT RISK” TIME: The period of time during which the aircraft may be subject to the failure effect under analysis.

AVAILABILITY: Qualitative or quantitative attribute that a system or equipment is in a functioning state at a given point in time. It is sometimes expressed in terms of the probability of the system (equipment) not providing its output(s), i.e., unavailability.

CERTIFICATION: The legal recognition that a product complies with the applicable regulations.

CERTIFICATION AUTHORITY: Organization or person responsible for granting approval in accordance with applicable regulations.

COMMON CAUSE: A single failure, error, or event that can produce undesirable effects on two or more systems, equipment, items, or functions.

DERIVED REQUIREMENTS: Requirements that introduce behaviors or characteristics beyond those specified in higher-level requirements.

DEVELOPMENT ASSURANCE: All those planned and systematic actions used to substantiate, at an adequate level of confidence, that development errors have been identified and corrected such that the system satisfies the applicable certification basis (derived from AC 25.1309 Draft ARSENAL revised and AMC 25.1309).

DEVELOPMENT ERROR: A mistake in requirements, design, or implementation.

EQUIPMENT: A physical object that can be installed and removed from the aircraft and performs one or more specific functions. Equipment contains one or more items.

ERROR: An omitted or incorrect action by a manufacturer, crew member, or maintenance person, or a mistake in requirements, design, or implementation (derived from AMC 25.1309).

EXPOSURE TIME: The period of time between when a specific system, equipment, or item, that can cause or contribute to the failure condition under analysis, was last known to be operating properly and when it will be known to be operating properly again.

EXTERNAL EVENT: An occurrence which has its origin distinct from the aircraft or the system being examined, such as atmospheric conditions (e.g., wind gusts/shear, temperature variations, icing, lightning strikes), operating environment (e.g., runway conditions, conditions of communication, navigation, and surveillance services), cabin and baggage fires, and bird-strike. The term is not intended to cover sabotage.

FAILURE: An occurrence which affects the operation of an aircraft, system, equipment, item, or piece-part such that it can no longer function as intended (this includes both loss of function and malfunction). Note: Errors may cause Failures but are not considered to be Failures.

SAENORM.COM : Click to view the full PDF of arp4761a

FAILURE CONDITION (FC): A condition having an effect on the aircraft and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events (AMC 25.1309).

FAILURE CONDITION CLASSIFICATION: A discrete scale allowing categorization of the severity of the effects of a failure condition. Classification levels are defined in the applicable regulation and advisory material. For example, AC 25.1309 Draft ARSENAL revised and AMC 25.1309 define the following classifications; Catastrophic, Hazardous, Major, Minor, and No Safety Effect.

FAILURE EFFECT: A description of the operation of an aircraft, system, equipment, or item as the result of a failure, i.e., the consequence(s) a failure mode has on the operation, function, or status of an aircraft, system, equipment, item, or aircraft occupants.

FAILURE MODE: A specific way in which a system, equipment, hardware item, or piece-part may fail.

FAILURE RATE: The expected frequency of occurrence of a specific failure mode over a period of time. The failure rate at time t may be calculated by dividing the failure density function f(t) by the reliability distribution function R(t) where:

$$R(t) = (1\text{-failure distribution function } F(t))$$

$$\lambda(t) = f(t)/(1-F(t))$$

Note that if the failure distribution function is exponential, the failure rate is constant and the failure rate can be approximately calculated by dividing the number of failures within a hardware item population, by the total unit operating hours.

FAULT: A manifestation of an error in an item or system that may lead to a failure.

FUNCTION: Intended behavior of an aircraft, system, equipment, or item regardless of implementation.

FUNCTION DEVELOPMENT ASSURANCE LEVEL (FDAL): The level of rigor of development assurance tasks performed to Functions. Note: The FDAL is used to identify the ARP4754B/ED-79B objectives that need to be satisfied for the aircraft/system functions.

FUNCTIONAL FAILURE SET (FFS): A set of one, or more members that are considered to be independent from one another (not necessarily limited to one system), whose development error(s) leads to a top-level failure condition.

FUNCTIONAL INDEPENDENCE: See INDEPENDENCE.

GUIDANCE: Recommended procedures for showing compliance with regulations.

GUIDELINE: Supporting information that can be helpful but is not considered to be guidance.

HARDWARE: The physical realization of systems, equipment, or items. May refer to these objects individually or collectively.

HAZARD: A condition resulting from failures, external events, errors, or a combination thereof where safety is potentially affected.

IMPLEMENTATION: The act of creating a reality from a specification.

SAENORM.COM : Click to view the full PDF of arp4761a

INDEPENDENCE: Specific types of independence include:

- FUNCTIONAL INDEPENDENCE: A characteristic that minimizes the likelihood of common development errors by using different functions.
- ITEM DEVELOPMENT INDEPENDENCE: A characteristic that minimizes the likelihood of common development errors by using different item designs.
- PHYSICAL INDEPENDENCE: A characteristic that minimizes the likelihood of common failures caused by physical failure, damage, or environmental effects by using physical separation or segregation between two or more things, e.g., hardware items, equipment, wiring, tubing.
- PROCESS INDEPENDENCE: A practice that minimizes the likelihood of development errors by using separation of responsibilities that assures the accomplishment of objective evaluation by someone other than the performer of the activity, e.g., validation activities are not performed solely by the developer of the requirement(s) of a system or item.

INDEPENDENCE PRINCIPLE: Features of an intended implementation where independence has been determined to be necessary.

INSPECTION: An examination of a system or item against a specific standard.

INTEGRATION: (1) The act of causing elements of a system/item to function together. (2) The act of gathering a number of separate functions within a single implementation.

INTEGRITY: Qualitative or quantitative attribute of a system, equipment, or an item indicating that it can be relied upon to work as intended.

ITEM: A defined and bounded set of either (one or more) hardware elements or (one or more) software elements which are treated as a single entity for analytical purposes.

ITEM DEVELOPMENT ASSURANCE LEVEL (IDAL): The level of rigor of development assurance tasks performed on Item(s); e.g., IDAL is the appropriate software level in DO-178C/ED-12C, and design assurance level in DO-254/ED-80 objectives that need to be satisfied for an item.

ITEM DEVELOPMENT INDEPENDENCE: See INDEPENDENCE.

LATENT FAILURE: A failure which is not detected and/or annunciated when it occurs.

MALFUNCTION: A condition where the operation of a function is different than intended, excluding the loss of function.

MEAN TIME BETWEEN FAILURES (MTBF): The average elapsed time between consecutive failures of a repairable system, equipment, or hardware item during operation under stated conditions.

MEAN TIME TO FAILURE (MTTF): The average elapsed time to failure for a non-repairable system, equipment, or hardware item during operation.

MEMBER: An aircraft or system function or item that may contain a development error causing its loss of function or malfunction. (Used only with regard to a Functional Failure Set.)

MINIMAL CUT SET (MCS): A set of primary events where removing any single primary event no longer results in the top event.

MODEL: An abstract representation of a given set of aspects of a system/function/item that is used for its analysis, implementation, simulation, or code generation and that has unambiguous, well-defined syntax and semantics.

MONITORING: The act of detecting the effects of a failure. May or may not result in mitigation or corrective action of the adverse effects as defined by the analyzing organization.

SAENORM.COM : Click to view the full PDF of arp4761a

PARTITIONING: The use of physical or logical boundaries to separate portions of a system or an item such that the portions may be considered independent.

PROCESS: A set of interrelated activities performed to produce a prescribed output or product.

RELIABILITY: The probability that a system, equipment, or hardware item will perform a required function under specified conditions, without failure, for a specified period of time.

REQUIREMENT: An identifiable element of a function specification that can be validated and against which an implementation can be verified.

RISK: The potential of an occurrence to cause harm defined by its probability and the severity of its consequence(s).

SAFETY: The state in which risk is acceptable.

SAFETY OBJECTIVE: A qualitative and/or quantitative attribute necessary to achieve the required level of safety for the identified failure condition, depending on its classification.

SAFETY REQUIREMENT: A requirement which is necessary to achieve either a safety objective or satisfy a constraint established by the safety process.

SEGREGATION: The use of a barrier to provide physical independence between hardware elements.

SEPARATION: The use of physical distance to provide independence between hardware elements.

SIGNIFICANT LATENT FAILURE: A latent failure which, in combination with one or more specific failures or events, would result in a Hazardous or Catastrophic failure condition (AC 25.1309 draft ARSENAL revised/AMC 25.1309).

SOFTWARE: Executable algorithm that runs on a computer. May refer to such elements individually or collectively.

SPECIFICATION: A collection of requirements which, when taken together, constitute the criteria that define the functions and attributes of an aircraft, system, equipment, or item.

SUBSYSTEM: A defined portion of a system that performs one or more specific functions.

SURVIVABILITY: The ability of an aircraft, system, or equipment to continue to function in a way that achieves safe aircraft operation after being affected by an outside influence, e.g., by a failure or environmental event external to the aircraft or system affected. Note that the subset crash survivability, aka crash resistance, refers to the ability of an aircraft design to protect the occupants (crew and passengers) from injury during/after a crash.

SYSTEM: A defined combination of subsystems, equipment, or items that perform one or more specific functions.

TRACEABILITY: The recorded relationship established between two or more elements of the development process. For example, between a requirement and its source or between a verification method and its requirement.

VALIDATION: The determination that the requirements for a product are correct and complete.

VERIFICATION: The evaluation of an implementation of requirements to determine that they have been met.

SAENORM.COM : Click to view the full PDF of arp4761a

2.3 Acronyms

AC	Advisory Circular (FAA)
AFHA	Aircraft Functional Hazard Assessment
AFM	Aircraft Flight Manual
AMC	Acceptable Means of Compliance (EASA)
ARP	Aerospace Recommended Practice (SAE)
ASA	Aircraft Safety Assessment
CCMR	Candidate Certification Maintenance Requirement
CEA	Cascading Effects Analysis
CFR	Code of Federal Regulations
CMA	Common Mode Analysis
CMCC	Certification Maintenance Coordination Committee
CMR	Certification Maintenance Requirement
CoFFE	Combined Functional Failure Effects
COTS	Commercial Off-the-Shelf
CS	Certification Specification
CTMC	Continuous Time Markov Chain
DD	Dependence Diagram
EASA	European Union Aviation Safety Agency
ETOPS	Extended-Range Operations
EUROCAE	European Organisation for Civil Aviation Equipment
EWIS	Electrical Wiring Interconnection Systems
FAA	Federal Aviation Administration
FADEC	Full-Authority Digital Engine Control
FC	Failure Condition
FC&C	Failure Conditions and Classifications
FDAL	Function Development Assurance Level
FFBD	Functional Flow Block Diagram

SAENORM.COM : Click to view the full PDF of arp4761a

FFS	Functional Failure Set
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FMES	Failure Modes and Effects Summary
FPM	Failure Propagation Model
FTA	Fault Tree Analysis
HIRF	High-Intensity Radiated Fields
HW	Hardware
IDAL	Item Development Assurance Level
IMA	Integrated Modular Avionics
I/O	Input/Output
LH	Left Hand
LOTC	Loss of Thrust Control
LRU	Line Replaceable Unit
MA	Markov Analysis
MBSA	Model-Based Safety Analysis
MBSE	Model-Based System Engineering
MC	Markov Chain
MCS	Minimal Cut Set
MF&MS	Multifunction and Multisystem
MM	Markov Model
MMEL	Master Minimum Equipment List
MRB	Maintenance Review Board
MSG-3	Maintenance Steering Group 3
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
ODE	Ordinary Differential Equation
PASA	Preliminary Aircraft Safety Assessment

SAENORM.COM : Click to view the full PDF of arp4761a

PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
RH	Right Hand
ROF	Required Order Factor
RTO	Rejected Takeoff
SEE	Single Event Effects
SEU	Single Event Upset
SFHA	System Functional Hazard Assessment
SSA	System Safety Assessment
SW	Software
TC	Type Certificate (or Certification)
TLD	Time-Limited Dispatch
TSF	Time Since Fault
ZSA	Zonal Safety Analysis

3. SAFETY ASSESSMENT PROCESS

3.1 Safety Assessment Process Overview

The safety assessment process is one of multiple processes integral to aircraft and system development. Other integral processes such as requirements management, configuration management, and process assurance are described in ARP4754B/ED-79B. The safety assessment process:

- Evaluates aircraft functions and the design of systems performing these functions.
- Identifies and classifies failure conditions associated with those functions and systems.
- Determines the minimum level of rigor to be applied to the associated development assurance activities according to the classification of those failure conditions.
- Identifies safety objectives and requirements.
- Hierarchically validates these safety requirements for completeness and correctness at each tier (e.g., aircraft, systems, and items).
- Confirms that the implementation satisfies its safety requirements and objectives.

The safety assessment process is iterative and both qualitative and quantitative in nature with its activities supporting the aircraft development process. Through these activities, the safety assessment process provides confidence that the likelihood of failures and errors that may lead to failure conditions has been minimized to a level commensurate with the severity of these failure conditions.

SAENORM.COM : Click to view the full PDF of arp4761a

Figure 1 depicts a top-level view of a typical development cycle timeline and the relationship of the safety assessment process to a development process. The development process and safety assessment process are iterative in nature. The safety assessment process includes the following principal processes generally initiated in sequence, but not necessarily completed in sequence. These processes may include the production of reports documenting the results of these processes.

- Aircraft Functional Hazard Assessment (AFHA)

  A systematic, comprehensive evaluation of aircraft functions to identify and classify failure conditions (FCs) of those functions according to their severity, and provide a basis for aircraft-level safety objectives.

- Preliminary Aircraft Safety Assessment (PASA)

  A systematic, comprehensive evaluation of a proposed aircraft architecture to provide confidence that the safety objectives resulting from the failure condition classifications can be met by developing safety requirements pertaining to those failure conditions.

- System Functional Hazard Assessment (SFHA)

  A systematic, comprehensive evaluation of system functions to identify and classify failure conditions of those functions according to their severity and provide a basis for system-level safety objectives.

- Preliminary System Safety Assessment (PSSA)

  A systematic, comprehensive evaluation of a proposed system architecture and equipment/item designs to provide confidence that the safety objectives resulting from the failure condition classifications and system-level safety requirements from the PASA can be met by developing associated system-level, equipment-level, and item-level safety requirements pertaining to those failure conditions.

- System Safety Assessment (SSA)

  A systematic, comprehensive evaluation of the implemented system to verify that applicable safety objectives and requirements are met.

- Aircraft Safety Assessment (ASA)

  A systematic, comprehensive evaluation of the aircraft to verify that applicable safety objectives and requirements are met.

The safety assessment process reflects multiple system-level processes (SFHAs, PSSAs, and SSAs) for an aircraft's multiple systems. Note that a system could consist of one or more systems (sometimes called "subsystems"), thereby entailing the system-level processes for each of those systems and hierarchal interfaces with other safety assessment processes.

SAENORM.COM : Click to view the full PDF of arp4761a

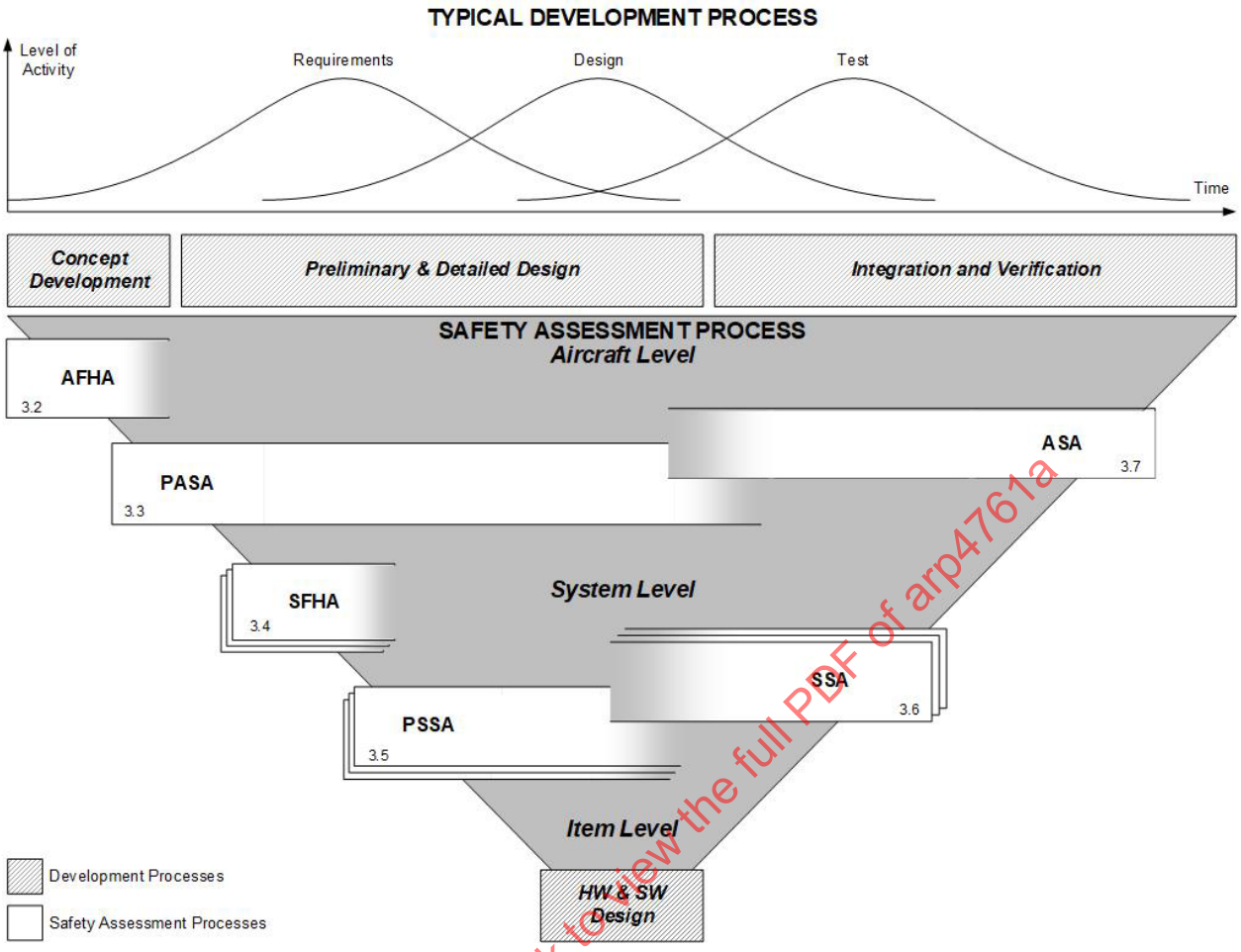


Figure 1 - Overview of safety assessment process

SAENORM.COM : Click to view the full PDF of arp4761a

3.1.1 Safety Assessment Process Activities and Interactions

Safety assessment process activities are conducted in conjunction with the associated development process activities and should be described in a plan such as the safety program plan in ARP4754B/ED-79B. Figure 2 highlights the safety assessment principal processes' interactions with key development process activities, such as those in ARP4754B/ED-79B. Figure 3 summarizes the safety assessment process and highlights its safety activities and interactions. The activities shown in these two figures are conducted in parallel with multiple interactions between the processes, but are presented separately to provide graphical clarity.

The safety assessment process begins in the AFHA process with the review of aircraft-level functions from the development process and the determination of aircraft/system-level failure conditions. Safety objectives based on the classification of those failure conditions are provided for use in the PASA process. In the PASA process, the proposed aircraft architecture is evaluated to provide confidence that the safety objectives resulting from the AFHA failure condition classifications can be met. Safety requirements pertaining to safety objectives associated with those failure conditions are established and passed on to the development process for allocation to systems, subsystems, and items. Requirements are also passed on to the PSSA processes for the systems allocated such requirements along with assigned Function Development Assurance Levels (FDALs).

Similar to and usually following the aircraft-level AFHA and PASA processes, the SFHA and PSSA processes are executed to accomplish similar activities and objectives at the system level. The development process allocates functions to systems and the SFHA process evaluates associated failure conditions and classifications for those functions. Safety objectives are established from those failure condition classifications. The PSSA process identifies safety requirements to satisfy those safety objectives. These safety requirements are then passed to other systems, subsystems, and items for implementation.

In some cases, the originator may flow safety objectives from the AFHA (SFHA) to the development process and the PASA (PSSA). In other cases, the originator may flow failure condition classifications to the development process and the PASA (PSSA) with safety objectives being established from these failure condition classifications within the PASA (PSSA) processes.

The SSA process verifies that the implemented system design meets the qualitative and quantitative safety objectives and requirements from the SFHA, PSSA, and PASA.

Similarly, the ASA process provides confirmation that aircraft-level analyses and SSAs' results verify the overall aircraft and systems design meets the qualitative and quantitative safety objectives and safety requirements from the AFHA and PASA.

Any change to the design or a principal assessment could precipitate a change to another principal assessment, e.g., a change to the PASA or SFHA could drive a change to the PSSA/SSA. As the design evolves, changes are made and the modified design is reassessed. This reassessment may modify existing safety requirements or identify new safety requirements to meet the safety objectives, which may necessitate further design changes. The safety assessment process is complete when the applicable SSA(s) and ASA results show that the applicable system-level and aircraft-level safety objectives have been satisfied and confirm applicable safety requirements have been met.

The safety assessment process for integrated systems should take into account the complexities and interdependencies which arise due to integration. In cases involving integrated systems, the safety assessment process is of fundamental importance in establishing appropriate safety objectives and safety requirements for each system and determining that the implementation satisfies these objectives and requirements.

Sections 3.2 through 3.7 provide descriptions of the six principal processes within the safety assessment process. The details of the processes in this ARP describe one means of performing those processes; other means of completing the objectives of the processes may be possible.

3.1.2 Safety Analysis Methods

The safety assessment process includes safety analysis methods which may be applied throughout the typical development cycle to provide the analyst a means of qualitatively and/or quantitatively assessing the safety of a design. These methods include Fault Tree Analysis (FTA), Dependence Diagrams (DD), Markov Analysis (MA), Model-Based Safety Analysis (MBSA), Failure Modes and Effects Analysis/Summary (FMEA/FMES), Cascading Effects Analysis (CEA), Particular Risk Analysis (PRA), Zonal Safety Analysis (ZSA), and Common Mode Analysis (CMA). The method(s) selected will vary based on system characteristics and organizational practices. The results of these methods may be incorporated into any of the higher-level assessments. Figure 3 shows where safety analysis methods can be used within the safety assessment process. The PRA/ZSA/CMA include consideration of physical and installation risks fundamental to the definition of both aircraft and system architectures. These analyses interact with the development process throughout the development lifecycle.

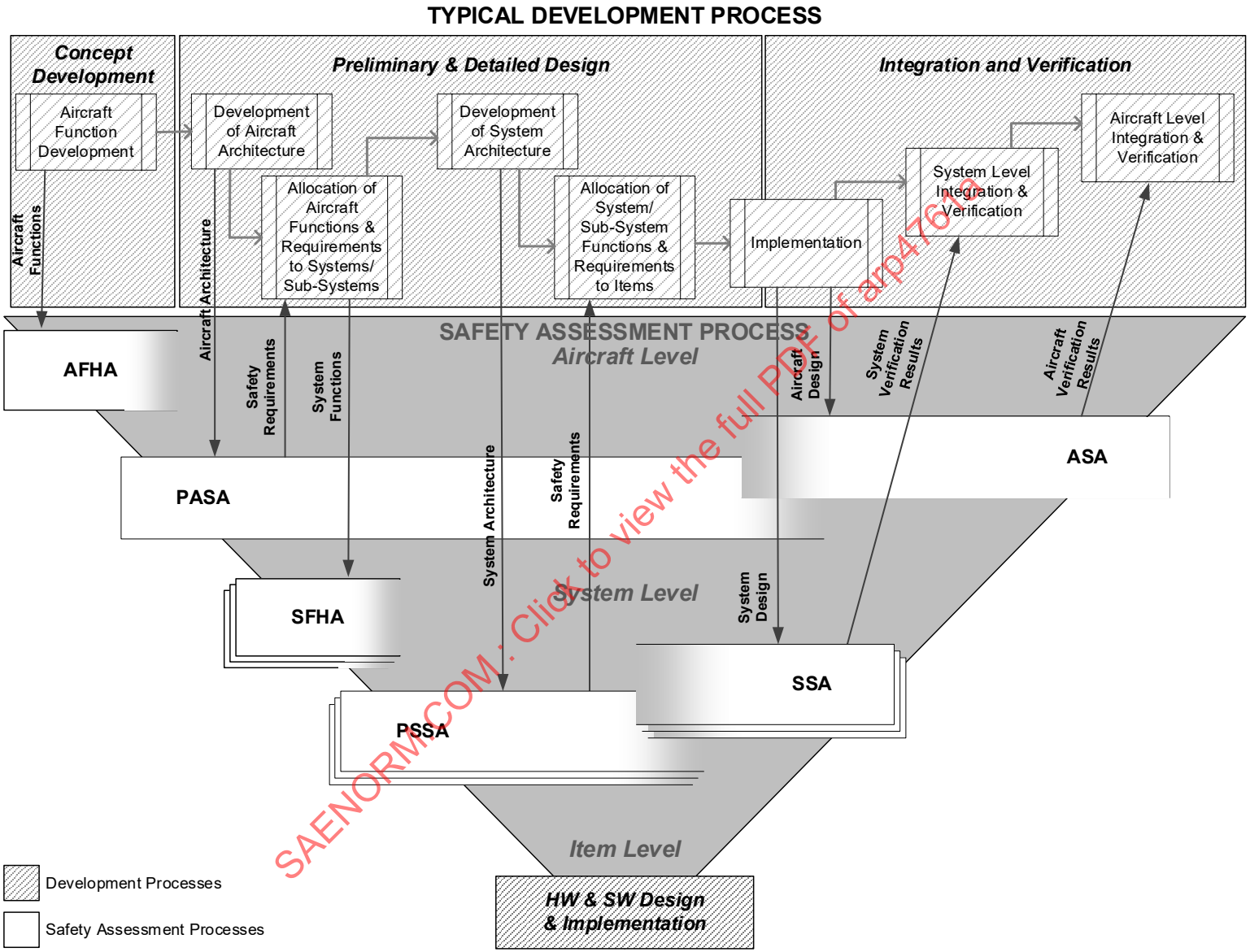
Independence between functions, systems or items may be required to satisfy the safety requirements. Therefore, it is necessary to ensure that such independence exists, or that the risk associated with dependence is deemed acceptable. The PRA, ZSA, and CMA provide methods for evaluation of independence or the identification of specific dependencies due to a common cause. These methods may also aid the PASA and PSSA in generation of independence requirements (e.g., physical, installation requirements).

The PRA and ZSA support the overall development of the specific aircraft, system, and equipment architectures by evaluating the overall architecture sensitivity to aircraft-level hazards. PRAs are managed from an overall aircraft perspective to address particular physical hazards, within or external to the aircraft, which could affect the entire airframe (or several aircraft sections) and/or impact one or more aircraft systems and their installation. ZSAs are managed from a zonal perspective to address physical hazards related to physical installation.

The PRA and ZSA are described as safety methods in this document, but depending on company organization of these aircraft-wide safety activities evaluating more than just common cause considerations, they may also be considered as processes in their own right.

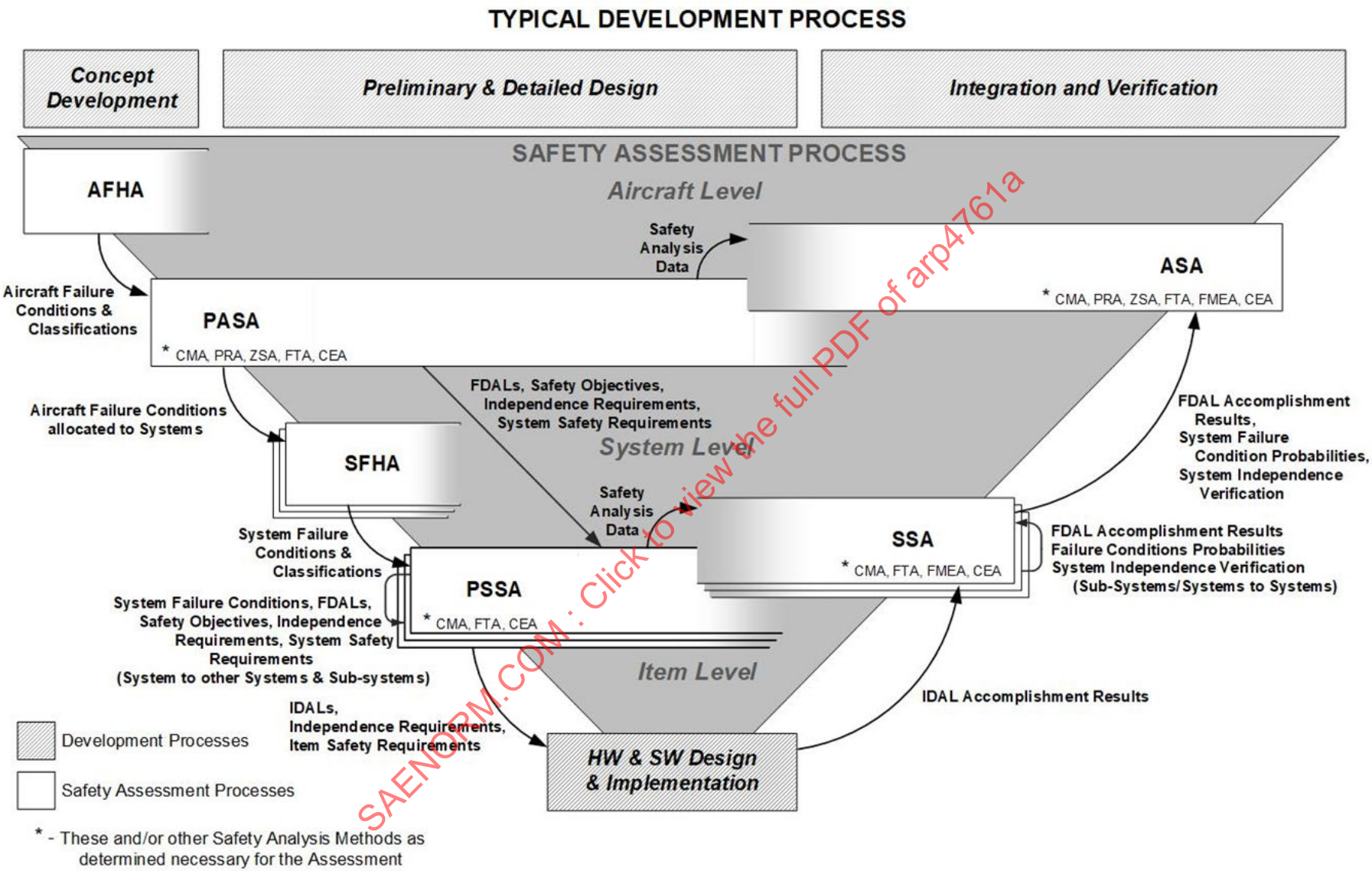
Section 4 summarizes the details of each safety analysis method addressed above.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure 2 - Safety assessment process interaction with a typical development process



SAENORM.COM : Click to view the full PDF of arp4761a

Figure 3 - General safety assessment process

3.2 Aircraft Functional Hazard Assessment (AFHA)

The AFHA is a systematic, comprehensive evaluation of the aircraft functions as defined at the beginning of aircraft development. An AFHA identifies and classifies the failure conditions associated with each aircraft-level function. The goal in conducting this AFHA is to clearly identify each failure condition along with the rationale for its severity classification. The classification of these failure conditions establishes the safety objectives that an aircraft should meet. The AFHA should also identify assumptions associated with aircraft and crew mitigations to limit the severity classification, e.g., operating limits, crew information presentation, operating procedures. The passing of failure conditions, their classifications, and associated assumptions from the AFHA to the PASA is the starting point for conducting the PASA.

For details in performing the AFHA, see Appendix A.

3.3 Preliminary Aircraft Safety Assessment (PASA)

The PASA is a systematic, comprehensive evaluation of a proposed aircraft architecture to determine how failures can lead to aircraft-level failure conditions identified by the AFHA and how the safety objectives can be met. The objective of the PASA is to use the safety objectives established from the failure conditions classifications to establish the safety requirements of the aircraft and to determine that the proposed architecture can reasonably be expected to meet the safety objectives. The PASA process is interactive and associated with design definition. Just as the design process is iterative, the PASA process is iterative.

The PASA addresses the failure conditions identified in the AFHA that may require an analysis at the aircraft level, in particular, failure conditions that cannot be allocated to a single system (i.e., AND-gates between different systems or functions). As addressed in 3.1, the PASA process may use various safety analysis methods. Common cause considerations are taken into account in the PASA process. The PASA methods of safety analysis may be qualitative and/or quantitative. See 3.8 on using depth of analysis to determine the type of analysis to apply in evaluating failure conditions. The PASA evaluates combined functional failure effects of the related systems and potential common cause failures between them, including consideration of their shared resources. The PASA also identifies safety requirements such as independence requirements and FDAL assignments for the associated aircraft functions. The development process allocates these safety requirements from the PASA to the individual PSSA processes. See 3.9 for details on development assurance level assignment. See Section 4 for descriptions of the various safety analyses that may be used in conducting the PASA. Once the aircraft-level safety requirements have been defined through PASA process and the implementing systems mature, the ASA process may be initiated as described in 3.7.

For details in performing the PASA, see Appendix B.

3.4 System Functional Hazard Assessment (SFHA)

The SFHA is a systematic, comprehensive evaluation of system functions conducted early in system development to identify and classify the failure conditions of each system-level function, including those fulfilling any aircraft-level functions allocated to the system. The goal in conducting the SFHA is to clearly identify each failure condition along with the rationale for its severity classification. The classification of these failure conditions establishes the safety objectives that the system should meet.

After aircraft functions have been allocated to systems by the design process, each system is examined using the SFHA process. If additional aircraft-level failure conditions affecting the system-level functions are identified, the SFHA is revised to identify and classify the system's failure conditions. Similarly, if system-level failure conditions affecting aircraft-level or other system-level functions are identified, these should be captured in the SFHA and passed to the AFHA. The SFHA should also identify assumptions associated with aircraft and crew mitigations to limit the severity classification, e.g., operating limits, crew information presentation, operating procedures. The passing of failure conditions, their classifications, and associated assumptions from the SFHA(s) to the PSSA(s) is used as the starting point for conducting the PSSA(s).

For details in performing the SFHA, see Appendix C.

SAENORM.COM : Click to view the full PDF of arp4761a

3.5 Preliminary System Safety Assessment (PSSA)

A PSSA process is a systematic, comprehensive evaluation of a proposed system architecture to determine how failures can lead to the system-level failure conditions identified by the SFHA. Safety objectives are established from failure conditions and classifications, and the PASA provides safety requirements based on the contribution of the system to aircraft failure conditions including allocated probability requirements and FDALs. The PSSA is used to establish the safety requirements of the system, including independence requirements, and to determine that the proposed architecture can reasonably be expected to meet the safety objectives identified by the SFHA or PSSA processes and safety requirements allocated from the PASA and/or higher-level systems. As addressed in 3.1, the PSSA process may use various safety analysis methods to determine these requirements. See 3.8 on using depth of analysis to determine the type of analysis to apply in evaluating failure conditions. The PSSA process should consider the potential impact of Single Event Effects (SEE) on electronic airborne systems. The PSSA also identifies the necessary FDAL and Item Development Assurance Level (IDAL) assignments for the system function and items. See 3.9 for details on development assurance level assignment. See Section 4 for descriptions of the various safety analyses that may be used in conducting the PSSA.

The PSSA process identifies where protective strategies may be needed to meet the safety objectives. Such protective strategies may include redundancy, monitoring, partitioning, development assurance rigor, built-in-test, and safety-related maintenance tasks and intervals.

The PSSA process is an iterative assessment conducted at multiple stages of system development. It is an on-going process, starting in the early phases of design with the evaluation of the system architecture to determine system-level safety requirements. System-level safety requirements are then allocated to subsystems and finally subsystem requirements are allocated to equipment/items. This safety requirements allocation to subsystems will determine hardware reliability requirements and development assurance requirements for both hardware and software (refer to ARP4754B/ED-79B). These requirements and development assurance levels are captured in applicable specifications. The PSSA assignment of IDALs to items determines the appropriate hardware and software development assurance rigor. The PSSA also generates item requirements including but not limited to safety, reliability, independence, and separation. Common cause considerations are taken into account in the PSSA process. Care should be taken to account for potential latent failures and significant latent failures and their associated exposure times.

Once safety requirements have been defined through the PSSA process and the implementing subsystems/items mature, the SSA process may be initiated.

For details in performing the PSSA, see Appendix D.

3.6 System Safety Assessment (SSA)

An SSA is a systematic, comprehensive evaluation of the implemented system to show that safety objectives from the SFHA and relevant safety requirements are satisfied. The difference between a PSSA and an SSA is that a PSSA is a process to evaluate proposed architectures and identify safety requirements; whereas the SSA is verification that the implemented design meets both the qualitative and quantitative safety objectives and requirements as defined in the SFHA and PSSA, and safety requirements passed from the PASA.

The SSA integrates the results of the various analyses to verify the safety of the overall system and to cover all the specific safety requirements identified in the PSSA. The SSA uses the quantitative values obtained from the reliability predictions, SEE analysis, FMEA, or FMES. The SSA ensures that all significant failure modes are considered for inclusion in the FTA. The SSA process documentation includes results of the relevant analyses and their substantiations as needed. The SSA also includes applicable common cause consideration results.

The SSA process is generally represented through succeeding levels of verification through different levels of systems, subsystems, and items. Through these upward hierarchical verification levels, the implementation is assessed against the safety requirements identified in the PSSA process.

For details in performing the SSA, see Appendix E.

SAENORM.COM : Click to view the full PDF of arp4761a

3.7 Aircraft Safety Assessment (ASA)

The ASA is a systematic, comprehensive evaluation of the complete aircraft to show that safety objectives from the AFHA/PASA and safety requirements from the PASA are satisfied. The difference between a PASA and an ASA is that a PASA is a method to evaluate proposed architectures and identify safety requirements; whereas the ASA is verification that the implemented design meets both the qualitative and quantitative safety objectives and requirements as defined in the AFHA and PASA.

The ASA integrates the results of the various analyses to verify the safety of the overall aircraft and systems. This aircraft safety assessment is refined and updated throughout the development process to reflect the updated design.

The ASA uses the results obtained from the PASA and SSAs and ensures assessment of interdependencies between the aircraft functions and systems. The ASA ensures that system failure modes are considered for inclusion. The ASA also includes applicable common cause consideration results.

For details in performing the ASA, see Appendix F.

3.8 Determining Depth of Analysis for Failure Conditions

Failure conditions for the aircraft/system function should be evaluated to determine how the aircraft/system will satisfy safety objectives. The depth of analysis that should be employed in the assessment of the failure conditions is typically based on the failure condition classification, and in some cases, other aircraft/system characteristics. This evaluation generally follows a course to determine what type(s) of analysis/assessment should be employed in analyzing the failure condition, e.g., design or installation appraisal, verification analysis, or qualitative and/or quantitative assessment. While the determination of the course of analysis is straightforward for most categories, additional criteria are usually required to determine the course of analysis for "Major" failure conditions. The safety analyst should consult Depth of Analysis Flow Charts and associated text in advisory material for the current guidance to be used in determining depth of analysis of failure conditions, e.g., AC 25.1309-1A, AMC 25.1309, and AC29.2C.

3.9 Function Development Assurance Level (FDAL) and Item Development Assurance Level (IDAL) Assignment

Safety process activities within the PASA and PSSA processes include the assignment of FDALs and IDALs which define the level of rigor of development assurance activities. These levels of rigor are used to substantiate, to an adequate level of confidence, that development errors that could contribute to failure conditions have been identified and corrected.

Appendix P provides details in performing development assurance level assignment.

3.10 Considerations of Human Error in the Safety Assessment Process

The safety assessment process described in this document assumes that flight crews, cabin crews, maintenance crews, and other individuals participating in the operation of the aircraft follow documented procedures in foreseeable operating conditions (normal, malfunction or abnormal, and emergency). Intentional or unintentional deviation from these procedures is not considered in the safety assessment process described herein.

With the exception of some aspects of the CMA and the ZSA, the safety effects of potential flight crew and maintenance errors are evaluated using different analysis techniques. Refer to the appropriate certification advisory material on human factors for accomplishing human factor safety evaluations.

SAENORM.COM : Click to view the full PDF of arp4761a

4. SAFETY ANALYSIS METHODS

The safety analysis methods addressed in this section are used to support the safety assessment processes described in Section 3.

4.1 Fault Tree Analysis/Dependence Diagram/Markov Analysis/Model-Based Safety Analysis

FTA, DD, and MA are top-down analysis techniques. These analyses proceed down through successively more detailed (i.e., lower) levels of the design. The MBSA is an analysis technique used to model the system architecture and its functional design in order to characterize system behavior when subjected to failures in order to obtain specific safety analysis results. The reader is reminded that when FTA is presented herein, the DD, MA, and/or MBSA analysis techniques may be applicable/selected depending on the circumstances and the types of data desired.

After identifying the failure conditions in the AFHA or SFHA, the FTA can be applied as part of a safety assessment to determine what single failures or combinations of failures, if any, exist at the lower levels that might cause each failure condition. The FTA basic events may get their failure rates from the FMEAs or FMESs. The FTA might also use other failure rate sources, such as a reliability prediction or SEE analysis.

For details in performing the FTA, see Appendix G. For details in performing the DD, see Appendix H. For details in performing the MA, see Appendix I. For details in performing the MBSA, see Appendix N.

4.1.1 Applications of the FTA, DD, MA, and MBSA

The completed FTA facilitates technical and management assessments and reviews because it identifies only the failure events (single failure or failure combinations) which could individually or collectively lead to the occurrence of the undesired top event. In contrast, an FMEA identifies only single failures, including some that may be of no concern.

The FTA facilitates subdivision of system-level events into lower-level events for ease of analysis.

The FTA may be used to evaluate a proposed aircraft or system architecture to identify single failures or failure combinations leading to the top event. The FTA may be used to:

a. Quantify probability of occurrence for the top event.

b. Evaluate a proposed aircraft or system architecture to establish hardware failure probability budgets or hardware failure rate budgets.

c. Evaluate a proposed aircraft or system architecture to identify Functional Failure Sets (FFS) in order to assign FDALs and IDALs during the PASA or PSSA process.

d. Assess the safety impact of an architecture or design modification in support of the PASA or PSSA.

e. Identify the need for a design modification or identify unique situations that require special attention.

f. Show compliance with qualitative or quantitative safety objectives as part of the PSSA/SSA or PASA/ASA.

g. Establish the need for maintenance tasks and intervals necessary to meet the requirements of the safety assessment. See Section 5 for discussion of maintenance tasks and intervals.

h. Establish the need for a crew procedure(s) used to mitigate failure conditions.

When conducting FTAs for the PASA/ASA or PSSA/SSA, it is beneficial to align the failure detection means allocated to the maintenance tasks and related exposure times with those used by the maintenance program for the aircraft. However, some circumstances may require the fault tree to drive the development of a new task or interval within the maintenance program to support safety requirement compliance. In many cases, failure detection means are provided by flight deck effects or are inherent within the system (e.g., being provided by self-test, power up tests).

SAENORM.COM : Click to view the full PDF of arp4761a

An FTA uses Boolean logic gates to show the relationship of a failure condition to the failure modes that may cause it. The two most common logic gates are the AND-gate and OR-gate. An AND-gate represents a condition in which the coexistence of all inputs is required to produce an output representing the higher-level event. An OR-gate represents a condition in which any one or more of the inputs produce an output representing the higher-level event. See Appendix G.

The DD replaces the FTA logic gates by paths to show the relationship of the failures; parallel paths are equivalent to the AND-gates and series paths are equivalent to the OR-gates. See Appendix H.

An MA calculates the probability of the system being in various states as a function of time. A state in the model represents the system status as a function of both the fault-free and faulty equipment and the system redundancy and monitoring. A transition from one state to another occurs at a given transition rate, which reflects equipment failure and repair rates. A system changes state due to various events such as equipment failure, reconfiguration after detection of a failure, completion of repair, etc. Each state transition is a random process which is represented by a specific differential equation. The differential nature of the model limits the computation at any point in the analysis to the probability of transitioning from any defined state to another state. The probability of reaching a defined final state can be computed by combinations of the transitions required to reach that state. See Appendix I.

An MBSA employs an analytical model called a Failure Propagation Model (FPM). The analyst uses a software application to perform an analysis of the system FPM and generate outputs such as failure sequences, minimal cut sets, or other safety-focused results. These outputs are compared to objectives and requirements by safety analysts as part of the overall safety assessment process. MBSA can be applied as a failure propagation method in performing an FMEA or CEA. See Appendix N.

SAENORM.COM : Click to view the full PDF of arp4761a

4.1.1.1 Analysis for Development or Design Errors

Systems, equipment, or their items (including software or hardware) may be qualitatively included in an FTA for the sake of evaluating the contribution of development errors to the top event (failure condition). A fault tree may be used to provide adequate analytic visibility of development safety issues for systems, especially when credit is taken for the following safety attributes:

a. Systems, equipment, or items which provide fail-safe protection against potential software development or design errors elsewhere in the aircraft or system, particularly where there may be complex functions implemented in software or hardware.

b. Systems, equipment, or items which provide protection against hardware failures.

Development or design errors (whether in the system, software, or hardware) are not the same as hardware failures. Unlike hardware failures, probabilities of such errors cannot be quantified. Therefore, numerical and categorical probabilities should not be indicated for potential errors in fault trees. Any analysis of these potential errors in an FTA should be expressed in terms of development assurance to protect against errors. The analysis should be evaluated on a purely qualitative basis. A relatively simple way of modeling the potential errors in a qualitative FTA can be done to determine the FFSs in order to assign FDALs or IDALs with architectural considerations in a PASA or PSSA, as described in Appendix P.

4.1.1.2 Average Probability

When conducting a quantitative FTA, the probabilities are estimated from the failure rates and exposure times of the basic events. Probability calculations for civil aircraft certifications are based on average probabilities calculated for all the aircraft of the same type. For the purpose of these analyses, the failure rates are usually assumed to be constant over time and are estimates of mature failure rates after infant mortality and prior to wear out.

If wear out or infant mortality is a consideration, then equipment reliability management methods such as “life limitations” or “enhanced burn-in” can be used to attain a constant failure rate. Failing that, other distribution functions (e.g., Weibull) would need to be applied. A Monte Carlo simulation could also be used. ARP5150A provides information regarding Weibull or Monte Carlo simulations, but these applications are beyond the scope of this document.

The analyses should calculate average probability of occurrence per flight hour for the failure condition assuming a typical flight of average duration and considering the appropriate exposure and “at risk” times. A more detailed discussion of the proper determination of exposure time and “at risk” times is contained in Appendix G.

When developing a new aircraft, the average flight time is usually determined from the customer requirements for the aircraft. This is an assumed value. When modifying an existing aircraft, the actual average flight time, based on in-service data, could be used.

4.2 Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects Summary (FMES)

An FMEA is a systematic, bottom-up method of identifying the failure modes of a system, function, or item and determining the effects on the next higher level. It may be initiated at any level within the system (e.g., piece-part, function, black box). Typically, an FMEA is used to identify failure effects resulting from single failures. Software can also be analyzed qualitatively using a functional FMEA approach.

An FMEA is coordinated to manage the specific analysis scope. The level of analysis of the FMEA can be adapted to have enough detail to allow the PSSA probability budgets to be met. The analysis may be accomplished at different levels of detail (e.g., component, function). An FMEA may be used as source data for failure rates in probabilistic analyses such as the FTA. Furthermore, an FMEA may be used to supplement the FTA by providing a complementary list of failure effects from the bottom up.

An FMES is a grouping of single failure modes which produce the same failure effect (i.e., each unique failure effect has a separate grouping of single failure modes). An FMES can be compiled from the aircraft manufacturer’s, system integrator’s, or equipment supplier’s FMEAs. Furthermore, an FMES is coordinated with the user to adequately address the need for inputs to higher-level FMEAs and/or SSA FTAs.

For details in performing an FMEA/FMES, see Appendix J.

4.3 Cascading Effects Analysis (CEA)

A CEA is a qualitative, bottom-up analysis which evaluates an initiating condition (e.g., a failure condition, failure mode, or combination of failure modes) and allows the analyst to determine the total effect on the aircraft for that initiating condition. The CEA iteratively identifies the direct and indirect effects that propagate from the initiating condition due to system dependencies. All systems directly or indirectly connected to the systems impacted by the initiating condition are considered in the CEA.

The CEA may be used to support any analysis that requires the determination of aircraft-level or multisystem effects for specific initiating conditions. For example, the CEA may be used to determine the system or aircraft effects of an FMEA failure mode, or the aircraft effects of a resource system (e.g., hydraulic, electrical) SFHA failure condition. The effects of each initiating condition are conveyed to the source analysis.

For details in performing the CEA, see Appendix O.

4.4 Zonal Safety Analysis (ZSA)

A ZSA is performed to evaluate the design and installation of systems and equipment to identify specific interactions or hazards, and potential maintenance hazards. The ZSA considers the physical installation of and interference between systems and equipment in order to identify potential hazards caused by mutual influences between equipment co-located on the aircraft as well as the influence of the zone operating environment on such installed equipment. The ZSA is generally performed by an airframe manufacturer but may also be performed by systems integrators or installers when applicable. ZSA concepts may also be useful in helping the PASA/PSSA processes generate physical installation requirements supporting identified Independence Principles and the SSA/ASA processes verify those requirements are met.

SAENORM.COM : Click to view the full PDF of arp4761a

The ZSA is intended to identify whether there are any zonal issues that could compromise intended independence (e.g., zone overheat affecting multiple equipment). Determining an installation solution in zones of limited volume can present challenges for which an alternate design solution or hazard mitigation should be considered.

For details in performing the ZSA, see Appendix K.

4.5 Particular Risk Analysis (PRA)

Particular risks are those physical events or influences which may violate independence, or compromise aircraft safety or aircraft survivability. These risks may be internal or external to the aircraft. Particular risks may influence several aircraft zones at the same time. Some of the particular risks may be subject to specific airworthiness requirements (e.g., engine uncontained rotor failures, tire burst).

The PRA is not a probabilistic analysis but a survivability analysis. Each particular risk is analyzed as a threat to the aircraft. The objective is not to determine how often these threats occur, but to determine the survivability of the aircraft in the presence of each threat. A probabilistic analysis may be used in support of the PRA, but the use of these analyses does not obviate the need for the survivability assessment performed in the PRA. PRA concepts may also be useful in helping the PASA/PSSA processes generate physical installation requirements supporting identified Independence Principles and the SSA/ASA processes verify those requirements are met. The results of some analyses conducted as part of the PRA, such as bird strike and tread separation analyses, may also contribute to the identification of structural design requirements.

For details in performing the PRA, see Appendix L.

4.6 Common Mode Analysis (CMA)

A CMA is a qualitative analytical method used to support evaluation of independence. In a CMA, engineering experience is systematically applied to review function, architecture, development or design, implementation, manufacturing, maintenance and operation in a logical way. Considerations are given to the independence of functions and their respective monitors. Identical systems or items could be susceptible to common development errors or failures that could cause simultaneous loss of function or malfunction of duplicate systems or items.

The CMA activity is used to facilitate the generation of requirements associated with independence and the assignment of development assurance levels associated with architecture considerations as part of PASA and PSSA. The CMA also supports independence verification occurring after implementation as part of SSA and ASA.

For details in performing the CMA, see Appendix M.

5. SAFETY-RELATED MAINTENANCE TASKS AND INTERVALS

The analytical methods in this ARP may assist manufacturers in the determination of maintenance tasks and associated intervals to ensure the aircraft can operate safely in the presence of failures. Consult the applicable regulations and guidance materials for the criteria to establish the required maintenance tasks.

The calculation of event probability associated with a latent failure takes into account the time during which the latent failure can persist without being detected.

Failures detected during periodic power-up or self-test routines may have short latent exposure time period. In other cases, however, the exposure time for some latent failures may be associated with equipment bench tests or specific aircraft maintenance tasks. In these cases, the latent period can be a considerable amount of time.

5.1 Certification Maintenance Requirements

Maintenance tasks and associated time intervals used to limit exposure times of Catastrophic and Hazardous failure conditions identified in the PSSA or SSA FTAs, are Candidate Certification Maintenance Requirements (CCMRs). Where detection is accomplished by an aircraft maintenance task, the time interval required to meet the safety objective should be transferred to the appropriate maintenance process for implementation of required maintenance procedures and time intervals.

SAENORM.COM : Click to view the full PDF of arp4761a

Some CCMRs associated with safety requirements compliance may be designated Certification Maintenance Requirements (CMRs). A CMR is a mandatory periodic task which is required to maintain the safety of the aircraft. CMRs are designed to verify that a certain failure has or has not occurred, particularly significant latent failures. A CMR is established during the design certification of the aircraft as an operating limitation of the type certificate. CMRs are established in accordance with applicable regulatory guidance, e.g., AC 25-19A/AMC 25-19.

Once established, CMRs are required maintenance tasks and must be accomplished by the operator at the prescribed intervals to maintain the airworthiness certificate of the aircraft. Where the detection method is identified to be provided by test, assurance must be provided that the test procedure, in fact, detects the latent failure of concern.

5.2 Maintenance Steering Group

CMRs are derived from a fundamentally different analysis process than the maintenance tasks and intervals that result from the Maintenance Steering Group (MSG-3) analysis associated with Maintenance Review Board (MRB) activities. MSG-3 analysis activity produces maintenance tasks that are performed for safety, operational, or economic reasons. The analysis defines a group of scheduled tasks to be accomplished at specified intervals to prevent deterioration of the inherent safety and reliability levels of the aircraft. The analysis also defines a group of non-scheduled tasks to restore the aircraft to an acceptable condition. CMRs on the other hand, are failure-finding tasks only, intended to limit the exposure to significant latent failures and wear out failures. The MSG-3 process examines failure paths by using the “next failure” criteria. (e.g., what is the next worst thing that can happen in the same system, given the first failure has occurred?). Once the MSG-3 process is complete, the minimum maintenance required is established in the MRB. Once the MRB issues their report of maintenance tasks, the aircraft operators use the report to develop their own maintenance program, working with their local authorities.

Consult AC 25-19A/AMC 25-19 for guidance on how CMR and MSG-3 tasks contribute to operators’ maintenance programs.

6. MASTER MINIMUM EQUIPMENT LIST (MMEL)

Modern aircraft are designed to have high function availability. The goal is that aircraft may be safely dispatched even if some of their components are inoperative. The list of equipment so designated is called the Master Minimum Equipment List (MMEL). Availability is usually accomplished through the use of redundancy. During the design development, a list is created through evaluation of such equipment. This list is used to determine if an aircraft can be dispatched with given equipment inoperative. For conditions where dispatch is allowed, there may be restrictions placed on the operation of the aircraft during the time allowed for dispatch in this configuration. Both qualitative and quantitative approaches have been shown acceptable to substantiate the limited time period for MMEL dispatch. The limited time period allows the aircraft to reach a major maintenance facility or to reach its next scheduled maintenance check. For example, FTA may provide rationale supporting an aircraft dispatch configuration for MMEL and be used to help determine allowable exposure time. The MMEL may also be considered in the PASA or PSSA to capture safety requirements (e.g., distinct annunciations or operational or maintenance constraints) that will be needed to ensure a successful assessment of the MMEL configuration. These applications of FTAs are associated with the risk of dispatch with equipment on the MMEL, not the average risk assessed for compliance with related regulations.

Consult CS-MMEL for guidance when the qualitative approach is supplemented by a quantitative approach.

7. TIME-LIMITED DISPATCH (TLD)

This section contains a discussion of a method currently being used to define and control dispatchability requirements for Full-Authority Digital Engine Control (FADEC) systems. The discussion is included here to provide background for this concept, Time-Limited Dispatch (TLD), which may be useful in approaching design solutions for other aircraft systems. The concept is one wherein a redundant system is allowed to operate for a predetermined length of time with faults present.

The TLD concept has been applied to dual-channel engine FADEC systems with regard to the failure condition of Loss Of Thrust Control (LOTC) of a single engine. Operating with faults present results in an increased probability of an LOTC event. TLD allows airlines to take advantage of the built-in safety margin of the FADEC system, permitting them to postpone maintenance actions for specific intervals, rather than possibly incurring delays and/or cancellations if they were forced to repair the faults prior to the next flight.

SAENORM.COM : Click to view the full PDF of arp4761a

TLD operation is conditional upon the resultant system operation and reliability being adequate to satisfy the safety requirements for operational approval. The recommended process for approval of TLD operations requires an analysis to show that the fleet average probability of an LOTC event is below a target level, such as 1.0E-05 events per operating hour. The certification authorities set the target level in terms of a fleet average LOTC rate. Faults that are classified as dispatchable are generally placed in either of two classes of dispatchable faults: a class that must be repaired in a short, defined time period and a class that is allowed to operate for a longer time before repair is required. Faults that are classified as non-dispatchable require immediate repair. Excluded from the set of dispatchable faults are those faults that must be repaired immediately (i.e., non-dispatchable faults) including those which unacceptably impact the LOTC rate. A list of which faults appear in each dispatch class and the allowable dispatch times for those faults are approved by the certification authorities. The engine type certificate data sheet will state whether the engine is approved with TLD. The limitations section of the engine maintenance manual should state the approved intervals for short-term and long-term dispatch.

Guidelines for TLD analysis for electronic engine control systems are described in ARP5107C which was revised by the SAE E-36 Committee and published in September, 2018. It provides methodologies and approaches which have been used for conducting and documenting the analyses associated with the application of TLD to the thrust control reliability of FADEC systems. It includes the background of the development of TLD, the structure of TLD that was developed and implemented on present generation commercial transports, and the use of Markov Analysis and analytic calculations to determine the periods of time during which an aircraft can be dispatched with known inoperative engine control system items, and to validate the application of TLD on FADEC-equipped aircraft. Although TLD can currently only be used for FADEC systems for LOTC, ARP5107C considers its techniques and processes applicable for other FADEC system failure effects and for systems other than FADEC (e.g., thrust reverser).

8. IN-SERVICE SAFETY ASSESSMENT

The granting of Type Certification (TC) for an aircraft is the transition point between the safety assessment before TC and the in-service safety assessment after TC. Documents describing practices for in-service safety assessments are ARP5150A and ARP5151A. Operators should consult applicable regulations from certification authorities.

To facilitate the beginning of the in-service safety assessment process, the designers may wish to develop a list of “safety-significant events” that the operators could include in their operator and service manuals to monitor or that a company field service engineer could monitor. The operators should be aware of these elements, and they may wish to pass any issues regarding these elements back to the manufacturer in accordance with ARP5150A Appendix M (Hazard Tracking) and Appendix N (Lessons Learned). The manufacturer should assess reports of issues with safety significant events in the field to determine if there is a trend or if the issue requires further investigation.

9. NOTES

9.1 Contribution Acknowledgement

The leadership of the S-18 and WG63 Committees would like to thank the committee members who have actively contributed, and their sponsoring companies, for the time, effort, and expense expended during the years of development of this document. Without the experience, cooperation, and dedication of these people, and other S-18 and WG63 committee members, development of this document would not have been possible.

SAENORM.COM : Click to view the full PDF of arp4761a

9.2 Contributors

Derek Achenbach
Shakil Ahmed
Kathryn Baksa
Steven Beland
Ahmed Butt
David Cummins
Michael Curran
John Dalton
Aharon David
Laura Dominik
Mark Eley
Sylvain Engel
Charlie Falke
Daniella Fernandes
Daniel Fogarty
Jean Gauthier
Damien Glynn
Mallory Graydon
Humberto Guimaraes
Ricardo Hachiya
Joel Harrison
Adrian Hiliuta
Lee Howard
Martin Hunter
Salvatore Infantino
Christopher Lacey
Pascal Lambert
Linh Le
Trevor Lewis
Ronald Liffrig
Jim Marko
Bob Mattern
Craig McMillan
Fred Moon
Karl Morris
Chad Moses
Isaac Munene
Laurence Mutuel
Mike Noorman
Mark Olson
Robert Olson
Ji Paik
Steven Pallotto
Michael Peterson
Warren Prasuhn
Gradimir Radovanovic
Jomar Rocha
Bradley Schafer
Douglas Sheridan
Joel Smith
Rob Soffe
Alvaro Tamayo
John Thomas
Lirong Tian
Archana Verma
Inder Verma
Komal Verma
Robert Voros
Andrew Wallington
Andy Ward
Kimberly Wasson
Steve Wilson
Franck Ybert

SAENORM.COM : Click to view the full PDF of arp4761a

9.3 Revision Indicator

A change bar (|) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

APPENDIX A - AIRCRAFT FUNCTIONAL HAZARD ASSESSMENT (AFHA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

A.1 INTRODUCTION 31
A.1.1 AFHA Process Overview 31

A.2 GATHER AFHA INPUTS 32
A.2.1 Review and Confirm Aircraft-Level Functions are Complete 32
A.2.2 Aircraft Functions 32
A.2.3 Aircraft Sub-Functions 33

A.3 IDENTIFY AIRCRAFT FAILURE CONDITIONS 34
A.3.1 Combined Failure Conditions 36

A.4 ASSESS AIRCRAFT FAILURE CONDITION EFFECTS 36

A.5 CLASSIFY FAILURE CONDITION BASED ON EFFECT SEVERITY 40

A.6 AFHA ASSUMPTIONS 41

A.7 AFHA OUTPUTS 41

A.8 FAILURE CONDITION PARAMETER AND EVENT CONSIDERATIONS 43
A.8.1 Crew Awareness 44
A.8.2 Flight Phases and Associated Operational Conditions 44
A.8.3 Operational Events 45
A.8.4 Environmental Conditions 45
A.8.5 Environmental Events 46

A.9 AFHA SUBSTANTIATION 46
A.9.1 AFHA Completeness 47
A.9.2 Failure Condition Effect Correctness 47
A.9.3 Failure Condition Classification Correctness 48

Figure A1 AFHA activities 32

Table A1 Example of aircraft functions 33
Table A2 Example of aircraft function decomposition 33
Table A3 Aircraft-level failure condition identification matrix example 35
Table A4 Frequently used effect term examples 37
Table A5 Aircraft-level failure condition effects matrix example 39
Table A6 Failure condition severity classification examples 40
Table A7 AFHA format example 42
Table A8 AFHA format example data definitions 43

SAENORM.COM : Click to view the full PDF of arp4761a

A.1 INTRODUCTION

The Aircraft Functional Hazard Assessment (AFHA) is a process that allows the identification and evaluation of potential hazards related to an aircraft regardless of the details of its design or implementation. It is performed early in the development process, re-evaluated anytime significant changes are made to aircraft functionality, and is used to establish the safety objectives for the functions of the aircraft to achieve a safe design.

When performing the AFHA, failure conditions are analyzed for their effect on the aircraft, crew and occupants to determine the associated severity classification. Flight phase, environmental and operational conditions should be considered in the assessment.

Top-level aircraft functions are typically decomposed to lower-level aircraft functions. This allows the analyst to determine if the functions and failure conditions under consideration are correct and complete for the chosen level of detail, and if the top-level function statement requires clarification. The level of detail resulting from this functional decomposition may vary between applications.

An AFHA does not consider the allocation of aircraft functions to systems. The AFHA may require change if the list of aircraft functions and failure conditions is found to be incomplete or incorrect, or if assumptions are found to be incorrect during the development process. The AFHA typically does not change as a result of system design. The effects of function allocation or design changes will likely be contained in a PASA or lower-level analysis.

A.1.1 AFHA Process Overview

The AFHA process is a top-down method for identifying failure conditions and assessing the severity of failure condition effects as shown in Figure A1.

The assessment process consists of the following activities:

a. Gather AFHA inputs.

b. Review and confirm the aircraft-level functions are complete.

c. Determine the failure conditions associated with the aircraft functions.

d. Determine the effects of each failure condition considering flight phases, operational and environmental conditions and events, and crew awareness.

e. Assess and classify the severity of each failure condition’s effects.

f. Capture and confirm AFHA assumptions.

For reuse of an existing and well vetted AFHA on a new or modified aircraft, aircraft functions and failure conditions should be re-examined to ensure the new application is similar in function, operation, and environment to the previous application.

SAENORM.COM : Click to view the full PDF of arp4761a

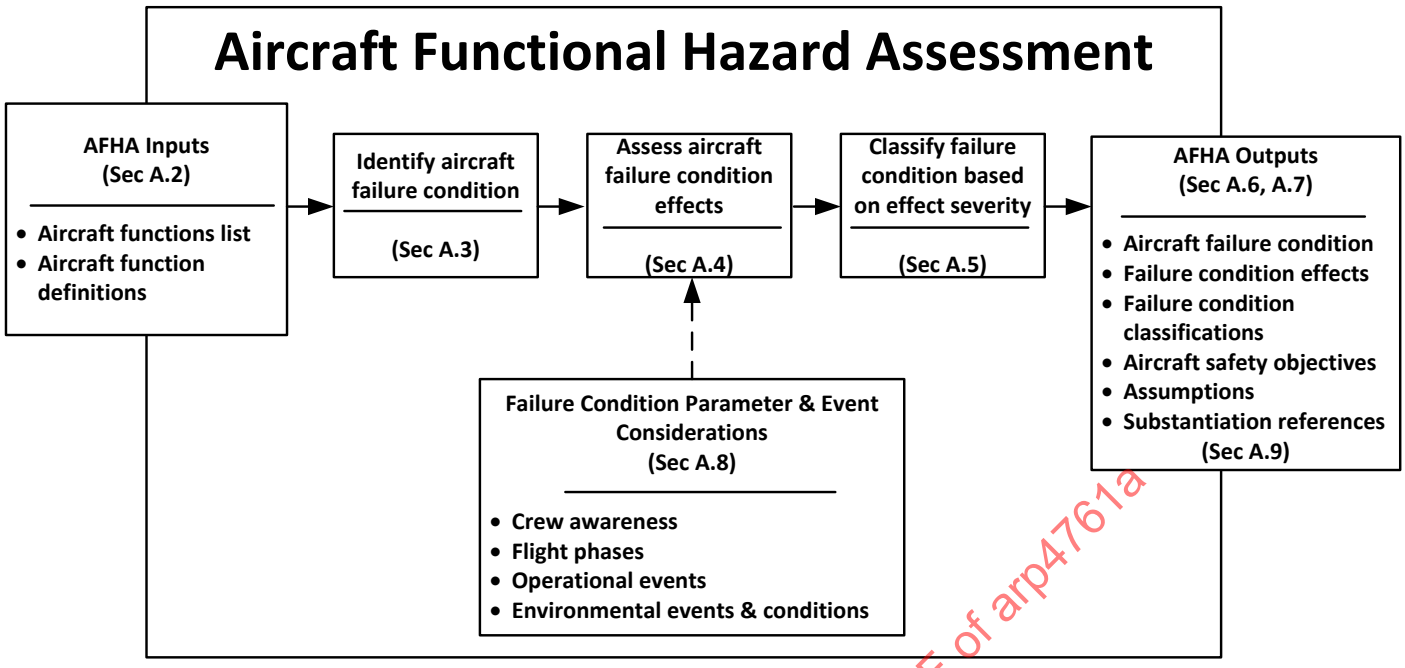


Figure A1 - AFHA activities

SAENORM.COM : Click to view the full PDF of arp4761a

A.2 GATHER AFHA INPUTS

The inputs to the AFHA are the aircraft-level functions, derived from the aircraft design objectives and the fundamental necessities of flight due to the laws of physics, and the operational and environmental conditions the aircraft is designed to encounter.

A.2.1 Review and Confirm Aircraft-Level Functions are Complete

The AFHA does not define aircraft functions; however, it requires a clear, explicit, and complete list of aircraft functions as an input.

For the AFHA, the aircraft functions should be described in terms of what the function is to accomplish, rather than the means envisioned to implement the function. For example, at the aircraft level it is recognized that a means of propulsion is required for sustained flight. This function could be described as “to provide thrust,” as this describes the objective and not the means to accomplish it.

The completeness of the function list is essential to AFHA. A complete list of functions includes all those functions necessary for the operation of the aircraft. There should be consistency between the functions analyzed in the AFHA and the aircraft functional requirements.

A.2.2 Aircraft Functions

Aircraft functions are broadly stated and intended to be inclusive of all possible implementations, as no functional decomposition or design decisions have yet been considered. The list of aircraft functions used as an input to the AFHA should include all functions performed by the aircraft as a whole. Table A1 provides an example set of aircraft functions for a passenger aircraft.

The aircraft functions are generally common to all aircraft designed to perform similar missions and are defined by the development process.

Table A1 - Example of aircraft functions

ID #	Function
1.	Provide aerodynamic performance
2.	Control aircraft trajectory
3.	Control aircraft energy
4.	Provide survivable environment
5.	Provide crew situational awareness
6.	Maintain structural integrity
7.	Provide emergency services
8.	Provide passenger services

A.2.3 Aircraft Sub-Functions

The aircraft functions may contain a breakdown into sub-functions, resulting in a hierarchical structure with two or more levels. Failure conditions are derived from the lowest level of the function decomposition and generally do not depend on system allocation or architecture. Functional decomposition does not imply a particular allocation of functions to systems, but allows more specific failure conditions to be derived and assessed in the AFHA. Functional decomposition may require extracting more detail from the referenced aircraft requirements or making assumptions regarding aircraft functionality which are not yet defined in the requirements. Any such functional assumptions should be documented and subsequently confirmed.

While the level of detail and the number of hierarchical levels of functional decomposition are left to the developer and analyst's discretion, descending to a level of detail that is dependent on system-level design is not recommended. An example of function decomposition is shown in Table A2.

Table A2 - Example of aircraft function decomposition

ID #	Function
1	Provide aerodynamic performance
1.1	Provide lift
1.1.1	Provide lift (no further decomposition at the aircraft level)
2	Control aircraft trajectory
2.1	Provide pitch stability and control
2.1.1	Provide pitch control
2.1.2	Provide pitch stability
…	(additional sub-functions omitted)
3	Control aircraft energy
3.1	Maintain or increase aircraft energy
3.1.1	Provide thrust
3.1.2	Reduce drag
3.2	Reduce aircraft energy
3.2.1	Provide controlled aerodynamic drag
3.2.2	Provide high lift capability
3.2.3	Provide deceleration on ground
4	Provide survivable environment
4.1	Provide breathable atmosphere
4.1.1	Provide oxygenated atmosphere
4.1.2	Prevent atmosphere toxicity
4.2	Provide survivable temperature
4.2.1	Provide cabin temperature control
…	(additional functions and sub-functions omitted)

SAENORM.COM : Click to view the full PDF of arp4761a

A.3 IDENTIFY AIRCRAFT FAILURE CONDITIONS

A failure condition is described by a statement that characterizes an abnormal state of a function. Failure conditions describe a failed state of the aircraft function including the amount and type of impairment. Knowledge of each function is necessary to properly define failure conditions which are correct in the context of the aircraft function, operation, and environment.

Failure conditions vary in detail with the level of function from which they are derived, from extremely broad descriptions for aircraft-level functions, such as “total loss of thrust” to very specific cases at the system-level function evaluation, such as “loss of altitude indication barometric correction.” Function decomposition to lower levels will lead to more detailed failure conditions which may be more appropriate for evaluation at the system level. Note that a failure condition is not the same as a failure mode, which describes how a particular device fails (e.g., open circuit resistor, valve jammed closed, fractured mechanical piece-part).

Failure conditions can be broadly categorized as the loss of a function or as a malfunction. Each function should be assessed and the potential for loss of the function and malfunction considered. In general, each aircraft function will have at least one loss of function and one malfunction of interest.

NOTE: The dictionary definition of malfunction includes loss of function. However, loss of function is separated here to conform to certification advisory material.

Loss of function may be total or partial. Total loss of function is a condition where the function cannot be performed by any means. Partial losses of function are conditions where the function can still be performed but only at reduced capability (e.g., reduced effectiveness or with increased difficulty). Examples of loss of function failure conditions may include:

a. Loss of oxygenated atmosphere for crew and passengers.

b. Loss of directional control of the aircraft on ground.

Malfunction is a condition where the operation of a function is different than intended excluding function loss. The aspect of the function which is incorrectly performed is described in the failure condition (e.g., erroneous, uncommanded action, misleading). Examples of malfunction failure conditions may include:

a. Uncommanded flight path pitch deviation.

b. Uncommanded release of oxygen masks for passengers.

c. Erroneous directional control of the aircraft on ground.

Failure conditions may have vastly different effects depending on whether the crew are notified and are able to perform timely mitigating actions. Where crew reaction is relevant and the effects of the failure condition are not intrinsically evident to the crew, separate failure conditions may be created considering whether the crew is aware or unaware of the condition. Examples of failure conditions considering crew awareness may include:

a. Loss of oxygenated atmosphere for crew and passengers with crew awareness.

b. Loss of oxygenated atmosphere for crew and passengers without crew awareness.

c. Loss of stall prevention functions with crew awareness.

d. Loss of stall prevention functions without crew awareness.

e. Loss of wing ice prevention with crew awareness.

f. Loss of wing ice prevention without crew awareness.

A failure condition identification matrix may be used to assist the analyst in considering all types of failure conditions for every function. This is one method of summarizing failure condition identification; other methods may be equally effective. Not all functions will have relevant failure conditions of all types.

SAENORM.COM : Click to view the full PDF of arp4761a

Table A3 illustrates a failure condition identification matrix for the aircraft level. Additional aircraft functions are added as additional rows. Additional types of failure conditions (such as distinct failure conditions with and without crew awareness) may be added as additional columns. These examples are not a full assessment and do not represent the only way to perform failure condition identification; they illustrate a useful method when performing an AFHA.

Failure conditions in the AFHA are broadly stated in order to provide a scope which encompasses all detailed failure scenarios that can lead to the top-level functional effect. Failure conditions should be derived from the list of aircraft-level functions.

If the functional decomposition is performed in such a way that the sub-functions identified are not related, failure conditions combining failures of multiple sub-functions may not be necessary. If the sub-functions are related, failure conditions combining failures of multiple related sub-functions should be identified. Functional dependency should be evaluated for all functions from which failure conditions are derived.

Table A3 - Aircraft-level failure condition identification matrix example

ID #	Aircraft Function	Total Loss	Partial Loss	Malfunction
3	Control aircraft energy			
3.1	Maintain or increase aircraft energy			
3.1.1	Provide thrust	3.1.1.T1 Insufficient thrust to maintain positive climb rate	3.1.1.P2 Insufficient thrust to meet required climb gradient	3.1.1.M1 Uncommanded high thrust
3.2	Reduce aircraft energy			
3.2.1	Provide controlled aerodynamic drag	3.2.1.T1 Total loss of controlled aerodynamic drag	3.2.1.P2 Reduced controlled aerodynamic drag	3.2.1.M1 Uncommanded aerodynamic drag device deployment
3.2.2	Provide high lift capability	3.2.2.T1 Total loss of high lift capability	3.2.2.P2 Reduced high lift capability	3.2.2.M1 Erroneous high lift device position without crew awareness 3.2.2.M2 Erroneous high lift device position with crew awareness
3.2.3	Provide deceleration on ground	3.2.3.T1 Total loss of deceleration on ground	3.2.3.P2 Reduced deceleration on ground capability	3.2.3.M1 Uncommanded deceleration on ground
4	Provide survivable environment			
4.1	Provide breathable atmosphere			
4.1.1	Provide oxygenated atmosphere	4.1.1.T1 Total loss of oxygenated air to crew and passengers	4.1.1.P2 Loss of oxygenated air to passengers only	None identified at the aircraft level
4.1.2	Prevent atmosphere toxicity	4.1.2.T1 Toxic atmosphere in flight deck or cabin	None identified at the aircraft level	None identified at the aircraft level
4.2	Provide survivable temperature and humidity			
4.2.1	Provide cabin temperature control	4.2.1.T1 Total loss of cabin temperature control	4.2.1.P2 Reduced cabin heating capability 4.2.1.P3 Reduced cabin cooling capability	4.2.1.M1 Cabin overheating 4.2.1.M2 Cabin excessive cooling

SAENORM.COM : Click to view the full PDF of arp4761a

A.3.1 Combined Failure Conditions

If the function list developed for the assessment includes related functions, the AFHA should consider combined failures of the related functions. Functions are related when they are used together or alternatively to accomplish a higher-level function. Functions are not related when they do not contribute to or affect any higher-level functions in common (other than due to crew workload or incapacitation).

Examples of related functions that would require combined failure conditions may include:

a. Navigation and communication (external communication is used as a means to accomplish navigation tasks).

b. Pressurization and supplemental crew oxygen provision (both are means to maintain crew oxygenation).

c. Pressurization and flight control function—speed brakes (both are means to prevent extended exposure to high cabin altitude).

d. Ground directional control by friction, aerodynamic force, or asymmetric thrust (all are means of directional control on ground).

As an example, if a functional breakdown of the “provide situational awareness” function from Table A1 identifies “provide navigation capability” and “provide communication capability” as separate aircraft functions, the combined failure condition “total loss of navigation and communication” should be identified. Alternatively, if the functional breakdown for the “provide situational awareness” function identifies “determine own position,” “determine heading,” and “collision avoidance” as sub-functions, only the individual failure conditions would be necessary, as these sub-functions are not related (each of them is independently necessary to accomplish the top-level aircraft function). In this case, the various contributors to each failure condition (including the combined loss of navigation and communication systems) would be identified in the PASA (see Appendix B).

A.4 ASSESS AIRCRAFT FAILURE CONDITION EFFECTS

The AFHA next examines each failure condition and determines the effects on the aircraft, crew, and occupants should the failure condition occur in each flight phase. The assessment of the effects begins with a narrative description of the consequences of the failure condition followed by a statement summarizing the failure condition’s overall impact. Comparison of the effects with the description of the hazard classifications in the applicable certification advisory material will aid in the failure condition classification process.

Flight phases are distinct time periods within an average flight duration; see A.8.2 for further detail. Failure condition effects may vary depending upon the flight phase at the time of failure condition occurrence. The failure condition effects may also be affected by operating or environmental conditions. The failure condition effects assessment considers the most severe plausible effects during each flight phase or condition. Separate failure conditions may be needed to capture a range of effects.

The effects of a failure condition for any particular flight phase are all the expected effects during the flight when the failure condition occurs in that flight phase. This includes immediate effects and effects that would occur during subsequent flight phases due to the same failure condition. For example, the effects of a “loss of ground deceleration” failure condition during the cruise flight phase include the fact that ground deceleration will be unavailable for the subsequent landing.

The effects are described by a narrative and characterized with brief statements regarding the effect in aircraft, crew and occupant categories. Not all failure conditions may have effects in all categories or the effects of a failure condition in each category may not have the same severity.

SAENORM.COM : Click to view the full PDF of arp4761a

a. "Effect on Aircraft" refers to the ability of the aircraft to perform its functions and to the aircraft's structural integrity. Aircraft effects are characterized by a statement evaluating the reduction in aircraft capability and safety margin caused by the failure condition.

b. "Effect on Flight Crew" refers to any direct physiological effect on flight deck crewmembers or to any increase in physical or mental activity required beyond the normal flight crew activity levels to counteract the effects of the failure and complete the flight safely. Typically, this includes the crew's means of detecting the failure condition (if any) and their expected actions. Effects on crew are characterized by a statement evaluating the adverse physiological effects on the crew (if any) and the increase in crew workload caused by the failure condition (if any).

c. "Effect on Occupants (Including Cabin Crew, Excluding Flight Crew)" refers to cabin crew or passenger discomfort, injury or fatalities. These effects may be the direct result of the failure condition, such as high G maneuvering or abnormal environmental conditions, or an indirect effect, such as loss of life due to loss of aircraft control resulting in an uncontrolled crash. Occupant effects are characterized by a statement evaluating the adverse physiological effects on the cabin crew or passengers caused by the failure condition.

Each of the failure condition's effects is qualitatively expressed. Usage of standard assessment terms facilitates consistency between failure condition descriptions.

The qualitative effects assessments should consistently evaluate the same effects across all failure conditions. For example, the summary statement for effects resulting in a delayed rotation at takeoff should be consistent across different failure conditions, whether the delayed rotation is caused by a reduction in available thrust, by an inadequate control surface configuration, or by any other cause.

Table A4 provides an example of frequently used assessment terms to summarize failure condition effects. Table A4 is based on certification guidance material applicable to transport category aircraft. A set of standard effect assessment terms should be obtained from the appropriate current guidance material.

Table A4 - Frequently used effect term examples

Effect on Aircraft	Effect on Flight Crew	Effect on Occupants (Including Cabin Crew, Excluding Flight Crew)
Loss of aircraft	Crew unable to accomplish required tasks, or Required crew strength or skill in excess of crew capability, or Crew incapacitation, or crew fatalities	Multiple occupant fatalities
Large reduction in aircraft functional capability or safety margin	Excessive crew workload increase, crew unable to fully accomplish required tasks, or Crew physical distress	Small number of occupant fatalities or severe injuries not including flight crew
Significantly reduced aircraft functional capability or safety margin	Significant crew workload increase, or Conditions impairing crew efficiency, or Crew physical discomfort	Occupant physical distress or non-fatal injuries
Slightly reduced aircraft functional capability or safety margin	Slight crew workload increase	Occupant physical discomfort
No effect on aircraft functional capability or safety margin	No effect on crew workload or physiology	No effect on occupant physiology

A matrix or table may be used to capture the evaluation of each failure condition, applicable flight phases, failure effects descriptions, and relevant environmental or operational conditions. The specific evaluation format for describing the effects is not critical, provided it is thorough.

SAENORM.COM : Click to view the full PDF of arp4761a

Table A5 illustrates a possible failure condition effects capture matrix for one aircraft-level failure condition. Similar tables would be constructed for each failure condition identified. The effects described in this example are illustrative; actual effects vary with each aircraft design.

In this method, one failure condition effects matrix is constructed for each failure condition. Additional depth can be added to the matrix by adding detail to the flight phases, such as separating “takeoff” into “takeoff below V1” and “takeoff above V1,” by adding specialized flight phases such as ETOPS cruise or CAT 2 approach, or by adding operational or environmental events to the failure condition. These are described further in Section A.8.

Initial assessment of the failure conditions should address the basic flight phases (taxi, takeoff, climb, cruise, descent, approach, and landing).

Assumptions may need to be established in order to predict some failure condition effects. Any such assumptions should be documented and subsequently confirmed.

SAENORM.COM : Click to view the full PDF of arp4761a

Table A5 - Aircraft-level failure condition effects matrix example

Function: 3 Control Aircraft Energy / 3.2 Reduce Aircraft Energy / 3.2.2 Provide High Lift Capability			
Failure Condition: 3.2.2.M1 Erroneous High Lift Device Position Without Crew Awareness			
Flight Phase	**Effect on Aircraft**	**Effect on Flight Crew**	**Effect on Occupants**
Taxi Takeoff	The affected high lift device may be at a position such that the maximum angle of attack and lift achievable are less than the expected values for the commanded configuration. No warning or indication is presented to the crew. Complete loss of angle of attack safety margin and lift capability is possible.	The crew will be unaware of the condition due to erroneous indications and lack of evident effects or system warnings. The crew will proceed with a normal takeoff; however, liftoff may not be possible at the expected rotation speed. No effective crew action to prevent a high-speed runway overrun.	Multiple occupant fatalities or severe injuries are possible.
Climb	The affected high lift device may fail to reach a fully stowed configuration. No warning or indication is presented to the crew. Complete loss of structural margins is possible if the device remains deployed at cruise speed.	The crew may be unaware of the condition due to erroneous indications and lack of evident effects or system warnings. Identification of the condition due to reduced aircraft acceleration and increased noise is possible, but would require significant crew experience. Crew action to maintain control of the aircraft is not effective should structural failure of the high lift device occur.	Multiple occupant fatalities or severe injuries are possible.
Cruise	Erroneous high lift position will be detected by crew due to aircraft effects. See Erroneous high lift positioning failure condition.		
Descent	Erroneous high lift position will be detected by crew due to aircraft effects. See Erroneous high lift positioning failure condition.		
Approach	The affected high lift device may be at a position such that the maximum angle of attack and lift achievable are less than the expected values for the commanded configuration. No warning or indication is presented to the crew. Complete loss of angle of attack safety margin and lift capability is possible.	The crew will be unaware of the condition due to erroneous indications and lack of evident effects or system warnings. The crew will proceed with a normal approach; however, lift capability may be insufficient at the expected reference speed. Stall recovery may not be possible at low altitude.	Multiple occupant fatalities or severe injuries are possible.
Landing	The affected high lift device fails to return to the stowed position for ground operation. No warning or indication is presented to the crew. No effect on functional capabilities for ground operation or safety margins.	The crew will be unaware of the condition until the external visual inspection preceding the subsequent flight. Crew will note the incorrect high lift device position during preflight walk around and note the equipment for maintenance action prior to dispatch.	No effect.

SAENORM.COM : Click to view the full PDF of arp4761a

A.5 CLASSIFY FAILURE CONDITION BASED ON EFFECT SEVERITY

When the identification and summary of all failure condition effects is complete, the failure condition classification activity can begin. A classification is established for each flight phase by assessing the effects on aircraft, crew and occupants. The most severe of these effects drives the failure condition classification in each flight phase. An overall failure condition severity classification may be determined by selecting the worst-case classification from the applicable flight phases.

It is important to avoid assuming a severity classification during the identification of failure effects, as the assessment process can be incomplete if there is excessive focus on preconceived outcomes for common failure conditions.

The statements of effects from Section A.4 are used to determine the classification of each failure condition by comparison to the appropriate regulatory guidance. Table A6 provides an example of such a reference, based on certification guidance material for transport category aircraft. The classifications are: Catastrophic, Hazardous, Major, Minor, and No Safety Effect. Determination of the severity classification is direct if the qualitative assessment of the effects is consistently performed and the summaries clearly stated.

Table A6 - Failure condition severity classification examples

Effect on Aircraft	Effect on Flight Crew	Effect on Occupants (Including Cabin Crew Excluding Flight Crew)	Classification
Loss of aircraft	Crew unable to accomplish required tasks, or Required crew strength or skill in excess of crew capability, or Crew incapacitation, or Crew fatalities	Multiple occupant fatalities	Catastrophic
Large reduction in aircraft functional capability or safety margin	Excessive crew workload increase, crew unable to fully accomplish required tasks, or Crew physical distress	Small number of occupant fatalities or severe injuries not including flight crew	Hazardous
Significantly reduced aircraft functional capability or safety margin	Significant crew workload increase, or Conditions impairing crew efficiency, or Crew physical discomfort	Occupant physical distress or non-fatal injuries	Major
Slightly reduced aircraft functional capability or safety margin	Slight crew workload increase	Occupant physical discomfort	Minor
No effect or aircraft functional capability or safety margin	No effect on crew workload or physiology	No effect on occupant physiology	No Safety Effect

SAENORM.COM : Click to view the full PDF of arp4761a

For many functions, published certification guidance material can be used as a reference for the qualitative categorization of failure effects and severity classification. This guidance may include a brief statement describing the failure condition and applying a severity classification directly, or may describe certain types of effects which are considered unsafe conditions. This data can be used as reference points to classify similar failure conditions.

A.6 AFHA ASSUMPTIONS

There are instances where details necessary to perform the AFHA are not yet available. In these cases, the safety analyst should make assumptions regarding operating or environmental conditions, airframe capabilities or other factors. Assumptions may be made for as-yet-unspecified development information. These are inputs to the AFHA process which are necessary, but were not yet available in the functional information provided to the AFHA process.

Any consideration made during the assessment that was not based on validated functional information should be documented as an assumption. Depending on the maturity of the aircraft definition at the time of the AFHA, the number of assumptions in an aircraft-level assessment may be significant or almost nonexistent.

Assumptions should be captured and formally communicated to the appropriate development information sources. The assumption may then be confirmed, or corrected based on new development information. In the latter case, a design change or a revision of the AFHA may be required.

Any assumptions made in the AFHA evaluation will be tracked as part of the development program activities.

A.7 AFHA OUTPUTS

The output of the AFHA process should include:

a. The list of aircraft-level functions and functional decomposition used as an input to the assessment including supporting discussions needed to aid the understanding of the function scope and purpose and the relationship between top-level functions and lower-level functions.

b. The detailed AFHA worksheet containing all the identified failure conditions, their effects during each flight phase, and their resulting severity classifications (which define the applicable safety objectives).

c. The list of assumptions used in identifying functions, performing the function decomposition, identifying failure conditions, determining failure condition effects or determining severity classifications.

d. The list of substantiation references used to determine failure conditions and effects are correct and complete.

Table A7 provides an example of a detailed AFHA results worksheet. Table A8 provides the definition description of the data field entries in the Table A7 AFHA example worksheet.

The AFHA is not expected to significantly change as the development process proceeds since the aircraft-level functions and decomposition do not depend on system architecture. Only assumptions found to be incorrect, changes to basic airframe definitions or high-level operating parameters have the potential to invoke a revision of the AFHA.

AFHA results are an input to the PASA. If the PASA identifies deficiencies in the analysis, or design deficiencies that cause aircraft functional information to be changed, this may result in an iteration of the AFHA.

SAENORM.COM : Click to view the full PDF of arp4761a

Table A7 - AFHA format example

1	2	3	4	5	6
ID #	**Failure Condition**	**Flight Phase**	**Effects of Failure Condition on Aircraft, Crew, Occupants**	**Severity Classification**	**Assumptions, Comments, Rationale or Reference to Supporting Material**
Aircraft Function: (4) Provide Survivable Environment			Sub-Function: (4.1) Provide breathable atmosphere		
Sub-Function: (4.1.1) Provide oxygenated atmosphere					
4.1.1.T1	Unannunciated total loss of oxygenated air to crew or passengers	Climb Cruise Descent	Aircraft: No effect. Crew: Unaware or unable to counter the effects of the condition, the crew may be incapacitated by hypoxia or unable to restore sufficient levels of oxygen to the occupants in time to prevent permanent physiological harm. Occupants: Multiple occupant fatalities or severe injuries are possible due to the direct effects of hypoxia or due to crew incapacitation and subsequent loss of aircraft control.	Catastrophic	14CFR/CS 25.841(a)(2)(ii) “Pressurized Cabins” 14CFR /CS 25.1441(d) “Oxygen equipment and supply” 14CFR /CS 25.1443(c)(2) “Minimum mass flow of supplemented oxygen” AC 25-20 (6)(e)&(7) “Pressurized Ventilation and Oxygen System Assessment for Subsonic Flight Including High Altitude Operations” EASA Certification Review Item “Airworthiness Standards for Subsonic Transport Aeroplanes to be operated above 41,000 ft.”

SAENORM.COM : Click to view the full PDF of arp4761a

Table A8 - AFHA format example data definitions

Column	Table Entry	Entry Definition
--	Aircraft Function Sub Function	The hierarchy of the aircraft function and sub-functions being analyzed. The number of levels in the aircraft-level functional decomposition is at the analyst's discretion; however, the decomposition of aircraft-level functions should not presume a particular allocation of functions to systems. See Section A.2.
1	ID No.	Unique numbering system for organization, tracking, and traceability.
2	Failure Condition	Description of the failure or impairment of the function. See Section A.3.
3	Flight Phase	List the applicable aircraft operational phases for this failure condition. See Section A.4.
4	Effect of Failure Condition on Aircraft, Crew, Occupants	Description of the failure condition effects on the aircraft, crew and occupants. Sufficient detail should be provided to understand the failure scenario and conclude the severity classification based on the captured effects. Separate effects statements and classifications may be provided for each flight phase or a generalized effect and worst-case classification provided for the failure condition in all flight phases or for groups of flight phases. See Section A.4.
5	Severity Classification	Catastrophic, Hazardous, Major, Minor, or No Safety Effect as defined in applicable certification guidance material. See Section A.5.
6	Assumptions, Comments, Rationale, or Reference to Supporting Material	Data supporting the determination of effects and classification of the failure condition, including any applicable guideline material. See Sections A.6 and A.9.

A.8 FAILURE CONDITION PARAMETER AND EVENT CONSIDERATIONS

The effects of each failure condition are determined by constructing a scenario narrating its expected outcome. The failure effect scenario description includes immediate effects due to the failure condition and subsequent resulting effects due to the same failure condition. The failure effect scenario may also include events occurring concurrently with the failure condition under evaluation. This scenario includes the parameters at the moment the failure occurs. The events may intensify or mitigate the effects of the failure condition, or affect the crew's ability to recognize and correctly react to the failure condition situation.

In this context the term "parameter" is used for factors that are always present and vary in quantity or intensity (e.g., aircraft weight, aircraft speed) and for factors that may be present or absent but are commonly encountered (e.g., clouds obscuring vision, icing conditions). The term "event" is used for factors that occur at a distinct time and place and that are not regularly encountered (e.g., windshear).

Evaluating the influence of parameters and events on the failure conditions is part of the AFHA process. These factors should be carefully considered as they may be significant in some instances and irrelevant in others. For example, a wet runway is a significant factor when evaluating failure conditions associated with friction-based deceleration features, but is not significant when evaluating failure conditions related to environmental control of the cabin. Failure condition effects should consider that the failure condition can occur at any moment and under any condition encountered in the operating envelope of the aircraft. The failure condition effects should account for the failure effects over the range of the operating envelope and the analyst may separate the failure effects if they differ across the envelope.

SAENORM.COM : Click to view the full PDF of arp4761a

Evaluating failure effects for each flight phase as described in Section A.4 provides a structure that facilitates addressing the influence of the various operational and environmental factors where appropriate. Generally, each flight phase will provide an expected value or a range of values for most operating conditions (e.g., the flight phase “landing” limits aircraft weight and speed to values expected during that part of the flight).

The intended operating limits of the aircraft define the boundaries for many of these factors. For example, an aircraft intended to operate at altitudes above 25000 feet will consider the effects of high altitude exposure when evaluating the effects of related failure conditions during the climb, cruise, and descent flight phases. These factors should include consideration at their most severe limit within the approved flight envelope.

Sections A.8.1 through A.8.5 provide a method to address operational and environmental parameters and events; however, other methods may be equally effective.

A.8.1 Crew Awareness

Whenever the failure effect is significantly affected by crew action, separate failure conditions should be created and assessed, which consider the crew being either aware or unaware of the failure condition.

For failure conditions with crew awareness (i.e., which have an associated alert or are evident), the description of effects on the crew should capture how the crew becomes aware of the failure condition, how the crew is assumed to act in response to it, and the result of the expected crew action.

For failure conditions without crew awareness (i.e., which neither have an associated alert nor are evident), it should be assumed that the crew will continue to perform their duties normally, which may affect the severity of the failure condition effects. (i.e., crew will not take any action regarding the failure condition).

A.8.2 Flight Phases and Associated Operational Conditions

The flight profiles the aircraft is expected to perform should be determined. Certain aircraft perform only or mostly one type of flight profile (e.g., airliners perform transport flight profile), while others may perform several distinct types of flight profiles (e.g., some rotorcraft may perform transport, search and rescue, and other types of profiles). Based on the expected flight profiles, a list of flight phases should be determined. A flight phase is a distinct period within a flight, generally associated to the tasks being accomplished by the aircraft and its flight crew. As a minimum for a transport category flight profile, taxi, takeoff, climb, cruise, descent, approach, and landing should be considered.

The identified set of normal flight (and ground operation) phases should be applied through the entire assessment. A more detailed breakdown of the flight phases may be used where relevant distinctions in failure effects exist within the basic flight phases. Since failures can occur at any time, all normal flight phases should be considered for all failure conditions to ensure completeness.

Operational conditions, such as aircraft weight, speed, and altitude, may be directly related to the various phases of flight. For each flight phase, operational conditions should be considered throughout the approved flight envelope.

Specialized flight phases may also be considered. In general, a specialized flight phase should be considered when all of the following are true:

a. The specialized flight phase is deliberately initiated.

b. The specialized flight phase persists for a measurable duration.

c. The duration of the specialized flight phase can be determined as a fraction of a mission profile.

d. A particular aircraft can be expected to experience the specialized flight phase multiple times during its service life.

Specialized flight phases should be systematically considered when evaluating all functions, though when the effects of a failure condition are not affected by the specialized flight phase, it can be considered not applicable. Some examples of specialized flight phases include go-around, holding, and steep approach.

SAENORM.COM : Click to view the full PDF of arp4761a

A.8.3 Operational Events

Distinct occurrences and flight operations which are only performed as a response to specific occurrences or failures may be considered operational events. In general, an occurrence or flight operation should be assessed as an operational event when all of the following are true:

a. The occurrence or flight operation occurs at a distinct time.

b. The occurrences or flight operations have a known statistical probability, fleet wide, or industry wide rate of occurrence.

c. A particular aircraft is not expected to frequently experience the occurrence or flight operation during its service life, or may not experience it at all.

These operational events should be systematically considered when evaluating all functions, though they should only be applied to relevant failure conditions. Some examples of occurrences and flight operations that can be considered operational events include Rejected Takeoff (RTO) and in-flight diversion.

Operational events should be added to the relevant failure condition statements, creating new combined failure conditions. When considering the combination, it is important to ensure that the operational event is independent from the original failure condition. Examples of combined failure statements at the aircraft level are:

a. Loss of deceleration capability and RTO.

b. Erroneous fuel quantity indication and in-flight diversion.

Where operational events affect the severity of the failure condition, the original failure condition should be retained and a combined failure condition (original failure condition and operational event) added to the AFHA. The combined failure condition should be assessed for all identified flight phases where the operational event can occur.

A.8.4 Environmental Conditions

Worst-case environmental conditions within the approved aircraft operating envelope should be considered to be present where relevant when evaluating the effects of failure conditions. These conditions are implicitly assumed and need not be specifically stated for every failure condition, though their influence should be described in the failure effects narrative when relevant. Examples of environmental conditions to be considered are:

a. Airfield temperature and altitude within the approved operating limits.

b. In-flight temperature and altitude within the approved operating limits.

c. Night time and clouds obscuring external vision, for aircraft approved for Instrument Flight Rules (IFR) operation.

d. Icing conditions, for aircraft approved for flight in known icing conditions.

e. Gusting and turbulence.

In some cases, the approved envelope for an environmental condition includes extremes that are infrequent. In these cases, it may be acceptable to define a range of normally encountered conditions, with conditions outside this range considered to be environmental extremes. Examples of potential environmental extremes include:

a. Cross winds at design limits.

b. High or low external temperature at design limits.

c. Gusts and turbulence at design limits.

SAENORM.COM : Click to view the full PDF of arp4761a

It may be acceptable to add the environmental extreme explicitly to the failure condition. Where environmental extremes affect the severity of the failure condition, the original failure condition should be retained and a combined failure condition (original failure condition and environmental extreme) added to the AFHA. Examples of failure conditions incorporating environmental extremes are:

a. Loss of yaw control and cross wind at limit conditions.

b. Loss of load alleviation functions and wind gust at limit conditions.

The combined failure condition should be assessed for all identified flight phases.

A.8.5 Environmental Events

Certain abnormal environmental occurrences may be considered environmental events. Examples of environmental events include:

a. Wind shear or microburst.

b. Iced runway.

c. Icing conditions, for aircraft not approved for flight in known icing conditions.

When an environmental event affects the severity of a failure condition, the original failure condition should be retained and a combined failure condition (original failure condition and environmental event) added to the AFHA. The combined failure condition should be assessed for all applicable flight phases.

A.9 AFHA SUBSTANTIATION

Substantiating data for the AFHA should be collected, showing that:

a. All the aircraft-level functions have been considered.

b. All failure conditions have been identified for each aircraft function.

c. The failure effects on the aircraft, crew and occupants are complete and correct for each failure condition occurring during each flight phase.

d. The correct failure classification has been selected based on the failure effects.

e. The assumptions used to develop the assessment are confirmed and evidence is provided. In cases where an assumption is incorrect, the correct information should be provided and the AFHA updated.

Substantiation of the completeness and correctness of the AFHA requires documentation of the rationale and assumptions for all failure effects and classifications.

For those failure conditions with effects that are not clearly predictable or demonstrably similar to previous applications, additional supporting information, such as simulation results, analytical studies, laboratory test results, flight test results, or field data may be necessary to substantiate the effects and classification. This information may be available in existing documentation or may have to be obtained from dedicated activities.

While comparison with previous experience may be sufficient rationale for typical failure effects and classifications, if a project integrates functions in new or novel ways, the assessment of effects may require more extensive examination.

SAENORM.COM : Click to view the full PDF of arp4761a

The failure condition identification matrix and failure condition effects matrix tools provide a guide for the assessment process. After initial assessments, the failure condition effects matrix may be expanded to include specialized flight phases, crew awareness, and environmental or operational conditions as previously described. These additional considerations may generate additional flight phases or new failure conditions combining failures with operational or environmental events. The rationale for the application of these factors to failure conditions should be recorded.

Documentation of supporting materials (e.g., analyses, studies, tests) used in determining the effects and classification of failure conditions should be preserved to substantiate the AFHA. When reusing AFHA content or substantiating by similarity, any applicable lessons learned acquired since the previous application should be incorporated.

A.9.1 AFHA Completeness

A multi-disciplinary engineering review is recommended to ensure that the AFHA has addressed all failure conditions and their effects. Reviewers should be able to find evidence within the AFHA documentation that:

a. All aircraft-level functions have been considered.

b. All failure conditions have been identified for each lower-level aircraft function in the aircraft function decomposition, including loss of the function and malfunction.

c. Where lower-level aircraft functions are related, all combined failure conditions which lead to the loss or malfunction of a higher-level aircraft function have been identified.

d. The effects of each failure condition have been determined for its occurrence during all flight phases, including any applicable specialized flight phases.

e. The influence of operating conditions, operational events, environmental conditions, and environmental events have been considered where appropriate.

f. All assumptions have been captured and confirmed.

AFHAs performed for previous aircraft of similar design and function may be reused, though effects and classifications should be confirmed to be applicable to the new design. Any gaps identified in previous analyses or other applicable lessons learned should be addressed.

A.9.2 Failure Condition Effect Correctness

There are multiple means to substantiate that the effects of each failure condition during each flight phase are correct. Different methods may be appropriate depending on the type of failure condition and the difficulty of assessing its consequences.

One or more of the following methods should be used to substantiate each failure condition’s effects:

a. Pilot and human factors evaluation: Failure conditions where crew reaction significantly influences the effects of the failure, should be evaluated by experienced pilots and human factors specialists. The means and timeliness of failure recognition, intuitive or procedural response and overall workload should be substantiated.

b. Engineering evaluation: Direct and indirect functional effects of the failure condition may be determined based on previous experience and knowledge of aircraft of similar design and operational characteristics, on data and rationale obtained through certification authority and industry literature, and on analytical or simulation results. Certification authorities and aircraft manufacturers may retain senior engineers recognized for their expertise and experience who may be consulted for this purpose.

c. Published historical data: Historic precedent or accident or incident narratives for similar occurrences can be used to determine the expected effects of the failure condition. Due to the fact that incidents or accidents are very specific occurrences, the analyst should ensure that the events in question are indeed representative of the failure condition.

SAENORM.COM : Click to view the full PDF of arp4761a

d. Published guidance: Certification authority provided guidance material may specify a severity classification for the failure condition. When such a classification is given, the effect on aircraft, on flight crew, and on occupants excluding fight crew may be inferred. When guidance material is used as a reference to establish a severity classification, it is necessary to substantiate that the details of the particular application being considered are fully consistent with the scenario described in the guidance material. Aircraft function, operational, and environmental conditions should be shown not to increase the severity of the failure conditions.

e. Testing: Where necessary and practical, controlled testing may be performed to assist in the substantiation of failure effects. Equipment, system rig or aircraft prototype testing may confirm effects of failure conditions on the aircraft. Pilot in the loop testing on representative flight simulation platforms may be used to evaluate crew reaction, crew workload, or controllability aspects of a failure condition.

A.9.3 Failure Condition Classification Correctness

Confirmation of the correct severity classification consists of evaluating the known failure effects in relation to the qualitative severity scales associated with the applicable severity classifications and determining that the correct severity classification has been selected for each failure condition during each flight phase. This task can typically be accomplished by inspection of the AFHA worksheets. Failure conditions classified as Catastrophic generally do not require confirmation, as this classification is the most severe and carries the most stringent safety objectives.

Failure condition severities and requirements that are specified in aircraft certification guidance material have usually been specified due to accident or incident experience, or collaborative expert experience and opinion. If the guidance material specifies a worst-case failure condition severity, there is likely no need to further assess effects unless the applicant desires to show justification that the worst-case effects implied by the guidance material are not applicable to their particular aircraft.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX B - PRELIMINARY AIRCRAFT SAFETY ASSESSMENT (PASA)

NOTE: The main body of this document contains information that places the procedures in this appendix in context. This appendix is to be used in conjunction with the main body of the document.

TABLE OF CONTENTS

B.1 PASA OVERVIEW 50

B.2 PASA INPUTS 51
B.2.1 Aircraft Functions and Failure Conditions from AFHA 51
B.2.2 Requirements 52
B.2.3 Initial Operational Considerations 52
B.2.4 Proposed Aircraft Architecture 52
B.2.5 Failure Conditions from System FHAs 52

B.3 INTERDEPENDENCE ANALYSIS 52

B.4 FAILURE CONDITION EVALUATION 54
B.4.1 Multifunction and Multisystem (MF&MS) Analysis 55
B.4.2 Assignment of FDALs 55
B.4.3 Supporting Analyses 56
B.4.4 PASA Safety Requirements and Assumptions 61

B.5 PASA COMPLETION 62

B.6 PASA OUTPUTS 63
B.6.1 Capturing PASA Outputs 63
B.6.2 Relationship Between PASA and ASA 64

Figure B1 PASA flow 51
Figure B2 Independence Principle flow through Common Cause Analyses 60

Table B1 Interdependence table example 53
Table B2 Combined Functional Failure Effects (CoFFE) table example 56
Table B3 Common Resource Analysis table example for failure condition “Loss of adequate deceleration means” 59

SAENORM.COM : Click to view the full PDF of arp4761a

B.1 PASA OVERVIEW

The Preliminary Aircraft Safety Assessment (PASA) process is a systematic examination of a proposed aircraft architecture. In the context of the AFHA failure condition safety objectives, the PASA also identifies aircraft-level safety requirements (e.g., FDAL, independence, probability, functional, or performance) to address AFHA failure conditions, whether they are allocated to one system or many systems.

The PASA identifies the interactions and dependencies between the aircraft systems, assesses how their failures can lead to the aircraft-level failure conditions identified by the AFHA, and determines whether the safety objectives can be met. The PASA process interacts with the development process by evaluating the proposed aircraft architecture and identifies the need for specific safety requirements. Just as the development process is iterative, the PASA process is iterative throughout the development cycle. Periodic updates to the PASA may be necessary as the aircraft architecture matures to ensure a complete set of data is available to support the aircraft certification.

The PASA is particularly important when evaluating complex integration of aircraft systems that pose additional failure combinations that might not otherwise be present when aircraft functions are implemented by stand-alone systems. From the aircraft-level perspective, typical interactions and interdependencies involve multiple systems that together implement an aircraft-level function; this includes reliance on common resources, e.g., hydraulic power, electrical power, air data, air-ground logic, common computing, and data networks.

The PASA process begins during the initial aircraft architecture development phase. The main objectives of the PASA are to assess the proposed aircraft architectures and develop safety requirements; with these requirements established, the aircraft and individual systems' development can proceed with reduced risk.

Throughout this appendix, reference is made to using Fault Tree Analyses (FTAs). It should be understood by the reader that Dependence Diagrams (DDs), Markov Analyses (MAs), or other techniques may be selected to accomplish the same purpose, depending on the circumstances and the types of data desired.

The PASA is conducted as shown in Figure B1. The PASA process includes the following activities which are described in more detail in the sections referenced:

a. Gather input data (Section B.2).

b. Perform an Interdependence Analysis (Section B.3).

c. Perform failure condition evaluation and propose safety requirements (Section B.4).

d. Determine whether safety considerations are achievable (Section B.5).

e. Document assessment results, including safety requirements (Section B.6).

SAENORM.COM : Click to view the full PDF of arp4761a

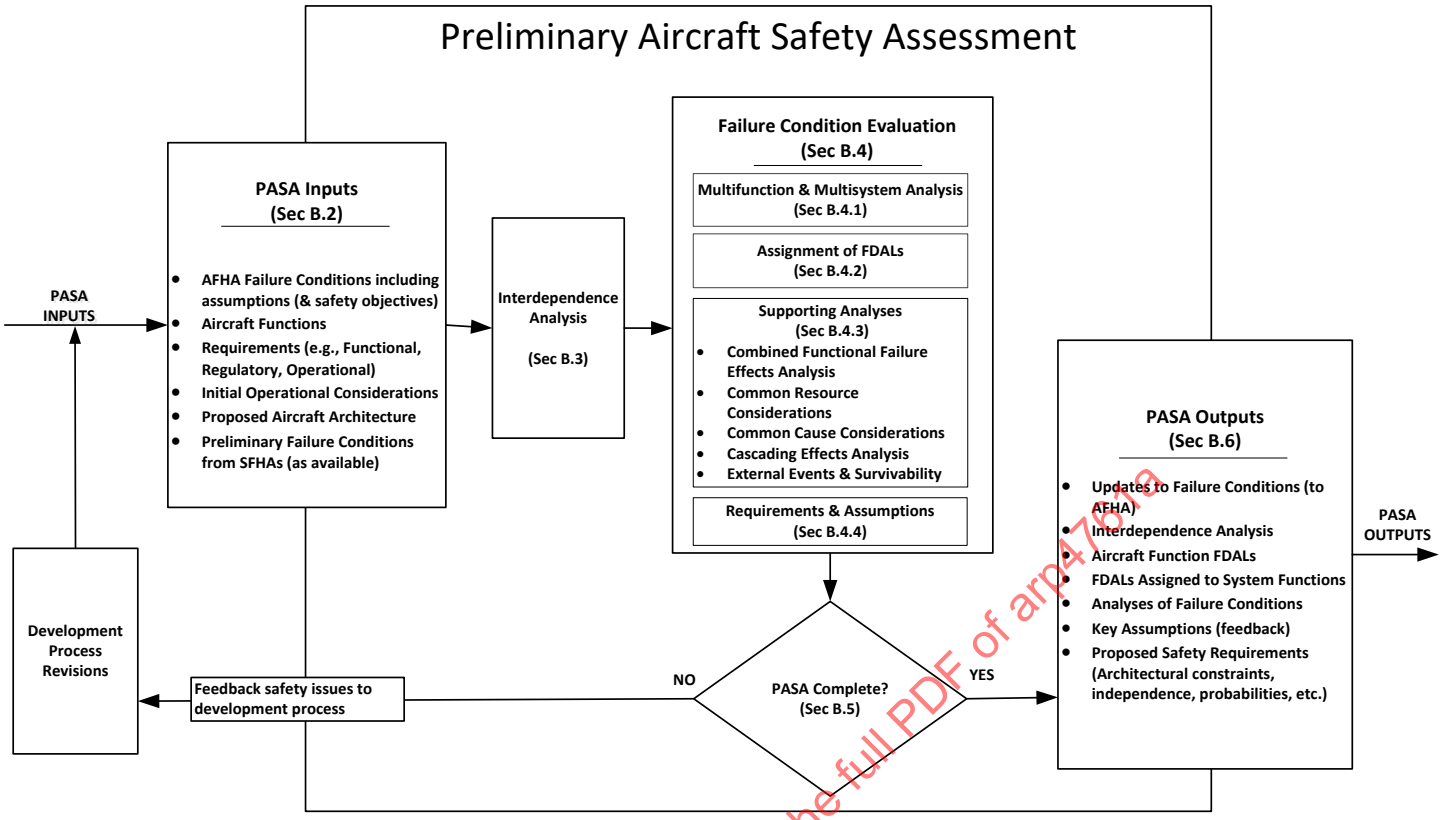


Figure B1 - PASA flow

If the PASA evaluation determines that the safety considerations are not achievable, feedback is provided to adjust the aircraft architecture and/or aircraft operations early in the development.

PASA should be performed in accordance with the depth of analysis outlined in 3.8 of the main body to scope the aircraft-level failure condition evaluations.

B.2 PASA INPUTS

These inputs constitute the minimum data necessary for the safety analyst to commence the assessment:

a. AFHA outputs including failure conditions and associated functions.

b. Requirements.

c. Initial operational considerations.

d. Proposed aircraft architecture.

System failure conditions from the SFHAs may also be helpful.

B.2.1 Aircraft Functions and Failure Conditions from AFHA

All aircraft functions and their associated failure conditions, safety objectives, and all assumptions from the AFHA should be identified for evaluation in the PASA. Safety objectives from the failure conditions may be expressed in terms of numerical probabilities or single failures influenced by regulations or company policies. Safety objectives may be either stated clearly in the AFHA or may be determined in the PASA.

SAENORM.COM : Click to view the full PDF of arp4761a

B.2.2 Requirements

Requirements which aid in the understanding of how the aircraft and systems should be used and how they interact with their environment need to be considered to provide context of the description of the aircraft architecture. These requirements may include, amongst others:

a. Functional: What the functions are intended to do.

b. Operational: How the aircraft will be used and maintained.

c. Certification: Applicable regulations and policies.

B.2.3 Initial Operational Considerations

The initial information such as operational procedure recommendations, training outlines, or flight limitations is used by the PASA to reflect the intended usage of the aircraft. Such initial information might be derived from prior similar aircraft procedures and may eventually be included in:

a. Aircraft Flight Manual (AFM).

b. Operations manual.

c. Annunciation checklists.

d. Training syllabus.

e. Instructions for Continued Airworthiness.

f. Expected aircraft usage parameters (e.g., flight phases, ETOPS, flight lengths).

B.2.4 Proposed Aircraft Architecture

A conceptual representation of the proposed architecture is essential to allow the architecture to be evaluated for compliance with the failure condition classifications from the AFHA and other applicable safety requirements. This aircraft architecture definition should include the aircraft function allocations to systems, system interactions, common resource systems, and other dependencies. As the design matures, a more detailed representation of the architecture may iteratively be applied to the PASA process.

B.2.5 Failure Conditions from System FHAs

The PASA considers system failure conditions as they contribute to the aircraft failure conditions. Although the SFHAs are not needed to start the PASA, these failure conditions are used to support a more complete analysis of the aircraft-level failure conditions to check the system failure conditions before the PASA is finished.

B.3 INTERDEPENDENCE ANALYSIS

Once the available input data has been gathered, the PASA process identifies the interdependencies of the systems functions and sub-functions that contribute to each aircraft-level failure condition. An Interdependence Analysis is used to provide visibility of the interactions between aircraft functions and systems so that they may present a more complete view of the interactions for the AFHA failure condition evaluations. The Interdependence Analysis can be used in the failure condition evaluation (Section B.4) to identify the need for functional independence and separation.

An Interdependence Analysis can be conducted by systematically following these process steps:

a. Select an aircraft-level function and associated AFHA failure conditions to analyze.

b. List all systems in the aircraft architecture (which may include resource systems).

SAENORM.COM : Click to view the full PDF of arp4761a

c. Identify which systems could contribute to that aircraft-level failure condition.

d. Repeat above steps for each aircraft-level function and associated AFHA failure condition.

Although the Interdependence Analysis can readily account for systems that have the aircraft functions allocated to them, it may also need some minimum input from SFHAs to eventually account for system aspects that were not allocated to the aircraft function (e.g., thrust control failure condition of inadvertent forward thrust affects aircraft-level function to decelerate the aircraft, but it is not allocated to the function).

The Interdependence Analysis may be accomplished using an interdependence table or some other means to track the interdependencies. An interdependence table is used to identify the system functions (obtained from the preliminary aircraft architecture), whether during normal operation or by system malfunction, that have an effect on an aircraft failure condition.

A partial example interdependence table example is shown in Table B1. In this example table, aircraft functions and failure conditions are listed in the Columns 1 through 3. The functions and failure conditions included are those analyzed by the AFHA. (Columns may be added to include other information about these failure conditions including classifications, flight phases, etc.)

Row 1 of the example table identifies the names of each system on the aircraft. Row 2 is used to list system functions, and in the Table B1 example, the Flight Controls System is partially decomposed into system sub-functions.

Working through the table from left to right, starting at Column 1, the first aircraft-level function is “Decelerate the aircraft on the ground.” Columns 5 through 8 are marked (with an “X”) to indicate when a relationship exists between a system function and the aircraft failure condition.

SAENORM.COM : Click to view the full PDF of arp4761a

Table B1 - Interdependence table example

Aircraft Function	Aircraft Failure Cond. #	Aircraft Failure Condition	System	Wheel Brake System				…	Flight Control System							Engine		…
			System Function /Implementation	Control Normal Brake	Control Emergency Brake	Provide Anti-Skid	Provide Auto-Brake	…	Control Ailerons	Control Spoilers	Control Rudder	Control Elevator	Control Stabilizer	Control Flaps	Control Slats	Control Thrust Direction	Control Throttle	…
Decelerate aircraft on ground	3.2.3.L1	Inability to stop the aircraft within the available runway		X	X	X	X	…		X				X	X	X	X	…
Decelerate aircraft on ground	#	Inadvertent activation of deceleration function on the ground		X	X	…	X	…	…	X	…	…	…	…	…	X		…

Note: This table is only partial.

Particular attention should be paid to those system functions (Row 2) which do not contribute to the aircraft-level function, but whose functional failures may nonetheless contribute to the aircraft-level failure condition, e.g., the high-lift system (flaps/slats) does not contribute directly to the aircraft-level function “deceleration on ground”; however, a non-extension of the flaps—a system failure condition—may contribute to the failure condition due to an aircraft approach speed that will be higher than normal. The resulting table illustrates which systems need to be considered when evaluating the aircraft-level failure conditions.

If more information is known about the aircraft architecture, the Interdependence table may be augmented by adding columns with the names of subsystems and/or resource systems, or replacing the system functions—“control of pitch,” for example—with implementation details; in this case, “control elevator” and ”control stabilizer.”

An interdependence diagram may additionally be used to provide a pictorial representation for each aircraft-level function and the factors that affect it. The interdependence diagram may also identify crew actions, operational/environmental considerations that may be associated with the specific scenario or explore those system functions that may be sensitive to these factors.

Further exploration of the interdependent nature of these relationships occurs in the Combined Functional Failure Effects (CoFFE) Analysis (Section B.4) as well as in the system's SFHA. The CoFFE analysis helps to develop the preliminary FTA and failure conditions which may be allocated to systems.

B.4 FAILURE CONDITION EVALUATION

The aircraft-level failure conditions are evaluated to determine the contribution of the functional failures of the systems identified in the Interdependence Analysis described in B.3. The failure condition evaluation activity helps to derive safety and design requirements for the various systems in order to establish that the aircraft-level system architecture can reasonably be expected to meet the aircraft-level safety requirements.

The steps discussed below are used in evaluating the systems functional failure combinations that contribute to those aircraft failure conditions of interest:

a. Multifunction and Multisystem (MF&MS) Analysis: This analysis (B.4.1) consists of a traditional top-down safety analysis which includes considerations such as failure probability allocations to systems and may capture Independence Principles to be assessed by the common cause methods.

b. FDAL assignment: The FDALs are assigned for each top-level aircraft function based on its failure condition classification(s) and for system functions related to the aircraft-level failure condition(s) (B.4.2). This process may also identify Independence Principles to support FDAL assignments based on architectural considerations. (Additional FDALs for system functions are defined in the PSSAs for failure conditions arising in the SFHA; see Appendix D.)

c. The following supporting analyses (B.4.3) are intended to gather the pertinent systems failure modes and can help assure thoroughness of the PASA. These use the results of the Interdependence Analysis to more specifically identify the contribution of systems to an aircraft failure condition before allocating FDALs and building fault trees.

    1. Combined Functional Failure Effects Analysis: This analysis (B.4.3.1) maps combined failures (whether loss of function or a malfunction) of system functions to assess the impact on the aircraft and helps to model branches in an FTA.

    2. Common Resource Considerations: This activity (B.4.3.2) analyzes the integrated effect of the loss of resources or the erroneous outputs of those resources on the systems functions involved in the aircraft-level function. Common resource considerations analysis validates the AFHA, provides initial review of resources further evaluated in CEA, may capture Independence Principles to be assessed by the common cause methods, and provides early validation of the proposed architecture.

    3. The Common Cause Considerations (B.4.3.3) are comprised of three analyses: Common Mode Analysis (CMA), Zonal Safety Analysis (ZSA), and Particular Risk Analysis (PRA). These analyses may aid the identification of independence requirements.

    4. The Cascading Effects Analysis (B.4.3.4) examines the direct and indirect connections between the systems and evaluates the effects resulting from the propagation of an initiating condition (e.g., a single failure or a combination of failures). The CEA is useful for understanding the behaviors of highly integrated aircraft and system architectures.

    5. External Events and Survivability Considerations (B.4.3.5) covers external events and survivability considerations.

As the above analyses are conducted their success will likely depend on expectations about the systems or assumptions about their use or relationships. The capture of such requirements and assumptions are discussed in B.4.4.

SAENORM.COM : Click to view the full PDF of arp4761a

B.4.1 Multifunction and Multisystem (MF&MS) Analysis

A preliminary MF&MS analysis is performed against the proposed aircraft architecture to understand the systems that contribute to an aircraft-level failure condition and to propose safety requirements. The analysis can be done by developing an FTA (see Appendix G or by using an equivalent technique) for each aircraft-level failure condition under consideration. Aircraft failure conditions which are able to occur due to a failure (or event) of a single system function may have the safety objectives determined in that system's SFHA/PSSA and need not be determined in the PASA. In contrast, failure conditions in the AFHA that cannot be allocated to a single system (i.e., AND-gates between different systems or functions) require an analysis at the aircraft-level. In the latter case, determination of specific safety requirements should be made in the PASA. The MF&MS analysis of an aircraft-level failure condition will identify the following:

a. How system functional failures (including resource systems) combine to lead to the considered aircraft failure condition (whether system failures are drawn from the SFHAs or assumed initially before the SFHAs are available).

b. What probability allocations to systems are necessary in order to meet classification criteria of the aircraft-level failure condition (expressed in quantitative or qualitatively—e.g., remote—terms). Where an aircraft-level failure condition may be caused by any one of a number of systems (a top-level OR-gate in the fault tree), the failure condition should be analyzed within each system.

c. Whether functional and physical (i.e., segregation/separation) independence requirements are adequately identified for systems whose failures combine to produce an aircraft-level failure condition. Additional Independence Principles may be identified through an examination of the multifunction FTA.

d. Whether there are evident single failures of the proposed architecture that can result in Catastrophic failure conditions.

In accordance with the depth of analysis outlined in 3.8 of the main body, the MF&MS analysis may use an FTA or other suitable analysis to accomplish the aircraft-level failure condition evaluations.

The supporting analyses in B.4.3 can help identify the fault tree branches or other relationships in this MF&MS analysis, particularly where the systems contributing to the aircraft-level failure condition cross traditional functional boundaries.

B.4.2 Assignment of FDALs

ARP4754B/ED-79B Section 5.2 introduces a set of principles for assignment of development assurance level with guidelines for architectural considerations and Appendix P provides a step-by-step FDAL assignment process description.

The PASA performs the activity of assigning FDALs only to aircraft-level functions and system functions directly tied to the aircraft architecture. The assignment of FDALs for the remaining systems and subsystem functions and for IDALs for items within a system is covered in the PSSA (see Appendix D).

The FDAL assignment process (see Appendix P) provides the recommended FDAL assignment(s) considering functional independence assumptions used in the assignment. These independence assumptions are treated as Independence Principles to be captured as requirements to ensure they are evaluated in the CMA.

The other analyses in Section B.4 may be useful to see relationships when assigning FDALs, particularly when crossing traditional functional boundaries.

Following completion of the FDAL assignment process detailed in Appendix P, and the supporting analyses in B.4.3 for each functional failure, an FDAL allocation for each functional failure can be assigned. A means to compare this FDAL with FDALs from all functional failures assessed in the PASA containing the same function is important to ensure that the highest FDAL for the associated function(s) will be allocated to the system-level development processes. Advisory material may specify the FDAL or IDAL at a level different than identified using ARP4754B/ED-79B guidelines.

SAENORM.COM : Click to view the full PDF of arp4761a

B.4.3 Supporting Analyses

It is helpful to keep track of the various ways systems can fail to provide insights of how systems failures could lead to the top failure conditions when conducting the MF&MS analysis. The following analyses are intended to gather the pertinent systems failure modes and can help assure completeness of the MF&MS analysis (B.4.1) and assignment of FDALs (B.4.2).

B.4.3.1 Combined Functional Failure Effects (CoFFE) Analysis

Using the knowledge gained in developing the Interdependence Analysis, the systems that affect each aircraft-level function are further developed using a CoFFE analysis. This analysis provides insights regarding system-level functional failures in support of the MF&MS analysis by exploring the combined failures of system functions and their impact on a given aircraft failure condition. The CoFFE analysis answers the question: “What high-level system functional failures combine to result in aircraft-level failure condition?” This analysis can be accomplished by the following steps:

a. Select an aircraft failure condition.

b. Identify the functions for the systems listed in the Interdependence Analysis for that failure condition.

c. Identify the system functional failure effects: the ways in which the loss, degradation or malfunction of each of those system functions may contribute to the aircraft-level failure condition (may initially use preliminary or assumed failure conditions until SFHAs become available).

d. Analyze these system functional failure effects individually and in combination with one another. The analysis may need to consider different degrees or types of degradation or malfunction of one or more systems to resolve whether a given combination results in the top-level failure condition.

e. Assess the contribution of each system functional failure relative to the aircraft-level failure condition.

Rationale may be used to limit the scope of this analysis. For example, a system functional failure having the same effect at the aircraft-level need not be combined with other functional failures in the CoFFE analysis (i.e., combination ABC need not be listed if it has the same effect as combination AB).

The CoFFE analysis does not contain requirements or assumptions of independence but can indicate where Independence Principles may be identified and independence requirements proposed.

One method of performing this analysis is through a CoFFE table. The following example of this table, Table B2, considers an aircraft-level failure condition of being unable to stop the aircraft on the runway after landing. This example illustrates a partial CoFFE table developed to assess the interaction of systems for stopping the aircraft on the runway. While the table shows simple losses and partial losses, a more complete CoFFE table would also consider potential malfunctions. The rows below the header are individual analysis cases relative to the aircraft-level failure condition being examined. The analysis results are captured in a results column (Column 6) with an explicit determination of the applicability to the condition in the next column (Column 7).

SAENORM.COM : Click to view the full PDF of arp4761a

Table B2 case 26 illustrates a need for an Independence Principle to address common causes affecting both wheel braking function and high lift function.

Table B2 - Combined Functional Failure Effects (CoFFE) table example

1	2	3	4	5	6	7
Case #	**Wheel Braking**	**Aerodynamic Braking**	**Thrust Reversing**	**High Lifting**	**Stopping Capability Result**	**Does It Result in Failure Condition Event?**
1	Failed	Failed	Failed	Failed	High-speed overrun	Yes
…						
26	Failed	Operational	Operational	Degraded	High-speed overrun	Yes
27	Failed	Operational	Operational	Operational	Low-speed overrun	No
…						

If the CoFFE table is written before the SFHA becomes available, the assumed system failure conditions and aircraft-level effects in this table should be checked for consistency with the SFHAs.

The CoFFE analysis can be an important part of identifying combinations of systems that contribute to the MF&MS analysis and highlight areas where Independence Principles are needed. The CoFFE analysis is used to assure completeness of the top-down identification of failures leading to the aircraft-level failure condition (i.e., assure identification of prominent branches under the top event of the FTA).

B.4.3.2 Common Resource Considerations

In typical modern aircraft architectures, more than one aircraft or system-level functions share a resource. Examples of such common resources include:

- Air data.
- Air/ground logic.
- Computer and data networks.
- Electrical power.
- Electronics cooling.
- Hydraulic power.
- Inertial data.
- Navigation data.
- Pneumatics.

The systems that provide the resources are potential common causes to be evaluated against the Independence Principles. Using the knowledge gained in developing the Interdependence Analysis, the common resource systems that are involved in each aircraft-level function are assessed to answer the questions:

a. How could the use of common resources violate independence of systems contributing to aircraft-level failure condition?

b. Are interactions across the aircraft-level functions considered in the SFHAs of common resource systems?

This results in capturing additional requirements for common resource systems. It aims to identify common resource relationships that otherwise might not be identified in the Interdependence Analysis.

The Common Resource Analysis explores the broad effect these resources can have on the systems involved in the aircraft-level function and a given aircraft failure condition. Common resources are those used broadly throughout the aircraft by several systems. These resources must also meet the availability and integrity requirements and have appropriate DAL assignments based on both the interfacing systems they support as well as their own local failure condition effects. Depending on the breadth of their use by systems, an integrated approach may be necessary to identify all of the aircraft-level functional separation requirements. This Common Resource Analysis requires knowledge of the aircraft architecture in order to assess which systems are involved and how they may affect the top event under study. As the program matures and resource allocations are made, the Common Resource Analysis should be revisited to ensure it reflects the planned architecture. A shared resource system, such as an Integrated Modular Avionics (IMA) or electrical power, may have its failure conditions more fully examined in its own SFHA to account for other impacts beyond the aircraft-level functional failure conditions examined in PASA.

The Cascading Effects Analysis (Appendix O) and Common Mode Analysis (Appendix M) may be used to support the Common Resource Analysis when determining the multisystem and aircraft-level effects of resource systems' loss/malfunction.

SAENORM.COM : Click to view the full PDF of arp4761a

For each aircraft-level function and relevant aircraft-level failure condition, the Common Resource Analysis table can be used to capture the analysis by following the process steps:

a. Identify table columns with each system contributing to the aircraft-level failure condition (as identified in the interdependence diagram) in the top row.

b. Identify table rows with resource system losses/malfunctions in left-hand column.

c. Describe effect of loss/malfunction of resource on each system contributing to the aircraft-level failure condition within each cell of the table.

d. For each row, assess aircraft-level effect by combining individual system effects caused by loss/malfunction of resource.

e. Once the Common Resource Analysis tables are prepared for each aircraft-level function and every relevant aircraft-level failure condition, the matrices can be combined (laid side-by-side) and evaluated to consider unforeseen interactions across the aircraft-level functions.

This is an iterative process, particularly for common resources which will be used by a number of aircraft functions and the design may evolve for some time. In this preliminary stage, the specific resources and the functional allocations to them are likely to be immature; consequently, the goal is to capture safety requirements so that the eventual architectures satisfy the safety objectives. Eventually, the common resource contribution to aircraft-level hazards will be confirmed in the ASA and SSAs. In some cases, an additional analysis, simulation or test to validate the effects of failures may be employed to confirm PASA assumptions and/or refine requirements.

Table B3 presents a simplified Common Resource Analysis table example with simple cases of total losses or partial losses (e.g., one of two channels), but without exhaustive consideration of the specific malfunction cases included.

This simplified Common Resource Analysis table example is developed to assess the interaction of common resource systems for stopping the aircraft on the runway. A complete analysis should also include explanation where there is no effect in a cell of the table.

Analysis of the Common Resource Analysis table may lead to additional safety requirements to ensure that the resource system redundancy and allocation is adequate to support the aircraft functions.

The Common Resource Analysis table can be an important part of ensuring that conceptual design has adequately considered common resources in the independence of systems that contribute to aircraft-level failure conditions and can be a useful compilation for those resource systems as they document their respective SFHAs and PSSAs.

SAENORM.COM : Click to view the full PDF of arp4761a

Table B3 - Common Resource Analysis table example for failure condition "Loss of adequate deceleration means"

Common Resource	Common Resource Failure Mode	Wheel Brake	Spoiler	Thrust Reverser	Flap	Aircraft-Level Effect on Failure Condition (FC)
Hydraulic	Partial Loss	Loss of any one (inboard or outboard) pair	Loss of any one (inboard or outboard) pair	Loss of one (LH or RH) side	Loss of any one (inboard or outboard) pair	Deceleration degraded but FC not realized. See Hydraulic SFHA
	Total Loss	Loss of all pairs	Loss of all pairs	Loss of both	Loss of all pairs	Loss of all deceleration means
	Under Pressure	Reduced performance	Potential loss of one or more spoiler pairs	Reduced deployment speed	Reduced performance	Deceleration degraded but FC not realized. See Hydraulic SFHA
Electrical Bus	Partial Loss	No effect Loss of redundancy	No effect Loss of redundancy	No effect Loss of redundancy	No effect Loss of redundancy	Loss of redundancy. See Electrical SFHA
	Total Loss	Loss of all pairs	Loss of all pairs	Loss of both	Loss of all pairs	Loss of all deceleration means
Ground Detection Information (GDI)	Partial Loss	No effect. Consolidated GDI is used. Loss of redundancy	No effect. Consolidated GDI is used. Loss of redundancy	No effect. Consolidated GDI is used. Loss of redundancy	--	Loss of redundancy. See Landing Gear SFHA
	Total Loss	Loss of all pairs	Loss of all pairs	Loss of both	--	Loss of all deceleration means

B.4.3.3 Common Cause Considerations

Independence between functions, systems, or items may be required to satisfy the higher-level safety or regulatory requirements. Therefore, it is necessary to ensure that such independence exists, or that the lack of independence is acceptable.

Certain architecture features, such as redundancy, protection, and monitoring, may need independence between their elements to satisfy higher-level safety requirements and objectives such as "no single failure" requirements or independence requirements related to development assurance level assignment. This need for independence is identified as an Independence Principle. A common cause affecting multiple elements may compromise the ability to meet safety objectives. A common cause affecting both the protection and the protected function, or the monitoring elements and the monitored function may compromise the ability to meet safety objectives.

Independence Principles may be identified through an examination of the aircraft architecture and functions correlated to the functional failures in the FTA (see B.4.1) where the combined functional failures are modeled to meet the no single failure safety objective or related to DAL assignment (see B.4.2). Independence Principles may be identified by evaluating the combination of events either using the fault tree AND-gates, minimal cut sets, or Functional Failure Sets.

Independence Principles should be identified where redundancy between elements, protection or monitoring of one element by another of the architecture is necessary to meet the no single failure safety objective.

SAENORM.COM : Click to view the full PDF of arp4761a

Independence Principles are evaluated and other possible sources are assessed to define Independence requirements. Independence requirements are characteristics of an intended implementation where independence has been determined to be necessary. To ensure that these characteristics are implemented, independence requirements should be proposed to the development process. The resulting independence requirements are documented as an output of the PASA process, and managed per the applicable requirements management plans.

After having identified Independence Principles the architecture is assessed for acceptability with respect to these identified Independence Principles. Iterative communications between PASA and common cause analyses are conducted to support an architecture that satisfies the Independence Principles identified in the PASA. The PASA then interacts with the common cause methodology to generate independence requirements being able to satisfy the Independence Principles using information tailored for the type and scope of project involved. This flow with the common cause methods of CMA, PRA, and ZSA is depicted in Figure B2.

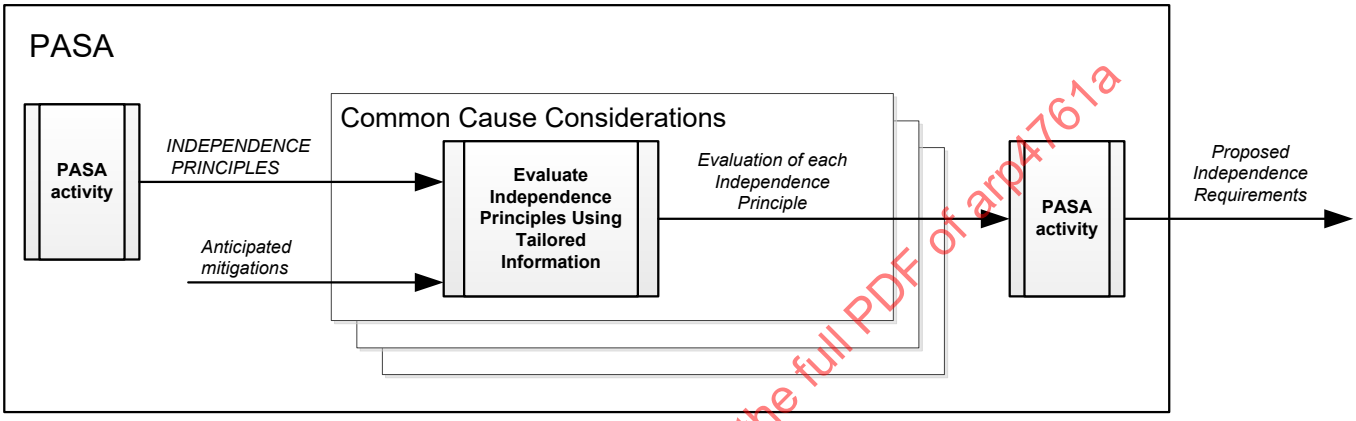


Figure B2 - Independence Principle flow through Common Cause Analyses

The resulting safety requirements are documented as an output of the PASA process, and managed per the applicable requirements management plans.

B.4.3.3.1 Aircraft-Level Common Mode Considerations

The CMA technique described in Appendix M can be used to support the generation of functional independence requirements and provides an example questionnaire (Table M1) which should be customized to meet the specific needs of the aircraft-level CMA. Factors to consider in the customization include the scope of the project (e.g., a new design or a changed design) and the maturity of the aircraft architecture definition (e.g., allocation of functions to systems, allocation of resources, spatial separation). The PASA uses the project tailored version of Table M1 as a starting point to evaluate the proposed aircraft architecture against the Independence Principles identified in the MF&MS analysis and the FDAL assignments discussed above.

Table M1 suggests other aircraft-level common causes pertinent to PASA such as installation design, and environmental considerations. Tailor or expand on the table as necessary to meet the needs of the project.

B.4.3.3.2 Zonal Considerations

The ZSA techniques (see Appendix K) may aid in determining whether the Independence Principles identified in the PASA and any identified physical segregation/separation requirements are adequately considered in the proposed physical installation.

Typically, ZSA may require design details that are not available during the PASA timeframe. Preliminary layout reviews would occur concurrently with the PASA process.

SAENORM.COM : Click to view the full PDF of arp4761a

B.4.3.3.3 Particular Risk Considerations

PRAs are safety activities managed from a global aircraft perspective. These analyses address particular physical hazards which could affect both aircraft structures and systems, thus impairing structural integrity of the aircraft, system safety margins, and intended independence. The PRA techniques (see Appendix L), could be used in conjunction with the MF&MS analysis to aid determining if the Independence Principles identified in the PASA and identified physical segregation/separation requirements are adequately considered in the proposed physical installation.

B.4.3.4 Cascading Effects Considerations

As dependencies between functions and systems are established (or are discovered) in the proposed aircraft architecture, the CEA techniques (see Appendix O) may be used to support the MF&MS analysis.

Typically, the CEA requires significant design detail regarding system to system interfaces that are not available during the PASA timeframe, but preliminary activity, including defining the cases to be analyzed by the CEA can be initiated.

B.4.3.5 External Events and Survivability Considerations

Events such as lightning strikes; bird strikes; fire; tire bursts; or ruptures of high energy equipment such as engine, APU, lithium batteries, and pressure vessels can pose aircraft-level risks affecting not only systems functions but also structural integrity. Some regulations (e.g., 14 CFR/CS 25.631, 25.863, and 25.963) specifically require considerations of external events. These events and proposed mitigation are assessed in PASA using PRA and ZSA techniques.

B.4.4 PASA Safety Requirements and Assumptions

Safety requirements and assumptions are captured as outputs of the PASA. Safety requirements are identified based on the results of the various PASA activities including developing safety requirements from Independence Principles generated within the PASA. Assumptions can be used to define safety requirements to support verification of the assumptions. These safety requirements would then be implemented by the development process.

B.4.4.1 Propose Safety Requirements

ARP4754B/ED-79B describes requirements capture (Section 5.3) and requirements validation (Section 5.4) provide guidance how to write requirements.

The PASA requires certain characteristics for the safety assessment to be valid. To ensure that these characteristics are implemented, safety requirements should be proposed to the development process to define the characteristics. Some requirements necessary for safety may already exist.

Each safety requirement should have a rationale that explains the need for the requirement and identifies the specific source (architecture, Independence Principle, fault tree, or similar analysis) that establishes the requirement need. This rationale should be as specific (e.g., fault tree gate) as possible to allow review of future changes for impact on safety and to aid in requirement validation activities. Sources of safety requirements may include:

a. Interdependence Analysis (B.3.0).

b. MF&MS analysis (B.4.1).

c. Failure probability budgets identified in PASA Fault Tree.

d. FDAL assignment (B.4.2).

e. Combined functional failure effects analysis (B.4.3.1).

f. Common resource considerations (B.4.3.2).

SAENORM.COM : Click to view the full PDF of arp4761a

g. Common cause considerations (B.4.3.3).

   1. CMA, particularly questionnaire for Independence Principles/requirements related to failures/errors and development errors (B.4.3.3.1).

   2. Zonal considerations (B.4.3.3.2).

   3. Particular-risk considerations (B.4.3.3.3).

h. Cascading effects considerations (B.4.3.4).

i. External events and survivability considerations (B.4.3.5).

These safety requirements specifically address the independence needed to achieve the safety objectives. Satisfying the independence requirement can be achieved by implementing features such as partitioning, monitoring, redundancy with appropriate development assurance, indication, isolation, separation, error tolerance, designed integrity, functional independence, or item independence.

B.4.4.2 PASA Assumptions

In addition to safety requirements, the PASA may depend on assumptions that cannot be confirmed when the PASA is being developed. These assumptions must be true for the PASA to be valid and should be captured as proposed requirements as discussed in B.4.4.1. Assumptions emerging in the PASA about crew actions or responses need to be captured and managed. This is needed to share such assumptions with the relevant stakeholders to enable the correct procedures to be captured in the applicable crew information and training.

B.5 PASA COMPLETION

The PASA determines whether the safety objectives associated with each individual aircraft-level failure condition can be satisfied and any necessary associated system requirements are derived. The aircraft architecture is assessed against the following points to confirm it can reasonably be expected to meet the aircraft-level safety objectives and requirements.

a. Have any of the inputs (aircraft architecture, requirements, assumptions, or failure conditions) changed requiring a further iteration of the PASA process?

b. Are all the failure conditions in the AFHA addressed by and allocated into either the PASA or to their respective SFHAs?

c. Have FDALs for the aircraft functions been assigned taking into account their respective failure conditions, with the rationales available, to validate these assignments for the proposed architecture?

d. Are the necessary independence requirements between functions identified for the aircraft/system architecture?

e. Are the safety requirements derived from this assessment identified for systems architecture and physical installation design?

f. Does the architecture introduce additional failure conditions not inherited from the AFHA, and if so, are the failure conditions identified herein consistent with the AFHA?

g. Are the failure conditions in PASA traceable to the AFHA to provide continuity of the analyses and visibility of any assumptions or relationships between these analyses? These PASA evaluations could identify additional failure conditions not initially apparent in the AFHA.

h. Has the potential for common errors between systems been assessed in the PASA process?

i. Are the system failure conditions considered in this PASA consistent with the SFHAs?

j. Have assumptions regarding crew actions or responses along with their safety context been compiled for coordination with relevant stakeholders?

SAENORM.COM : Click to view the full PDF of arp4761a

k. Are the interdependencies from the common resources analysis sufficiently identified to ensure the SFHA/PSSA takes them into consideration?

l. Have the derived requirements determined by the development process to have a potential safety impact been addressed by this safety assessment?

m. Have the results of development phase common cause methods been assessed?

The preliminary assessment may conclude that satisfying the safety requirements is not achievable by the proposed architecture. If so, the resulting safety requirements should be provided to the development process to guide adjustment of the architecture, requirements, or operations which will be re-evaluated through this preliminary assessment process until they are found to be achievable.

B.6 PASA OUTPUTS

The PASA process results provide sufficient analysis information to validate safety requirements derived from the PASA and may be used for some validation records. Once the PASA process confirms that the known aircraft architecture can reasonably be expected to meet the aircraft-level safety requirements, the outputs are captured.

B.6.1 Capturing PASA Outputs

The results of the PASA process should be documented in a manner to allow traceability of the steps outlined in Section B.1 in developing the PASA documentation. The documentation provides an archive of requirements derived by the PASA process and links from this information to specific system processes commencing with the PSSA. The outputs to be captured upon completion of the PASA include:

a. Corrections or additions of aircraft-level failure conditions (for the AFHA and/or SFHAs consideration).

b. Interdependence Analysis to support system-level assessments and common cause activities.

c. Summary of the FDAL assignment to the aircraft function and to system contributing functions with rationale identifying aircraft failure conditions.

d. Analysis used to evaluate the failure conditions (e.g., preliminary fault trees).

e. Key assumptions made in the evaluation of the failure conditions (e.g., flight crew procedures).

f. Proposed safety requirements for development of each system which may include:

    1. Architectural design constraints including separation, segregation and functional independence requirements (e.g., implementation in common resource system like IMA mitigated by independent backup function).

    2. Interface requirements.

    3. Initial failure probability allocations for contributing systems with associated qualitative and quantitative requirements.

    4. Other, such as survivability requirements.

The PASA is a series of evaluations that when conducted identify safety requirements based primarily on the inputs defined in Figure B1. During these evaluations, it may become apparent that some aircraft failure conditions have been identified where the associated system allocation combinations were not foreseen during the AFHA process. These failure conditions will be required to be directed back to the AFHA process or if more appropriate to the SFHA for assessment. This should result in a defined failure condition classification and may also identify further quantitative or qualitative requirements for that condition. These newly identified requirements would then re-enter the PASA process or continue on from the SFHA at the PSSA process level. In addition to identifying new key assumptions, the PASA evaluations may also confirm or correct assumptions captured during AFHA/SFHA process.

SAENORM.COM : Click to view the full PDF of arp4761a

The outputs of the PASA also become inputs to both the SFHA and PSSA processes. These outputs are used as inputs at the system-level analyses in a systematic manner similar to that of the AFHA and PASA processes, but for systems architecture to identify system-level safety requirements. While the PASA produces initial safety requirements for some systems, the full set of safety requirements is completed through an iterative flow through the SFHA and PSSA for their respective systems.

B.6.2 Relationship Between PASA and ASA

Once the aircraft-level safety requirements have been defined through the PASA process, and the maturity of implementing systems develops, the process converts to assessing the satisfaction of these aircraft-level safety requirements through the system-level PSSAs and SSAs. The results of these assessments are documented in the ASA, which may be updated incrementally as the aircraft architecture matures. Once the ASA process starts, PASA data may need to be maintained in the PASA records and/or in the aircraft development life cycle data (e.g., requirements and their rationale).

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX C - SYSTEM FUNCTIONAL HAZARD ASSESSMENT (SFHA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

C.1 INTRODUCTION 66
C.1.1 SFHA Process Overview 66

C.2 SFHA INPUTS 67
C.2.1 Review and Confirm System-Level Functions 67

C.3 IDENTIFY SYSTEM FAILURE CONDITIONS 68
C.3.1 Combined Failure Conditions 71

C.4 ASSESS SYSTEM FAILURE CONDITION EFFECTS 71

C.5 CLASSIFY FAILURE CONDITION BASED ON EFFECT SEVERITY 75

C.6 SFHA ASSUMPTIONS 76

C.7 SFHA OUTPUTS 77

C.8 FAILURE CONDITION PARAMETER AND EVENT CONSIDERATIONS 79
C.8.1 Crew Awareness 79
C.8.2 Flight Phases and Associated Operational Conditions 79
C.8.3 Operational Events 80
C.8.4 Environmental Conditions 81
C.8.5 Environmental Events 81

C.9 SFHA SUBSTANTIATION 81
C.9.1 SFHA Completeness 82
C.9.2 Failure Condition Effect Correctness 82
C.9.3 Failure Condition Classification Correctness 83
C.9.4 SFHA Reuse 83

Figure C1 SFHA activities 67

Table C1 System-level failure condition identification matrix example (pneumatic system) 70
Table C2 System-level failure condition effects matrix example (flight control system) 73
Table C3 Frequently used effect terms examples 74
Table C4 Failure condition severity classification examples 75
Table C5 SFHA format example data definitions 77
Table C6 Example SFHA capture table 78

SAENORM.COM : Click to view the full PDF of arp4761a

C.1 INTRODUCTION

The System Functional Hazard Assessment (SFHA) is a process that allows the identification and evaluation of potential hazards related to an aircraft system function regardless of the details of its implementation. It is performed at the beginning of system development process, re-evaluated anytime significant changes are made to the aircraft system, and used to establish the safety objectives for the systems functions to achieve a safe design.

System failure conditions are analyzed for their effect on the aircraft, crew and occupants to determine the associated severity classification. Crew awareness, flight phase, and environmental and operational conditions should be considered in the assessment.

The SFHA assesses system-level functions. The SFHA should assess both explicitly and implicitly defined functions identified in the system development information, though ideally all functions would be explicitly defined. The system functions and aircraft-level functions are linked by the aircraft-level architecture and the function allocation. The representation of the aircraft and system-level functions should be consistently passed from the AFHA/PASA to the SFHA.

The method described in this appendix describes one means of fulfilling the SFHA process.

The SFHA is dependent on how aircraft-level functions have been allocated to systems through the development process. SFHAs for the same system can be significantly different from one aircraft model to the next, depending on aircraft architecture and operation.

The SFHA evaluates the functions performed by the system, contributed to by the system, or affected by the system and determines the effects of failure conditions and their severity. The SFHA does not analyze potential causes for system failure or specific failure modes of equipment. For example, the effects of "loss of airspeed indication" are the same whether the design is mechanical, analog, or digital. The SFHA should not assume knowledge of the detailed design of the system, even if the proposed design is known at the time of SFHA development.

C.1.1 SFHA Process Overview

The SFHA process is a top-down method for identifying system failure conditions and assessing the severity of failure condition effects as shown in Figure C1.

The assessment process consists of the following activities:

a. Gather SFHA inputs.

b. Review and confirm that the system-level functions list includes all the functions the system is intended to perform per the system-level documentation, and those it may affect as determined by the PASA.

c. Determine the failure conditions associated with each system function.

d. Determine the effects of each failure condition considering flight phases, operational and environmental conditions and events, and crew awareness.

e. Assess and classify the severity of each failure condition's effects.

f. Capture SFHA assumptions.

SAENORM.COM : Click to view the full PDF of arp4761a

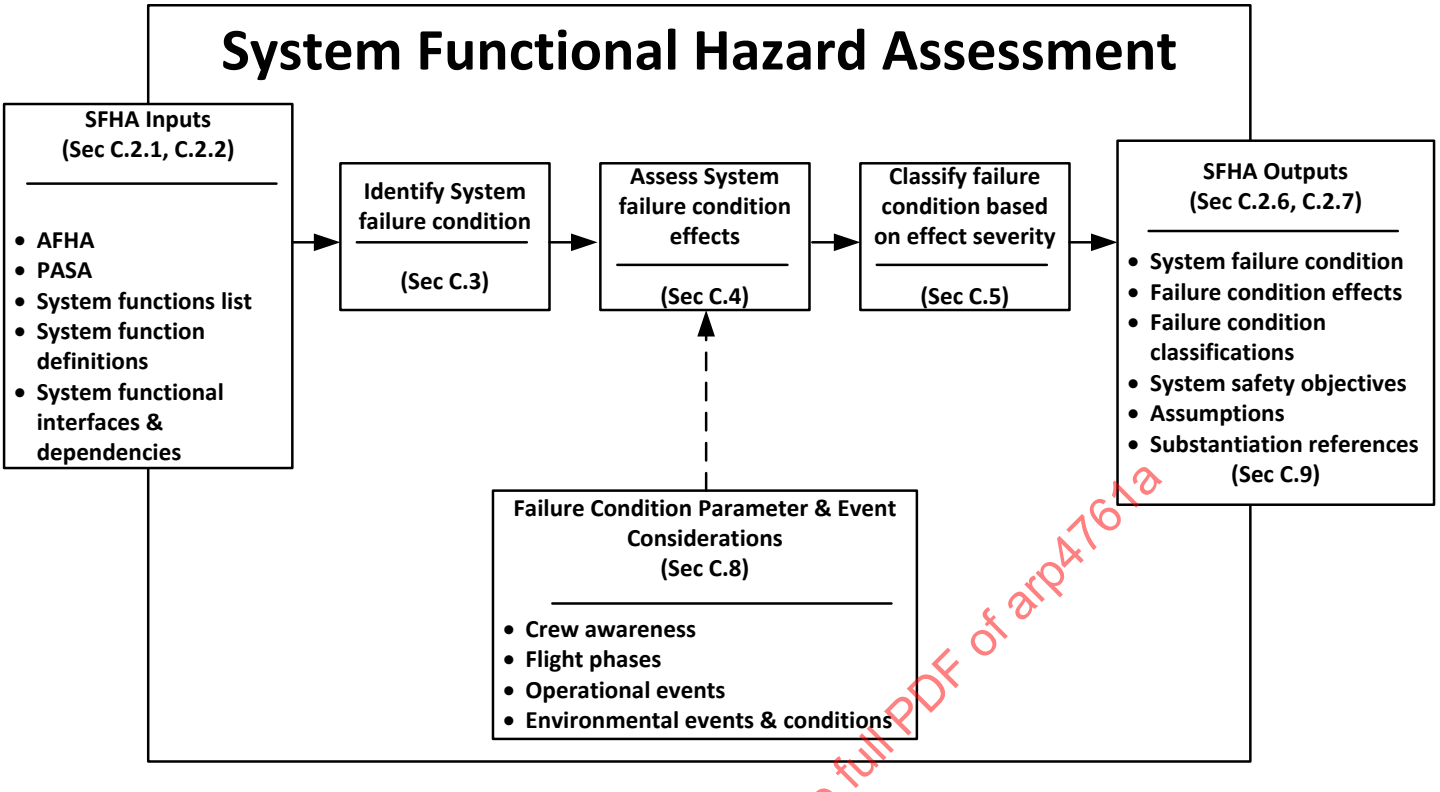


Figure C1 - SFHA activities

The SFHA process is very similar to the AFHA process. A separate SFHA should be performed for each system.

C.2 SFHA INPUTS

The following inputs are used to perform the SFHA:

a. All system-level functions explicitly or implicitly defined in the system development information.

b. External system interfaces and system dependencies from the development information.

c. Relationship between the functions of the system being assessed and the aircraft-level failure conditions obtained from the PASA.

d. The associated aircraft-level failure condition effects obtained from the AFHA where aircraft-level relationships have been identified.

e. The SFHA failure conditions and effects from “downstream” user systems where these user systems rely on outputs from the system under analysis.

C.2.1 Review and Confirm System-Level Functions

The SFHA does not define system functions. However, it requires a clear, explicit, and complete list of system functions as an input.

For the SFHA, the system functions should be described in terms of what the system is to accomplish, rather than the means envisioned to implement the system function. System functions may be the intended behaviors of the system, such as intended actions of the system, the prevention of undesirable system function actions, and the provision of outputs that are in turn used by other systems.

SAENORM.COM : Click to view the full PDF of arp4761a

System function definitions consider the relationship of the system to aircraft-level functions, the design objectives and the general nature and structure of the system. Consideration of detailed system architecture and implementation should be avoided, even when the intended design is known. For instance, the supply of electrical power by the aircraft power distribution system is a system-level function of the power distribution system. The power supply within equipment that receives power from the power distribution system is not a system-level function of that system.

An initial list of system functions is obtained from the system development information. The system development information may not list all the system functions explicitly, at the required level of detail or at an appropriate level of abstraction for the SFHA. The function list may be improved based on the relationship between the functions of the system being assessed and the aircraft-level failure conditions obtained from the PASA, or based on an understanding of the purpose of the system on the aircraft and the capabilities that must be accomplished by the system to achieve that purpose.

C.3 IDENTIFY SYSTEM FAILURE CONDITIONS

A failure condition is described by a statement that characterizes the nature of the failure or impairment of a function. The failure condition descriptions define the type of impairment, but not the causes of the failure condition. Knowledge of each function is necessary to properly hypothesize failure conditions which are correct in the context of the system function.

Failure conditions can be broadly categorized as the loss of a function or as a malfunction. Each function should be assessed and the potential for loss of the function and malfunction considered. In general, each system function will have at least one loss of function and one malfunction of interest.

Note that the dictionary definition of malfunction includes loss of function. However, loss of function is separated here to conform to certification advisory material.

Loss of function may be total or partial. Total loss of function is a condition where the function cannot be performed by any means. Partial losses of function are conditions where the function can still be performed but only at reduced effectiveness, with increased difficulty or by means other than the normal means used to accomplish it.

Malfunction is a condition where the operation of a function is different than intended excluding function loss. The aspect of the function which is incorrectly performed is described in the failure condition (e.g., erroneous, uncommanded action, misleading).

Examples of system-level loss of function failure conditions may include:

a. Loss of airspeed indication.

b. Loss of control of one elevator.

c. Loss of cabin pressurization control.

Examples of system-level malfunction failure conditions may include:

a. Erroneous altitude indication.

b. Erroneous movement of one aileron.

c. Excessive cabin air inflow.

The failure condition identification process should be strictly functional, and should avoid including failure conditions based on equipment or piece-part failure modes, which are properly addressed in an FTA or FMEA.

When the system contains multiple subsystems, loss of function of each subsystem should be identified as a partial loss of function failure condition for the system as a whole. The failure condition statements in these cases are still functional statements. Reference to equipment failure modes should be avoided. Only the highest level system definitions are referred to in the SFHA.

SAENORM.COM : Click to view the full PDF of arp4761a

Failure conditions may have vastly different effects depending on whether the crew are notified and are able to perform timely mitigating actions. Where crew reaction is relevant and the effects of the failure condition are not intrinsically evident to the crew, separate failure conditions may be created considering whether the crew is aware or unaware of the condition. Depending on the system function and failure condition, crew can refer to either the flight crew and/or cabin crew.

Examples of failure conditions involving crew awareness may include:

a. Loss of cabin pressurization control with crew awareness.

b. Loss of cabin pressurization control without crew awareness.

c. Loss of stall barrier with crew awareness.

d. Loss of stall barrier without crew awareness.

e. Loss of wing ice prevention or removal with crew awareness.

f. Loss of wing ice prevention or removal without crew awareness.

One method to consider all types of failure conditions for every function is to summarize them in a failure condition identification matrix. Other methods may be equally effective. Not all functions will have relevant failure conditions of all types.

Table C1 illustrates a failure condition identification matrix for the system-level. Additional system functions are added as additional rows. Distinct failure conditions with and without crew awareness, or additional types of malfunction may be added within the columns or as additional columns. Equipment failure modes should not be added. These examples illustrate a useful method when performing an SFHA. The examples are not a full assessment and do not represent the only way to perform failure condition identification.

The function names and failure conditions shown in Table C1, and their underlying assumptions, are an example only. Differences in aircraft functional allocation may generate different failure condition lists for similar systems on different aircraft. Functional breakdown, function and failure condition naming and organization may be different for different projects and developers.

SAENORM.COM : Click to view the full PDF of arp4761a

Table C1 - System-level failure condition identification matrix example (pneumatic system)

ID #	System Function	Loss of Function		Malfunction	
		Total Loss	Partial Loss	Uncommanded Action	Erroneous Parameter
1	Control pneumatic system				
1.1	Regulate bleed air sources				
1.1.1	Control bleed air pressure	1.1.1.T1 Total loss of bleed air pressure regulation	1.1.1.P1 Bleed system 1 (left) loss of bleed air pressure regulation 1.1.1.P2 Bleed system 2 (right) loss of bleed air pressure regulation	Not applicable (function normally active)	1.1.1.M1 Bleed system 1 (left) overpressure 1.1.1.M2 Bleed system 2 (right) overpressure Note: Low pressure conditions are considered loss of bleed supply
1.1.2	Control bleed air temperature	1.1.2.T1 Total loss of bleed air temperature regulation	1.1.2.P1 Bleed system 1 (left) loss of bleed air temperature regulation 1.1.2.P2 Bleed system 2 (right) loss of bleed air temperature regulation	Not applicable (function normally active)	1.1.2.M1 Single bleed system over temperature 1.1.2.M2 Both bleed systems over temperature 1.1.2.M3 Single bleed system under temperature 1.1.2.M4 Both bleed systems under temperature
1.2	Distribute bleed air to user systems				
1.2.1	Provide bleed air to air conditioning system	1.2.1.T1 Total loss of bleed air supply to air conditioning system without crew awareness 1.2.1.T2 Total loss of bleed air supply to air conditioning system with crew awareness	1.2.1.P1 Loss of bleed system 1 (left) air supply to air conditioning system 1.2.1.P2 Loss of bleed system 2 (right) air supply to air conditioning system	Not applicable (function normally active)	See “Control bleed air pressure” and “Control bleed air temperature”
1.2.2	Provide bleed air to anti-icing system	1.2.2.T1 Total loss of bleed air supply to anti-icing system without crew awareness 1.2.2.T2 Total loss of bleed air supply to anti-icing system with crew awareness	1.2.2.P1 Loss of bleed system 1 (left) air supply to anti-icing system 1.2.2.P2 Loss of bleed system 2 (right) air supply to anti-icing system	Not applicable (function normally active)	See “Control bleed air pressure” and “Control bleed air temperature”
1.2.3	Provide bleed air to engine air starters	1.2.3.T1 Total loss of bleed air supply to engine air starters	1.2.3.P1 Loss of bleed air supply to one engine air starter	1.2.3.M1 Uncommanded bleed air delivery to an engine air starter	See “Control bleed air pressure” and “Control bleed air temperature”

SAENORM.COM : Click to view the full PDF of arp4761a

C.3.1 Combined Failure Conditions

When a system includes multiple functions used together or interchangeably to accomplish a higher-level system or aircraft function, combined failure conditions of the related functions should be included in the SFHA. An example of related functions is “Navigation” and “Communication”, both of which might appear as system functions in an avionics SFHA. Since communication may be used as a means to determine position and track, and for collision avoidance (i.e., to navigate), these functions are related. The SFHA for this system would include the individual failure conditions “loss of all communication” and “loss of all navigation,” as well as a combined failure condition “loss of all communications and loss of all navigation.”

C.4 ASSESS SYSTEM FAILURE CONDITION EFFECTS

The SFHA next examines each failure condition and determines the effects on the aircraft, flight crew, and occupants (including cabin crew). The assessment of the effects begins with a narrative description of the consequences of the failure condition followed by a statement summarizing the failure condition’s overall impact. The use of standardized wording from the certification advisory material in the summary statements will aid in the failure condition classification process.

Flight phases are distinct time periods within an average flight duration as discussed in C.8.2. Failure condition effects may vary depending upon the flight phase at the time of failure condition occurrence. The failure condition effects may also be affected by other operating or environmental conditions. The failure condition effects assessment considers the most severe plausible effects during each flight phase or condition. Separate failure conditions may be needed to capture a range of effects.

The effects of a failure condition for any particular flight phase are all the expected effects during the flight when the failure condition occurs in that flight phase. This includes immediate effects and effects that would occur during subsequent flight phases due to the same failure condition. For example, the effects of a “loss of ground deceleration” failure condition during the cruise flight phase include the fact that ground deceleration will be unavailable for the subsequent landing.

The effects are described by a narrative and characterized with brief statements regarding the effect on aircraft, flight crew and occupant (including cabin crew) categories. Not all failure conditions may have effects in all categories or the effects of a failure condition in each category may not have the same severity.

a. “Effect on aircraft” refers to the ability of the aircraft to perform its functions and to the aircraft’s structural integrity. Aircraft effects are characterized by a statement evaluating the reduction in aircraft capability and safety margin caused by the failure condition.

b. “Effect on flight crew” refers to flight deck crew awareness and reaction to the failure condition, as well as any physiological effects on the crew members. Crew effects are characterized by a statement evaluating the increase in crew workload and the physiological effects on the crew caused by the failure condition.

c. “Effect on occupants excluding flight crew” refers to cabin crew or passenger discomfort, injury or fatalities. Occupant effects are characterized by a statement about occupant physical discomfort, distress, or injuries caused by the failure condition.

The failure condition effects in the SFHA should consider the failure condition’s full impact on the aircraft, including the indirect effects resulting from other systems that may be affected by the initial system failure condition. To determine the effects of failure conditions of systems that provide energy or information to multiple other systems, it is necessary to perform analysis of the aircraft systems as a whole. The methods used for this analysis may be different for different projects and developers.

For example, the effects assessment of the “Total loss of bleed air supply to air conditioning system” failure condition may include the loss of conditioned air to the cabin and subsequent depressurization and emergency descent—though these functions are not directly performed by the bleed air system.

The effects of a system-level failure condition that can directly cause aircraft-level failure conditions should include the full effects of those aircraft-level failure conditions.

SAENORM.COM : Click to view the full PDF of arp4761a

The effects of a system-level failure condition that combines with others to cause aircraft-level failure conditions should consider the reduction in aircraft safety margins and any partial degradation of the aircraft functions caused by the individual system-level failure condition alone.

It is important to avoid assuming a classification during the identification of failure effects, as the assessment process can be incomplete if there is excessive focus on preconceived outcomes for common failure conditions.

A matrix or table may be used to capture the evaluation of each failure condition, applicable flight phases, failure effects descriptions, and relevant environmental or operational conditions. The specific evaluation format for describing the effects is not critical, provided it is thorough.

Table C2 illustrates a possible failure condition effects capture matrix for system-level failure conditions. Similar tables would be constructed for each failure condition identified in each system. The effects described in this example are illustrative; actual effects vary with aircraft and system design.

In this method, one failure condition effects matrix is constructed for each failure condition. Additional depth can be added to the matrix by adding detail to the flight phases, such as separating “takeoff” into “takeoff below V1” and “takeoff above V1,” by adding special flight phases such as ETOPS cruise or CAT 2 approach, or by adding other operational or environmental events to the failure condition. Operational and environmental events are described further in Section C.8.

Initial assessment of the failure conditions should address the basic flight phases (taxi, takeoff, climb, cruise, descent, approach, and landing).

Each of the failure condition’s effects is qualitatively assessed. Usage of consistent assessment terminology facilitates consistency between failure condition descriptions.

Table C3 provides an example of frequently used assessment terms to summarize failure condition effects. Table C3 is based on certification guidance material applicable to transport category airplanes. A set of standard effect assessment terms should be obtained from the appropriate guidance material.

Knowledge of the system’s functional relationship to aircraft-level functions, and knowledge of system interfaces and the dependence of other systems on outputs provided by the system being analyzed are necessary to determine the overall effect of system-level failure conditions on the aircraft. In early stages of development, it may be necessary to make assumptions regarding these dependencies.

Operational or environmental events and conditions that could intensify the severity of failure condition effects should be considered. Where these events can substantially affect the severity of failure condition effects, separate failure conditions combining functional failures with the relevant operational or environmental events should be added to the SFHA. See Section C.8 for further details on external conditions and events.

SAENORM.COM : Click to view the full PDF of arp4761a

Table C2 - System-level failure condition effects matrix example (flight control system)

Function: 2 Control Aircraft Trajectory/2.2 Provide Lateral-Directional Stability and Control/2.2.1 Provide Roll Control			
Failure Condition: Aileron Surface Hardover			
Flight Phase	**Effect on Aircraft**	**Effect on Flight Crew**	**Effect on Occupants Excluding Flight Crew**
Taxi	The failed surface will move to its mechanical stop. No effect on aircraft safety for ground operation.	The crew will identify the failure by failure indications in the flight deck. The flight operation will be aborted. No significant effect on the crew.	No safety effect on occupants excluding flight crew.
Takeoff	The failed surface will move to its mechanical stop. The opposite aileron, roll spoilers, and rudder are available for lateral directional control. Excessive reduction in functional capability due to limited residual maneuvering authority.	The crew will identify the failure by noting a rapidly developing roll tendency. The crew will attempt to counter the failure by applying opposite roll control and yaw control. Pilot may be unable to prevent wing contact with the ground at low altitude.	Multiple severe injuries or fatalities are possible.
Climb Cruise Descent Approach	The failed surface will move to its mechanical stop. The opposite aileron, roll spoilers, and rudder are available for lateral directional control. Significant reduction in functional capability due to limited residual maneuvering authority.	The crew will identify the failure by noting a rapidly developing roll tendency. The crew will counter the failure by applying opposite roll control and yaw control. The crew will use roll trim to reduce control forces after level flight is restored. A significant increase in workload is required to counter the effects of the failure and complete the flight.	Non-fatal injuries or physical discomfort are possible due to rapid maneuvering.
Landing	The failed surface will move to its mechanical stop. The opposite aileron, roll spoilers, and rudder are available for lateral directional control. Excessive reduction in functional capability due to limited residual maneuvering authority.	The crew will identify the failure by noting a rapidly developing roll tendency. The crew will attempt to counter the failure by applying opposite roll control and yaw control. Pilot may be unable to prevent wing contact with the ground at low altitude.	Multiple severe injuries or fatalities are possible.

SAENORM.COM : Click to view the full PDF of arp4761a

Table C3 - Frequently used effect terms examples

Effect on Aircraft	Effect on Flight Crew	Effect on Occupants (Including Cabin Crew, Excluding Flight Crew)
Loss of aircraft	Crew unable to accomplish required tasks, or Required crew strength or skill in excess of crew capability, or Crew incapacitation, or Crew fatalities	Multiple occupant fatalities
Large reduction in aircraft functional capability or safety margin	Excessive crew workload increase, or Crew unable to fully accomplish required tasks, or Crew physical distress	Small number of occupant fatalities or severe injuries not including flight crew
Significantly reduced aircraft functional capability or safety margin	Significant crew workload increase, or Conditions impairing crew efficiency, or Crew physical discomfort	Occupant physical distress or non-fatal injuries
Slightly reduced aircraft functional capability or safety margin	Slight crew workload increase	Occupant physical discomfort
No effect on aircraft functional capability or safety margin	No effect on crew workload or physiology	No effect on occupant physiology

SAENORM.COM : Click to view the full PDF of arp4761a

C.5 CLASSIFY FAILURE CONDITION BASED ON EFFECT SEVERITY

When the identification and summary of all failure condition effects is complete, the failure condition classification activity can begin. The severity classification is determined using the most severe integrated effects associated with a failure condition.

A single classification for the failure condition is the worst-case effect in any flight phase or separate classifications may be determined for each flight phase, based on the integrated worst-case effects on the aircraft, crew, and occupants effects categories for each flight phase.

The effects of system-level failure conditions that contribute to aircraft-level failure conditions, as identified by the PASA process, should be compared to the AFHA. The effects and classifications in the AFHA and SFHAs should reinforce each other, and conflicts between them should be evaluated and rationalized. If the system-level failure condition directly causes the aircraft-level failure condition, the severity classification will be the same. If the system-level failure condition is only a contributor to the aircraft-level condition, it may have less severe consequences and a lower classification.

The summary of effects from Section C.4 are used to classify each failure condition using the appropriate certification guidance material. Table C4 provides an example of such a reference based on certification guidance material applicable to transport category aircraft. The classifications used are: Catastrophic, Hazardous, Major, Minor and No Safety Effect. Determination of the severity classification is direct if the qualitative assessment of the effects is consistently performed and the summaries clearly stated.

SAENORM.COM : Click to view the full PDF of arp4761a

Table C4 - Failure condition severity classification examples

Effect on Aircraft	Effect on Flight Crew	Effect on Occupants (Including Cabin Crew, Excluding Flight Crew)	Classification
Loss of aircraft	Crew unable to accomplish required tasks, or Required crew strength or skill in excess of crew capability, or Crew incapacitation, or Crew fatalities	Multiple occupant fatalities	Catastrophic
Large reduction in aircraft functional capability or safety margin	Excessive crew workload increase, or Crew unable to fully accomplish required tasks, or Crew physical distress	Small number of occupant fatalities or severe injuries not including flight crew	Hazardous
Significantly reduced aircraft functional capability or safety margin	Significant crew workload increase, or Conditions impairing crew efficiency, or Crew physical discomfort	Occupant physical distress or non-fatal injuries	Major
Slightly reduced aircraft functional capability or safety margin	Slight crew workload increase	Occupant physical discomfort	Minor
No effect or aircraft functional capability or safety margin	No effect on crew workload or physiology	No effect on occupant physiology	No Safety Effect

For many functions, published certification guidance material can be used as a reference for the qualitative categorization of failure effects and severity classification. Certification guidance may include a brief statement describing the failure

condition and applying a severity classification directly, or may describe certain types of effects which are considered unsafe conditions. This data can be used as reference points to classify similar failure conditions.

C.6 SFHA ASSUMPTIONS

In some cases, there may be information required to perform the SFHA that is not yet available or is subject to change. For example, details about the aircraft's handling and performance, operational and environmental envelope, functional integration between systems, crew awareness features, and crew operating procedures may not be fully available early in the development process.

Any assumptions made in the SFHA to support system function identification, failure condition derivation or effects determination can significantly affect the results of the assessment and should be documented. The assumptions related to airframe capability, operational and environmental limits are returned to the aircraft-level for confirmation, while assumptions about the capabilities of other systems and the functional interfaces between systems are passed to those other systems for confirmation.

As an example of this situation, an SFHA for the pressurization control system may assume that the aircraft is capable of an emergency descent from maximum cruise altitude within a certain time limit. This assumption may affect the aircraft design parameters. Insufficient descent capability could limit the maximum altitude at which the aircraft may operate.

Any assumptions made in the SFHA evaluation will be tracked as part of the development process activities.

SAENORM.COM : Click to view the full PDF of arp4761a

C.7 SFHA OUTPUTS

The output of the SFHA process is documentation containing:

a. Reference to the list of system functions and any supporting material needed to aid the understanding of their scope and purpose.

b. The detailed SFHA worksheet, containing all the identified failure conditions, their effects during each flight phase, and their resulting severity classifications.

c. The list of assumptions used in identifying system functions, identifying failure conditions, determining failure condition effects, and determining severity classifications.

Table C5 provides the definition of the data fields for an example SFHA worksheet. Table C6 provides an example of a detailed SFHA results worksheet.

Table C5 - SFHA format example data definitions

Column	Table Entry	Entry Definition
--	System Function	The function being analyzed. See Section C.2.
1	ID No	Unique numbering system for organization, tracking, and traceability.
2	Failure Condition	Description of the failed state of the function. See Section C.3.
3	Flight Phase	List the applicable aircraft operational phases for this failure condition. See Section C.4.
4	Effect of Failure Condition on Aircraft, Crew, Occupants	Description of the failure condition effects on the aircraft, crew and occupants. Sufficient detail should be provided to understand the failure scenario and conclude the severity classification based on the captured effects. Separate effects statements and classifications may be provided for each flight phase or a single generalized effect and worst-case classification provided for the failure condition. See Section C.4.
5	Severity Classification	Catastrophic, Hazardous, Major, Minor, or No Safety Effect as defined in applicable certification guidance material. See Section C.5.
6	Assumptions, Comments, Rationale, or Reference to Supporting Material	Data supporting the determination of effects and classification of the failure condition, including any applicable guideline material. See Sections C.6 and C.9.

SAENORM.COM : Click to view the full PDF of arp4761a

Table C6 - Example SFHA capture table

1	2	3	4	5	6
ID No.	**Failure Condition**	**Flight Phase**	**Effects of Failure Condition on Aircraft, Crew, Occupants**	**Severity Classification**	**Assumptions, Comments, Rationale or Reference to Supporting Material**
System: (OXS) Oxygen system					
Function: (OXS.1) Provide supplemental oxygen to crew					
OXS.1.L1	Loss of supplemental oxygen to crew without crew awareness	Takeoff Climb Cruise Descent	Aircraft: Significant decrease in safety margins due to the loss of backup means of providing a breathable atmosphere. Crew: Unaware of the condition, the crew will proceed normally with the flight. The crew will detect the condition during pre-flight checks on the subsequent flight. No effect on flight crew workload. Occupants: No effect.	Major	FAR/CS 25.1441(d): “Oxygen equipment and supply” FAR/CS 25.1443(c)(2): “Minimum mass flow of supplemented oxygen” AC 25-20 (6)(e)&(7): “Pressurized Ventilation and Oxygen System Assessment for Subsonic Flight Including High Altitude Operations” EASA Certification Review Item: “Airworthiness Standards for Subsonic Transport Aeroplanes to be operated above 41,000 ft”
		On ground Approach Landing	Aircraft: Supplemental oxygen is not available for the crew. No indication or warning is provided. No effect on safety margins due to low altitude. Crew: Unaware of the condition, the crew will proceed normally with the approach and landing. The crew will detect the condition during pre-flight checks on the subsequent flight. No effect on flight crew workload. Occupants: No effect.	No Safety Effect	

SAENORM.COM : Click to view the full PDF of arp4761a

C.8 FAILURE CONDITION PARAMETER AND EVENT CONSIDERATIONS

The effects of each failure condition are determined by constructing a scenario narrating its expected outcome. The failure effect scenario description includes immediate effects due to the failure condition and subsequent resulting effects due to the same failure condition. The failure effect scenario may also include events occurring concurrently with the failure condition under evaluation. This scenario includes the parameters at the moment the failure occurs. The events may intensify or mitigate the effects of the failure condition, or affect the crew's ability to recognize and correctly react to the failure condition situation.

In this context the term "parameter" is used for factors that are always present and vary in quantity or intensity (e.g., aircraft weight, aircraft speed) and for factors that may be present or absent but are commonly encountered (e.g., clouds obscuring vision, icing conditions). The term "event" is used for factors that occur at a distinct time and place and that are not regularly encountered (e.g., windshear).

Evaluating the influence of parameters and events on the failure conditions is part of the SFHA process. These factors need to be carefully considered as they are significant in some instances and may be irrelevant in others. For example, a wet runway is a significant factor when evaluating failure conditions associated with friction-based deceleration features, but is not significant when evaluating failure conditions related to environmental control of the cabin. Failure condition effects should consider that the failure condition can occur at any moment and under any condition encountered in the operating envelope of the aircraft. The failure condition effects should account for the failure effects over the range of the operating envelope and the analyst may separate the failure effects if they differ across the envelope.

Evaluating failure effects for each flight phase as described in Section C.4 provides a structure that facilitates addressing the influence of the various operational and environmental factors where appropriate. Generally, each flight phase will provide an expected value or a range of values for most operating conditions (e.g., the flight phase "landing" limits aircraft weight and speed to values expected during that part of the flight).

The intended operating conditions of the aircraft define the boundaries for many of these factors. For example, an aircraft intended to operate at altitudes above 25000 feet will consider the effects of high altitude exposure when evaluating the effects of related failure conditions during the climb, cruise and descent flight phases. These factors should include consideration at their most severe limit within the approved flight envelope.

C.8.1 through C.8.5 provide a method to address operational and environmental parameters; however, other methods may be equally effective.

C.8.1 Crew Awareness

Whenever the failure effect can be significantly influenced by the crew, separate failure conditions should be created and assessed, which consider the crew being either aware or unaware of the failure condition.

For failure conditions with crew awareness (i.e., which have an associated alert or are evident), the description of effects on the crew should capture how the crew becomes aware of the failure condition, how the crew is assumed to act in response to it, and the result of the expected crew action. In some cases, it may be necessary to substantiate crew identification and reaction.

For failure conditions without crew awareness (i.e., which neither have an associated alert nor are evident), it should be assumed that the crew will continue to perform their duties normally, which may affect the severity of the failure condition effects (i.e., crew will not take any action regarding the failure condition).

C.8.2 Flight Phases and Associated Operational Conditions

The flight profiles the aircraft is expected to perform should be obtained, along with the corresponding list of flight phases. Certain aircraft perform only or mostly one type of flight profile (e.g., airliners perform transport flight profile), while others may perform several distinct types of profiles (e.g., some rotorcraft may perform transport, search and rescue, and other types of profiles). A flight phase is a distinct period within a flight, generally associated to the tasks being accomplished by the aircraft and its flight crew. As a minimum for a transport category flight profile, taxi, takeoff, climb, cruise, descent, approach, and landing should be considered.

SAENORM.COM : Click to view the full PDF of arp4761a

The identified set of normal flight and ground operation phases should be applied throughout the entire assessment. A more detailed breakdown of the typical flight phases may be used where relevant distinctions in failure effects exist within the basic flight phases (e.g., to differentiate severity or assumptions). Since failures can occur at any time, all normal flight phases should be considered for all failure conditions to ensure completeness.

Operational conditions, such as aircraft weight, speed, and altitude, may be directly related to the various phases of flight. For each flight phase, operational conditions should be considered throughout the approved flight envelope.

Specialized operational phases may also be treated as flight phases. In general, a specialized flight phase should be considered when:

a. The specialized flight phase is deliberately initiated.

b. The specialized flight phase persists for a measurable duration.

c. The duration of specialized flight phase can be determined as a fraction of a mission profile.

d. A particular aircraft can be expected to experience the specialized flight phase multiple times during its service life.

Specialized flight phases should be systematically considered when evaluating all functions, though when the effects of a failure condition are not affected by the special flight phase, it can be considered not applicable. Some examples of conditions that can be considered specialized flight phases include go-around, holding, and steep approach.

C.8.3 Operational Events

Distinct occurrences and flight operations which are only performed as a response to specific occurrences or failures may be considered operational events. In general, an occurrence or flight operation should be assessed as an operating event when:

a. The occurrence or flight operation occurs at a distinct time.

b. The occurrences or flight operations have a known statistical probability, fleet wide or industry wide rate of occurrence.

c. A particular aircraft is not expected to frequently experience the occurrence or flight operation during its service life, or may not experience it at all.

These operational events should be systematically considered when evaluating all functions, though they should only be applied to relevant failure conditions. Some examples of occurrences and flight operations that can be considered operational events include: Rejected Takeoff (RTO), in-flight diversion, baggage compartment fire, and smoke in the flight deck or cabin.

Operational events should be added to the failure condition statement, creating a new combined failure condition. When considering the combination, it is important to ensure that the operational event is independent from the original failure condition. Examples of combined failure statements at the system-level may include:

a. Loss of baggage compartment smoke detection and baggage compartment fire.

b. Loss of cabin pressure dump capability and smoke in flight deck.

Where operational events affect the severity of the failure condition, the analysis should consider two scenarios: the failure condition without the operational event and the failure condition combined with the operational event. Both scenarios should be assessed for all identified flight phases.

SAENORM.COM : Click to view the full PDF of arp4761a

C.8.4 Environmental Conditions

Worst-case environmental conditions within the approved aircraft operating envelope should be considered to be present where relevant when evaluating the effects of failure conditions. These conditions are implicitly assumed and need not be specifically stated for every failure condition, though their influence should be described in the failure effects narrative when relevant. Examples of environmental conditions to be considered include:

a. Airfield temperature and altitude at or within the approved operating limits.

b. In-flight temperature and altitude at or within the approved operating limits.

c. Night time and clouds obscuring external vision, for aircraft approved for Instrument Flight Rules (IFR) operation.

d. Icing conditions, for aircraft approved for flight in known icing conditions.

e. Gusting and turbulence at or within limits.

It may be acceptable to add the environmental extreme explicitly to the failure condition. Where environmental extremes affect the severity of the failure condition, the analysis should consider two scenarios: the failure condition without the environmental extreme and the failure condition combined with the environmental extreme. Examples of failure conditions incorporating environmental extremes are:

a. Loss of yaw control and limit cross wind.

b. Loss of load alleviation function and limit gusting conditions.

Both scenarios should be assessed for all identified flight phases.

C.8.5 Environmental Events

Certain unusual and discrete environmental occurrences outside the approved operating envelope may be considered environmental events. Examples of environmental events include:

a. Windshear or microburst.

b. Iced runway.

c. Icing conditions for aircraft not approved for flight in known icing conditions.

Where environmental events affect the severity of the failure condition, the analysis should consider two scenarios: the failure condition without the environmental event and the failure condition combined with the environmental event. Both scenarios should be assessed for all identified flight phases.

Particular risks should not be added to SFHA failure conditions except where system functions exist specifically for the purpose of preventing or mitigating the effects of the particular risk (e.g., a windshear alerting system). For further details on particular risks, see Appendix L.

C.9 SFHA SUBSTANTIATION

Substantiating data for the SFHA should be collected, showing that:

a. The system-level functions have been identified.

b. The failure conditions have been identified for each system function.

c. The failure effects on the system, crew, and occupants are complete and correct for each failure condition occurring during each flight phase.

SAENORM.COM : Click to view the full PDF of arp4761a

d. The correct failure classification has been selected based on the failure effects.

e. The assumptions used to develop the assessment are confirmed and evidence is formally provided by the development process. Where an assumption is found to be incorrect, the SFHA should be updated accordingly.

Substantiation of the completeness and correctness of the SFHA requires documentation of the rationale and assumptions for all failure effects and classifications.

For those failure conditions with effects that are not clearly predictable or demonstrably similar to previous applications, additional supporting information, such as simulation results, analytical studies, laboratory test results, flight test results, or field data may be necessary to substantiate the effects and classification. This information may be available in existing documentation or may have to be obtained from dedicated activities.

While comparison with previous experience may be sufficient rationale for typical failure effects and classifications, if a project integrates functions in new or novel ways, the assessment of effects may require more extensive examination.

Documentation of supporting materials (e.g., analyses, studies, tests) used in determining the effects and classification of failure conditions should be preserved to substantiate the SFHA. When reusing SFHA content or substantiating by similarity, any applicable lessons learned acquired since the previous application should be incorporated.

C.9.1 SFHA Completeness

A peer review is recommended to ensure that the SFHA has addressed all identified failure conditions and their effects. Reviewers should be able to find evidence within the SFHA documentation that:

a. The system-level safety-related functions have been identified, and the functional decomposition is complete such that the lower-level system safety-related functions are sufficient to accomplish top-level system safety-related functions.

b. The failure conditions have been identified for each lower-level system safety function, including loss of the function and malfunction.

c. Where lower-level system functions are related, that combined failure conditions which lead to the loss or malfunction of a higher-level system function have been identified.

d. The effects of each failure condition have been determined for its occurrence during all defined flight phases, including any applicable special flight phases.

e. The influence of operating conditions, operational events, environmental conditions, and environmental events have been considered where appropriate.

f. Assumptions have been captured for subsequent confirmation.

C.9.2 Failure Condition Effect Correctness

There are multiple means to substantiate that the effects of each failure condition during each flight phase are correct. Different methods may be appropriate depending on the type of failure condition and the difficulty of assessing its consequences.

One or more of the following methods should be used to substantiate each failure condition’s effects:

a. Pilot and human factors evaluation: Failure conditions where crew reaction significantly influences the effects of the failure, should be evaluated by experienced pilots and human factors specialists. The means and timeliness of failure recognition, intuitive or procedural response and overall workload should be substantiated.

b. Engineering evaluation: Direct and indirect functional effects of the failure condition may be determined based on previous experience and knowledge of system of similar design and operational characteristics, on data and rationale obtained through Certification Authority and industry literature, and on analytical or simulation results. Certification Authorities and system manufacturers may retain senior engineers recognized for their expertise and experience who may be consulted for this purpose.

SAENORM.COM : Click to view the full PDF of arp4761a

c. Published historical data: Historic precedent or accident or incident narratives for similar occurrences can be used to determine the expected effects of the failure. Due to the fact that incidents or accidents are very specific occurrences, the analyst should ensure that the events in question are indeed representative of the failure condition.

d. Published guidance: Certification Authority provided guidance material may specify a severity classification for the failure condition. When such a classification is given, the effect on system, on flight crew, and on occupants excluding flight crew may be inferred. When guidance material is used as a reference to establish a severity classification, it is necessary to substantiate that the details of the particular application being considered are fully consistent with the scenario described in the guidance material. System function, operational, and environmental conditions should be shown not to increase the severity of the failure conditions.

e. Testing: Where necessary and practical, controlled testing may be performed to assist in the substantiation of failure effects. Equipment, system rig or system prototype testing may confirm effects of failure conditions on the system. Pilot in the loop testing on representative flight simulation platforms may be used to evaluate crew reaction, crew workload, or controllability aspects of a failure condition.

C.9.3 Failure Condition Classification Correctness

Confirmation of the correct severity classification consists of evaluating the known failure effects in relation to the qualitative severity scales associated with the applicable severity classifications and determining that the correct severity classification has been selected for each failure condition during each flight phase. This task can typically be accomplished by inspection of the SFHA worksheets.

Failure condition severities and requirements that are specified in system certification guidance material have usually been specified due to accident or incident experience, or collaborative expert experience and opinion. If the guidance material specifies a worst-case failure condition severity, there is likely no need to further assess effects unless the applicant desires to show justification that the worst-case effects implied by the guidance material are not applicable to their particular system.

C.9.4 SFHA Reuse

When assessing a system that is similar to a previous design, it may be possible to use the previous SFHA failure conditions and classifications. Use of previous SFHA content requires that the system installed on the new or modified aircraft be shown to be equivalent to the previous application in function, operation, environment, and in its relationship to other systems and to the aircraft-level functions.

Any gaps identified in previous analyses or other applicable lessons learned should be addressed.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX D - PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

D.1 INTRODUCTION 85
D.1.1 PSSA Process Overview 85

D.2 GATHER PSSA INPUT DATA 86
D.2.1 Failure Conditions and Classifications from SFHA 86
D.2.2 Requirements Input Data 86
D.2.3 Proposed System Architecture, Including System Interfaces 87

D.3 FAILURE CONDITION FUNCTIONAL MAPPING 87

D.4 PSSA FAILURE CONDITION EVALUATION 88
D.4.1 FDAL and IDAL Assignment 88
D.4.2 Evaluate Design Against Safety Requirements and Objectives 89
D.4.3 PSSA Safety Requirements and Assumptions 92

D.5 PSSA COMPLETION 94

D.6 GENERATE PSSA OUTPUTS 95
D.6.1 Capturing PSSA Process Data 95
D.6.2 Outputs to Lower-Level PSSA Process 95
D.6.3 Outputs to Higher-Level PSSA or PASA Process 95
D.6.4 Relationship Between PSSA and SSA 96

Figure D1 PSSA process 86

SAENORM.COM : Click to view the full PDF of arp4761a

D.1 INTRODUCTION

The Preliminary System Safety Assessment (PSSA) process is a systematic examination of a proposed system architecture which evaluates the failure conditions and associated safety objectives identified by the System Functional Hazard Assessment (SFHA) and safety requirements allocated from the Preliminary Aircraft Safety Assessment (PASA). Through the PSSA process, proposed safety requirements for the system, subsystem, and items may be generated to guide the architecture development as necessary to meet the safety objectives and requirements. The PSSA process is interactive and associated with the design definition. Just as the development process is iterative, the PSSA process is iterative. The PSSA is a continual process throughout the requirements capture and validation phase of the development cycle. Updates to the PSSA documentation may be necessary as the system architecture matures to ensure a complete set of PSSA/System Safety Assessment (SSA) data is available to support the aircraft certification.

NOTE: The process outlined in this appendix should be followed for any design changes occurring during the verification phase of development, but documentation could be included in the SSA output.

The PSSA process addresses failure conditions and classifications identified in the SFHA for the system being analyzed. In addition, the PSSA may also address safety requirements allocated to the system from applicable higher-level safety assessments e.g., probabilistic allocations, separation and isolation. The methods of analysis may be qualitative and/or quantitative.

There can be more than one level of PSSA performed based on roles and responsibilities at the system organization level (e.g., aircraft manufacturer, supplier). The various levels of PSSA support a single analysis performed on a system. The highest level PSSA is performed based on the SFHA in combination with safety requirements output from the PASA. Lower-level PSSAs (e.g., Line Replaceable Unit (LRU) level PSSAs) are performed based on requirements and failure conditions and classifications from higher-level safety assessments.

Throughout this appendix, reference is made to using Fault Tree Analysis (FTA). It should be understood by the reader that Dependence Diagrams (DD), Markov Analysis (MA), Model-Based Safety Analysis (MBSA), or other techniques may be selected to accomplish the same purpose, depending on the circumstances and the types of data desired.

D.1.1 PSSA Process Overview

The purpose of the PSSA is to determine whether the proposed architecture can reasonably be expected to meet the objectives based on the failure conditions and classifications from the SFHA, safety requirements from the PASA and any higher-level PSSAs. Additionally, if the PSSA finds that the safety objectives and requirements are not achievable for a proposed architecture, feedback should be provided to adjust the system architecture early in the development. This activity also generates safety requirements for the design and feeds assumptions made back to the higher level. This assessment is made in accordance with the following activities and detailed in the referenced sections.

a. Gather PSSA input data (Section D.2).

b. Define failure condition functional mapping (Section D.3).

c. Perform failure condition evaluation (Section D.4).

d. Determine if architecture can meet safety requirements and objectives (Section D.5).

e. Generate PSSA outputs (Section D.6).

Figure D1 provides an overview of the PSSA process.

SAENORM.COM : Click to view the full PDF of arp4761a

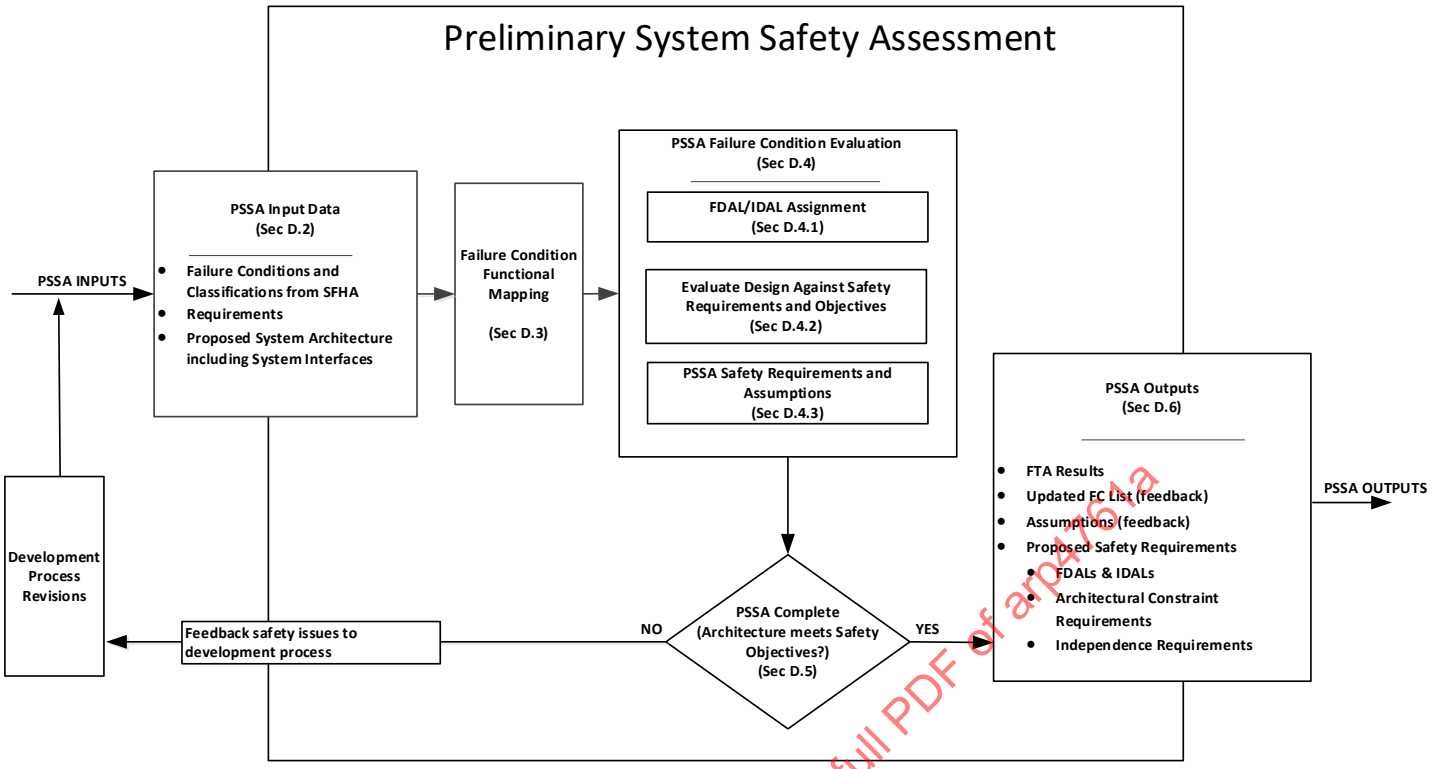


Figure D1 - PSSA process

D.2 GATHER PSSA INPUT DATA

The inputs outlined in this section constitute the minimum data set necessary for the safety analyst to perform the PSSA assessment.

a. Failure conditions and classifications from SFHA.

b. Requirements input data, including that from higher-level safety assessments.

c. Proposed system architecture, including system interfaces.

D.2.1 Failure Conditions and Classifications from SFHA

Allocated failure conditions and classifications from the SFHA pertaining to the function under analysis should be identified for evaluation in the PSSA. Safety objectives, which may be expressed in terms of numerical probabilities or no single failures influenced by regulations or company policies, are indicated by the failure condition classification in the SFHA. These safety objectives may be included in the SFHA or determined by the PSSA.

D.2.2 Requirements Input Data

Requirements input data includes safety requirements allocated from the PASA and, when applicable, higher-level PSSAs. These PASA or higher-level PSSA safety requirements provide additional allocations and constraints that may be required due to combinations of failures involving multiple systems contributing to the aircraft-level failure conditions. If these additional allocations and constraints are not provided to the PSSA, they would be assumptions as discussed in D.4.3.2.

SAENORM.COM : Click to view the full PDF of arp4761a

D.2.2.1 Certification Requirements

Certification requirements and regulatory guidance appropriate for the type of system under consideration should be included in the requirements input data.

D.2.2.2 Allocated FDAL

The Function Development Assurance Level (FDAL) allocation should be captured for the system. The FDAL allocation should include visibility to aircraft/system-level failure conditions and classifications to ensure that the FDAL/Item Development Assurance Level (IDAL) assignment process considers the aircraft/system-level failure condition and classification data. As part of the FDAL allocation from the higher level, it is important to understand if the FDAL has been assigned based on independence identified for the purposes of FDAL allocation at the system-level. Appendix P highlights that the aircraft-level failure condition classification be considered when assigning FDALs and IDALs based on independence characteristics of the system.

D.2.2.3 Allocated Probability Budget

When two or more systems contribute to a failure condition, each system may have an allocated probability budget. The system under evaluation needs to know its allocated probability budget(s) for its respective failures.

D.2.2.4 Architecture Requirements

Any specific architecture requirements including constraints needed at the higher level to support the PASA or higher-level PSSAs should be included in the assessment. These architectural requirements may be driven by aircraft (or higher system) level common cause method evaluations. The PSSA will receive these as independence requirements (e.g., no single failure shall result in current draw above specified tolerance on both power inputs).

D.2.2.5 Operational Requirements

Expected average aircraft usage parameters for the fleet type (e.g., average flight profile, flight phase constraints, ETOPS, flight lengths, power on times, check intervals) should be included in the inputs to the assessment.

D.2.3 Proposed System Architecture, Including System Interfaces

A conceptual representation of the proposed system architecture from the system development process is essential to allow evaluation of the architecture's ability to meet the requirements and the objectives of the failure condition classifications from the SFHA. This system architecture definition should include a list of system equipment, functions of each equipment, and their interrelationships (e.g., data and control flow).

The definition of how the system interfaces with the external systems is needed to complete the analysis of the proposed architecture. This definition should include FDALs and IDALs, allocated probabilities, aircraft parameters that are used as exposure times, reversionary modes (alternate operating modes with reduced capability), and independence requirements for interfacing systems (power/data sources/selection devices).

As the design matures, a more detailed representation of the architecture may be input to the process.

D.3 FAILURE CONDITION FUNCTIONAL MAPPING

The goal of failure condition functional mapping is to obtain a better understanding of the system and the specific functions causing or contributing to a given failure condition to be analyzed prior to commencement of the failure condition evaluation. Along with descriptive documentation based on design data, functional mapping also equips the safety analyst with the knowledge necessary to confirm that the architecture to be evaluated can reasonably be expected to satisfy the requirements for the failure condition severity classifications from the SFHA.

SAENORM.COM : Click to view the full PDF of arp4761a

The mapping of architectural features/functions to the failure conditions under analysis should identify and assess the interdependencies of the system/equipment functions that affect each failure condition. The functional mapping is performed using the following steps:

a. Identify the architectural features, functions, or items of the system/equipment under analysis that affect each failure condition accounting for any hierarchical relationships between systems/equipment, functions, and items.

b. Identify characteristics of the architecture under analysis, such as mitigation strategies, monitors, data flow, etc., that impact the analysis of each failure condition.

c. Identify the proposed method (qualitative and/or quantitative) of analyzing the failure condition.

During this mapping, tracking the functions that do not map to existing failure conditions should also be maintained for consideration for future failure condition updates to the SFHA and/or identifying new requirements (e.g., separation requirements and operational requirements). Consideration as to whether the functions being mapped contain common resources (e.g., power, processor) should be noted and accounted for during the mapping exercise. This may directly influence FDAL and IDAL assignments, probability allocations and the need for independence identified in the analyses.

D.4 PSSA FAILURE CONDITION EVALUATION

The proposed architecture should be evaluated for each identified failure condition from the SFHA. The main body of this document provides guidance on depth of analysis depending on failure condition classification (see main body 3.8). The PSSA failure condition evaluation activities include:

a. Assign FDAL and IDAL based on the system failure conditions and classifications. System architecture may also be considered when assignment based on architectural attributes is desired.

b. Evaluate design against safety requirements and objectives—preliminary analysis based on the proposed architecture being evaluated in the PSSA.

c. Identify requirements and assumptions based on FDAL and IDAL, FTA (e.g., AND-gates), FMEA/FMES, and common cause considerations.

The initial evaluation is made at a time in the design process when the design details may not yet be fully available. Consequently, the PSSA failure condition evaluation may need to rely in part on engineering judgment or on in-service experience with similar designs. In addition to internal sources, this could include inputs from the OEM, other suppliers, and certification authorities. This use of engineering judgment or in-service experience should be documented with rationale. This process is of an iterative nature and becomes more complete during the evolution of the design.

D.4.1 FDAL and IDAL Assignment

The FDAL and IDAL assignment process is shown in Appendix P. The FDAL assignment is output from the PASA and/or higher-level PSSAs, and failure conditions and classifications originate in the SFHA. The output of the FDAL assignment process is a list of the functions, their respective FDALs, and the Functional Failure Sets (FFSs). Also, the IDAL assignment for the items that implement the function is made based on the architecture and the respective FDAL. All failure conditions from the SFHA that can be impacted by a function or item should be considered when assigning the FDAL and IDAL. The output of the IDAL assignment process is a list of the items involved with the functions, their respective IDALs, and the FFSs. The identification of Independence Principles associated with the FFSs is described in D.4.2.2.1. For legacy systems and items that were developed prior to the FDAL and IDAL assignment per ARP4754B/ED-79B, see P.4.3.1.

NOTE: Although protection levels for HIRF (AC 20-158A) and lightning (AC 20-155A) have similar safety considerations, such protection levels should not be confused with FDALs or IDALs. The HIRF and lightning protection levels drive hardening to protect from those external events in-service and also drive environmental test levels. By comparison, FDALs and IDALs drive the rigor of the development assurance activities to address potential errors in requirements, design and implementation occurring during development. This ARP does not cover assignment of HIRF and lightning protection levels.

SAENORM.COM : Click to view the full PDF of arp4761a

D.4.1.1 FDAL/IDAL Assignment Consideration(s)

Where FDAL or IDAL assignment is applied to multiple member FFSs, the highest level FDAL assignment for the function (from the PASA or higher-level PSSA) should be considered. The FDAL or IDAL assigned to each member should satisfy ARP4754B/ED-79B Table 3, Note 2. Further details can be found in Sections P.3 and P.4. Advisory material may specify the FDAL or IDAL at a level different than identified using ARP4754B/ED-79B guidelines.

When a lower FDAL function interfaces with a higher FDAL function, the impact on the higher FDAL function needs to be assessed for the loss of or erroneous output from the lower FDAL function or item to ensure it cannot impact the higher FDAL function. For example, Level C functions may output to a Level A function so the impact on the Level A function needs to be assessed for the loss of or erroneous output from the Level C function or item to rationalize such use by the Level A function.

For each failure condition, the contribution of potential error within function and item development should be evaluated to ensure that an item receives the correct IDAL in accordance with the most stringent assignment after evaluating the item's contribution in all failure conditions. Because an item can contribute in many failure conditions, to streamline the analysis, one may be able to limit the number of failure conditions to be analyzed taking advantage of certain design decisions. For example, if the decision is to set the minimum IDAL to level C regardless of lower hazard classifications, then one may be able to limit the evaluation to the failure conditions that are Hazardous and more severe.

D.4.2 Evaluate Design Against Safety Requirements and Objectives

The design evaluation is performed to show how physical failures in the system can contribute to the system's failure conditions and allocated safety requirements. The evaluation is based on the proposed system architecture, including architecture mitigations (such as mitigation strategies, monitors and data flow) and its functional mapping to the failure conditions identified. It may be possible when maintaining a conservative approach (e.g., all failure modes of the equipment or hardware item are included in the failure rate) to model multiple failure conditions using a single fault tree when functional mapping is similar.

The evaluation done at this stage should:

a. Construct a failure model using FTA.

b. Identify Independence Principles.

NOTE: Major failure conditions may be evaluated using the techniques in Section D.4 as necessary. See 3.8 in the main body of this document for further information.

Where the SFHA includes crew awareness to limit the severity of a failure condition, features necessary for crew awareness should be identified as safety requirements or provided to a higher level as assumptions by the PSSA process.

D.4.2.1 Construct and Analyze a Fault Tree

Once the inputs listed in Section D.2 are of a maturity that can support a functional mapping (discussed in Section D.3) of the proposed architecture, an analysis model of failures should be constructed using a fault tree (or equivalent method) to show how failures combine to lead to the considered failure condition. See appropriate appendix for details on how to use the method chosen for modeling (i.e., FTA, DD, Markov, MBSA etc.).

Analyze the fault tree to ensure that no single physical failure of the proposed architecture can result in Catastrophic failure conditions. An approach would be to evaluate the minimal cut set(s) of the fault tree for single point failure.

Determine if safety objectives (see appropriate certification guidance material for mapping of qualitative failure condition severities to allowable quantitative probability values) associated with the failure conditions and quantitative safety requirements can be met by the proposed system architecture and the budgeted failure probabilities.

SAENORM.COM : Click to view the full PDF of arp4761a

The budgeted failure probabilities to meet the safety requirements and objectives can use estimated failure rates, failure rate allocations or data from a failure rate assessment. (The need to maintain margin in the analysis results to meet the safety objectives may be dependent on the maturity of the failure rate data. When using field performance as an input to the probability budget, it is recommended to use conservative failure rates so that any future changes in field performance do not invalidate the safety assessment.)

In addition to physical failures, the PSSA process should consider the potential impact of Single Event Effects. The Single Event Effects consideration may take the form of a qualitative or quantitative analysis (e.g., DD, FTA, MBSA, MA, or FMEA). Examples are provided in Appendix G and AIR6219 of how to evaluate Single Event Effects impacts on an implementation. Similar evaluation can be performed using the other methods.

D.4.2.1.1 Consideration of Latent Failures

Analyze the fault tree to identify latent failures that have an exposure time of longer than one flight cycle. The failure condition to which these latent failures contribute should also be identified.

Determine the maximum interval and test/monitor coverage for latent failures that will allow the analysis to show that the architecture will meet the requirements. This includes:

a. System monitors and their check intervals.

b. Check intervals for backup redundancy.

c. Built-In-Test (BIT) functions and their test activation intervals.

d. “Not to exceed” interval for maintenance tasks (e.g., CCMR intervals).

e. Safety required return to service testing (i.e., any identified return to service testing that mitigates a latent failure).

D.4.2.2 Identification of Need for Independence

Certain system architecture features, such as redundancy, protection and monitoring, may need independence between their elements in order to satisfy the system’s safety requirements and objectives such as “no single failure” requirements or independence requirements related to development assurance level assignment when considering the architecture of system functions. This need for independence is identified as an Independence Principle in this ARP. A common cause affecting multiple redundant elements of a system may compromise the system’s ability to meet availability safety objectives. A common cause affecting both the protection and the protected function, or the monitoring elements and the monitored function of a system may compromise the system’s ability to meet integrity safety objectives.

The need for independence to achieve safety requirements and objectives should be identified and captured in formal independence requirements as discussed in D.4.3. Independence Principles may be identified using various methods; two commonly used methods are described in the following sub-sections. The Independence Principles identified using these methods may result in more specific independence requirements with consideration of a CMA questionnaire (see Appendix M). The CMA questionnaire addresses potential common causes (hardware failure, errors, environment, etc.) and checks the need for generation of new independence requirements.

D.4.2.2.1 Identification of Independence Principles by Design Analysis

Independence Principles may be identified through an examination of the proposed function allocation, the associated FDAL/IDAL assignment, system architecture, and how these relate to the failure conditions identified in the SFHA and to the safety requirements from higher-level analyses (PASA or higher-level PSSA).

Independence Principles may be identified through an examination of the proposed function allocation by reviewing the allocation of higher-level functions to lower-level functions, and the allocation of functions to elements of the architecture. Wherever a higher-level function is allocated to multiple lower-level functions, identify whether the lower-level functions are intended to have redundancy (i.e., each independently accomplish the higher-level function) or monitoring/protection (i.e., one or more lower-level functions capable of detecting, preventing, or otherwise limiting the effects of another’s malfunction) to establish the need for independence.

SAENORM.COM : Click to view the full PDF of arp4761a

When a lower-level function is implemented by multiple elements of the architecture, analysis of this implementation can identify the elements intended to have redundancy, monitoring or protection. Identify Independence Principles wherever lower-level function redundancy, monitoring, or protection is relied on to achieve qualitative or quantitative safety requirements. This identification of Independence Principles by design analysis generally follows the steps outlined in this section. These have been separated into Independence Principles for “failures/errors” and Independence Principles used in the assignment of FDALs and/or IDALs for clarification of identification.

Independence Principles for failures/errors (includes design, installation, manufacturing errors, etc.) are determined by performing the following:

a. Gather the applicable failure conditions from the SFHA and safety requirements from higher-level analyses.

b. Gather descriptions of the system’s design concept and architecture.

c. Where redundancy between elements of the system architecture is necessary to meet safety objectives, identify Independence Principles (a need for independence between those elements).

d. Where protection or monitoring of one element by another element of the system architecture is necessary to meet safety objectives, identify Independence Principles (a need for independence between those elements).

Independence Principles for FDAL and IDAL assignment are determined by performing the following:

a. Gather the applicable failure conditions from the SFHA and safety requirements from higher-level analyses.

b. Gather the function allocation and FDAL assignment to the functions of the system of interest.

c. Where lower-level functions have been assigned FDAL using Table P2, Option 1 or Option 2, identify Independence Principles (a need for independence between those functions).

d. Where items have been assigned IDAL using Table P2, Option 1 or Option 2, identify Independence Principles (i.e., a need for independence between those items).

After each Independence Principle has been identified, determine whether the elements are subject to common cause failure, common cause error, or both (utilizing the CMA questionnaire). Independence requirements generation based on the output of these steps is discussed in D.4.3.1.

SAENORM.COM : Click to view the full PDF of arp4761a

D.4.2.2.2 Identification of Independence Principles by Fault Tree Analysis

Independence Principles may be identified through an examination of the FTA that support PSSA examination of the failure conditions. This FTA examination generally follows using the steps in one of the sub-methods outlined in D.4.2.2.2.1 or D.4.2.2.2.2. In both cases the resulting independence requirements are documented as an output of the PSSA process and managed per the applicable requirements management plans. The steps in this section can be used to identify the independence needed between members when FDAL or IDAL assignment is taking credit for the architecture. (i.e., If the analyst is using a fault tree to model the combinations of potential development errors leading to the failure condition.)

D.4.2.2.2.1 Identification of Independence Principles by AND-Gate Analysis

The fault tree AND-gate analysis examination method to identify Independence Principles generally follows these steps:

a. Gather fault trees related to the system of interest.

b. Identify the AND-gates and AND combinatorial logic gates (k of n) in the FTA gate structure.

c. For each identified AND-gate, evaluate the remaining elements under the gate to determine the Independence Principle(s) that have/has been modeled by the FTA. Further review is not necessary for elements that do not model Independence Principles (e.g., gates performing math functions, external environmental or operational events).

d. Where independence is modeled in the FTA gate, identify the Independence Principle between those elements (eliminate duplicates).

e. Repeat steps b through d until all identified AND-gates have been evaluated.

After each Independence Principle has been identified, determine whether the elements are subject to common cause failure, common cause error, or both (utilizing the CMA questionnaire). Independence requirements generation based on the output of these steps is discussed in D.4.3.1.

If the FTA assumes independence in the modelling of the event represented by AND-gates, then all the possible combinations of fault tree basic events under the AND-gates should be identified and a rationale should be provided for the assumed independence between the various combinatorial base events.

If the FTA models common fault tree basic events that appear on both sides of an AND-gate, then these gates do not represent an Independence Principle. Combinations of other fault tree basic events under the AND-gate may still be identified as Independence Principles. For example, when a fault tree contains (X OR Y) AND (X OR Z), then X is a single event and does not indicate any independence and Y AND Z represents an Independence Principle.

D.4.2.2.2.2 Identification of Independence Principles by Cut set Analysis

Independence Principles can be identified by evaluating the combination of events in the fault tree minimal cut set. The fault tree cut set analysis method to identify Independence Principles generally follows these steps.

a. Gather fault trees related to the system of interest.

b. For each fault tree, extract the minimal cut sets.

c. Where appropriate, determine a minimal cut set list truncation (e.g., by limiting the order and/or the acceptable probability of occurrence).

d. For each minimal cut set, review the events and eliminate events that are inherently independent (e.g., events performing math functions, external environmental or operational events).

e. For each minimal cut set, evaluate the remaining elements to identify the Independence Principle.

f. Repeat steps b through e until all minimal cut sets have been evaluated.

If a minimal cut set appears in multiple fault trees, the Independence Principle only needs to be identified once. This may be accomplished by temporarily OR-ing fault trees containing common elements prior to evaluating the cut sets.

After each Independence Principle has been identified, determine whether the elements are subject to common cause failure, common cause error, or both (utilizing the CMA questionnaire). Independence requirements generation based on the output of these steps is discussed in D.4.3.1.

SAENORM.COM : Click to view the full PDF of arp4761a

D.4.3 PSSA Safety Requirements and Assumptions

Proposed safety requirements and assumptions are captured as outputs of the failure condition evaluation. Proposed safety requirements are identified based on the results of the various PSSA activities. These proposed safety requirements would then be implemented by the development process. Assumptions can be used to define an element of the assessment that is outside of the control of the assessment level being accomplished.

D.4.3.1 Generate Safety Requirements for the Design of Systems or Items

The PSSA requires certain characteristics of the system and/or item for the safety assessment to be valid. To ensure that these characteristics are implemented in the system or item, safety requirements should be proposed to the development process to define the characteristics. Some requirements necessary for safety may already exist. The PSSA process identifies these as safety requirements.

Each of these safety requirements identified at the system-level should be allocated to the items that make up the system. These proposed safety requirements from the PSSA process can directly be distributed to the appropriate levels of the formal system, hardware, and software requirements (e.g., a specific software safety requirement could result in the creation of a low-level software requirement). In addition, each safety requirement should have a rationale that explains the need for the requirement and identifies the specific analyses (fault tree or similar analysis) that establishes the requirement need. This rationale should be as specific (e.g., fault tree gate) as possible to allow review of future changes to the system for impact on safety and to aid in requirement validation activities. These proposed safety requirements include:

a. Requirements to support independence for the proposed implementation. Independence requirements can be created by examining the Independence Principles from D.4.2.2 using the following CMA questionnaire areas as a guide:

    1. CMA (see Appendix M) questionnaire for Independence Principles/requirements related to failures/errors.

    2. CMA (see Appendix M) questionnaire for Independence Principles/requirements related to development errors for FDAL/IDAL assignment.

b. The development assurance levels (FDAL/IDALs) for system, hardware and software development processes including any independence requirements used in the FDAL or IDAL assignment as established in D.4.1.

c. Requirements for associated probability budgets identified in PSSA FTA as noted in D.4.2.1.

d. Requirements allocated to items (both hardware and software) to support detection of physical hardware failures as established in D.4.2.1 for systems, hardware, and software development processes. Some examples may include:

    1. Monitor operational requirements such as:

        i. Monitor thresholds.

        ii. Monitor cycle times (including counts before monitor takes action).

        iii. Monitor confirmation constraints as number of detection cycles to confirm or maximum delay allowed to confirm a failure detection.

        iv. Monitor scrub (verification) times.

        v. Monitor fault response.

        vi. Monitor coverage (functional path coverage or specific misbehavior to detect).

        vii. Monitor independence from monitored function.

    2. For redundant architectures:

        i. Hardware independence.

        ii. Source selection and voting.

        iii. Reconfiguration (when and to what new configuration).

    3. Required tests including return-to-service tests if necessary to support the exposure times.

e. Mitigation techniques for Single Event Effects as noted in D.4.2.1, if needed.

When an FMEA/FMES is being used alone or mitigated failures from the FMEA/FMES are used to support an FTA, the FMEA/FMES may identify the need for safety requirements.

SAENORM.COM : Click to view the full PDF of arp4761a

D.4.3.2 PSSA Assumptions

In addition to safety requirements on the system or items, there may be characteristics of external systems or the aircraft that must be true for the PSSA to be valid. These characteristics should be stated as assumptions in the PSSA. Characteristics that must be true for the PSSA to be valid and are under the control of the organization performing the PSSA should be captured as proposed requirements as discussed in D.4.3.1. Some potential assumptions include:

a. Average flight length.

b. Average power up time.

c. Assumptions for the design to be provided to the aircraft-level development process (e.g., crew actions, equipment installation, power independence, segregation of wiring).

d. The safety maintenance tasks and associated “not to exceed” times if applicable.

e. Interfacing systems properties (e.g., FDALs, IDALs, Independence Principles, undeveloped events external to the systems including probability and/or dormancy period).

f. FDALs and IDALs assigned by the PSSA process for confirmation at the aircraft-level (ensure that the principles in ARP4754B/ED-79B Section 5.2 remain satisfied).

These assumptions are also outputs of the PSSA process as identified in bullet e. of D.6.1.

D.5 PSSA COMPLETION

The PSSA determines whether the safety objectives associated with each system failure condition can be satisfied and identified safety requirements can be met by the proposed system architecture. The answer to this question is not limited to quantitative probabilistic requirements or FDAL/IDAL assignment, but considers the collective results of the failure condition evaluation process.

The system architecture should be assessed against the following points to confirm it can be reasonably expected to meet the system safety objectives and requirements:

a. Have the quantitative analyses shown that the proposed system implementation of the architecture can reasonably be expected to satisfy the numerical requirements and safety objectives?

b. Have FDALs and IDALs for the functions and items implementing the system been assigned with rationale to substantiate the assignment and do the assignments meet the FDAL/IDAL input requirements from higher-level safety assessments?

c. Are the necessary independence requirements for functions and items identified and captured in the system architecture?

d. Are the safety requirements for the system architecture identified?

e. Have the safety requirements, including FDAL and IDAL assignment, been accepted by the development process?

f. Does the architecture introduce additional failure conditions not inherited from the SFHA, and if so, have they been communicated to the higher-level safety assessments?

g. Is there an identifiable relationship between the safety requirements and the safety assessment that necessitated the requirement?

h. Have assumptions from any lower-level PSSAs been confirmed, if such assumptions have already been fed back from lower levels?

SAENORM.COM : Click to view the full PDF of arp4761a

i. Have assumptions been captured?

j. Have the derived requirements determined by the development process to have a potential safety impact been addressed by this safety assessment?

If the collective results of the failure condition evaluation process indicate that the proposed architecture is capable of meeting applicable requirements and all necessary PSSA outputs have been generated, the results of the PSSA are captured as part of the documentation set.

In the event that a potential issue with meeting the requirements is identified, the results are reported back to the applicable system or equipment architecture development process to aid in requirements and architecture changes. If the potential issue is associated with a requirement allocated down from a higher-level safety process (e.g., PASA), the results may be referred back to the higher-level process to determine if a change to the requirement can be made while allowing the higher-level safety requirements to be met.

D.6 GENERATE PSSA OUTPUTS

Once the PSSA process confirms that the system architecture under evaluation can reasonably be expected to meet the system-level safety objectives, the outputs are captured as a baseline. The PSSA process results provide sufficient analysis information to validate safety requirements identified from the PSSA process and may be used for some validation records.

D.6.1 Capturing PSSA Process Data

The results of the PSSA process should be documented so that there is evidence of the steps taken in developing the PSSA data. The PSSA analyses are representative of an architecture that is expected to meet the safety requirements and objectives. This assessment documentation provides source justification of the proposed safety requirements developed during the PSSA process. The source justification may include references to fault trees, qualitative summaries, and system specifications. Linkage to this source information will assist in the evaluation of future requirements change impact.

The PSSA outputs to be captured as a baseline upon completion of the PSSA include:

a. Safety requirements provided to the PSSA process (see D.2.2).

b. Evaluation results for safety requirements and safety objectives (e.g., FDAL/IDAL assignment, FTA, DD, MA, MBSA).

c. Safety requirements from the PSSA process (see D.4.3.1).

d. An updated failure condition list which includes the rationale for how the safety requirements (qualitative and quantitative) can be met with the chosen architecture (linkage between SFHA and PSSA; e.g., FTAs).

e. Assumptions that are required to make the PSSA valid (see D.4.3.2).

D.6.2 Outputs to Lower-Level PSSA Process

A PSSA may be performed at any level. The outputs to lower-level PSSAs are the failure effects of concern, qualitative requirements, budgeting probabilities and development assurance levels identified during a higher-level PSSA or PASA including further FDAL and IDAL assignment constraints. After the inputs are received, the PSSA lower-level process is equivalent to that described in Sections D.1 to D.5.

D.6.3 Outputs to Higher-Level PSSA or PASA Process

Any assumptions used in the analysis need to be validated via feedback to the higher-level safety analyses. This may include outputs to PSSAs at the same level (e.g., interfacing systems). PSSA FDAL and IDAL feedback is provided to ensure that the interaction of system-level FDALs and IDALs and independence attributes meet the aircraft-level safety requirements.

SAENORM.COM : Click to view the full PDF of arp4761a

D.6.4 Relationship Between PSSA and SSA

The outputs of the final PSSA are input to the SSA process where they can be re-evaluated against the implemented design for verification purposes.

Once system safety requirements have been defined in a PSSA process, and the implementation of the system is mature, the safety process transitions to the SSA. The SSA activities verify that the implemented system supports the safety objectives and other safety requirements. The PSSA data may need to be maintained to ensure a complete set of PSSA/SSA data is available to support the aircraft certification.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX E - SYSTEM SAFETY ASSESSMENT (SSA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

E.1 INTRODUCTION 98
E.1.1 SSA Process Overview 98

E.2 GATHER SSA INPUT DATA 99

E.3 EVALUATE SAFETY OBJECTIVES AND REQUIREMENTS 100
E.3.1 Confirm Safety Requirements Established in PSSA Processes are Satisfied 100
E.3.2 Confirm Safety Objectives and Requirements are Satisfied 101

E.4 SSA COMPLETION 102

E.5 GENERATE SSA OUTPUTS 103
E.5.1 Capturing SSA Process Data 103
E.5.2 Linkage of the SSA to the ASA 103

Figure E1 System Safety Assessment process 99

SAENORM.COM : Click to view the full PDF of arp4761a

E.1 INTRODUCTION

The System Safety Assessment (SSA) is a systematic examination of a system, its architecture and its installation to demonstrate that the implemented system meets its safety requirements and safety objectives. The SSA process verifies that the implemented design meets the objectives associated with the failure conditions and classifications defined in the SFHA. The SSA process also verifies that the implemented design meets the safety requirements allocated to the system in order to meet safety objectives. Qualitative and quantitative methods of analysis are used as appropriate to demonstrate that the safety requirements and objectives are met.

The SSA process may include the application of the analysis methods at more than one level of abstraction (system, subsystem, equipment or part of equipment) or by more than one organization (e.g., aircraft manufacturer, system supplier). The various levels of SSA support a single analysis performed on a system. The SSA is performed based on the safety objectives from the SFHA in combination with safety requirements allocated to the system.

Throughout this appendix, reference is made to using Fault Tree Analysis (FTA). It should be understood by the reader that Dependence Diagrams (DD), Markov Analysis (MA), Model-Based Safety Analysis (MBSA), or other techniques may be selected to accomplish the same purpose, depending on the circumstances and the types of data desired.

E.1.1 SSA Process Overview

The SSA process is an approach for verifying that the safety requirements allocated to the system and safety objectives from the SFHA, have been met by the actual implementation. Figure E1 describes the process flow for the SSA. This SSA includes the following steps:

a. Gather SSA input data (Section E.2).

b. Evaluate safety objectives and requirements (Section E.3).

c. Determine if the implemented system satisfies the safety requirements and objectives (Section E.4).

d. Generate SSA outputs (Section E.5).

SAENORM.COM : Click to view the full PDF of arp4761a

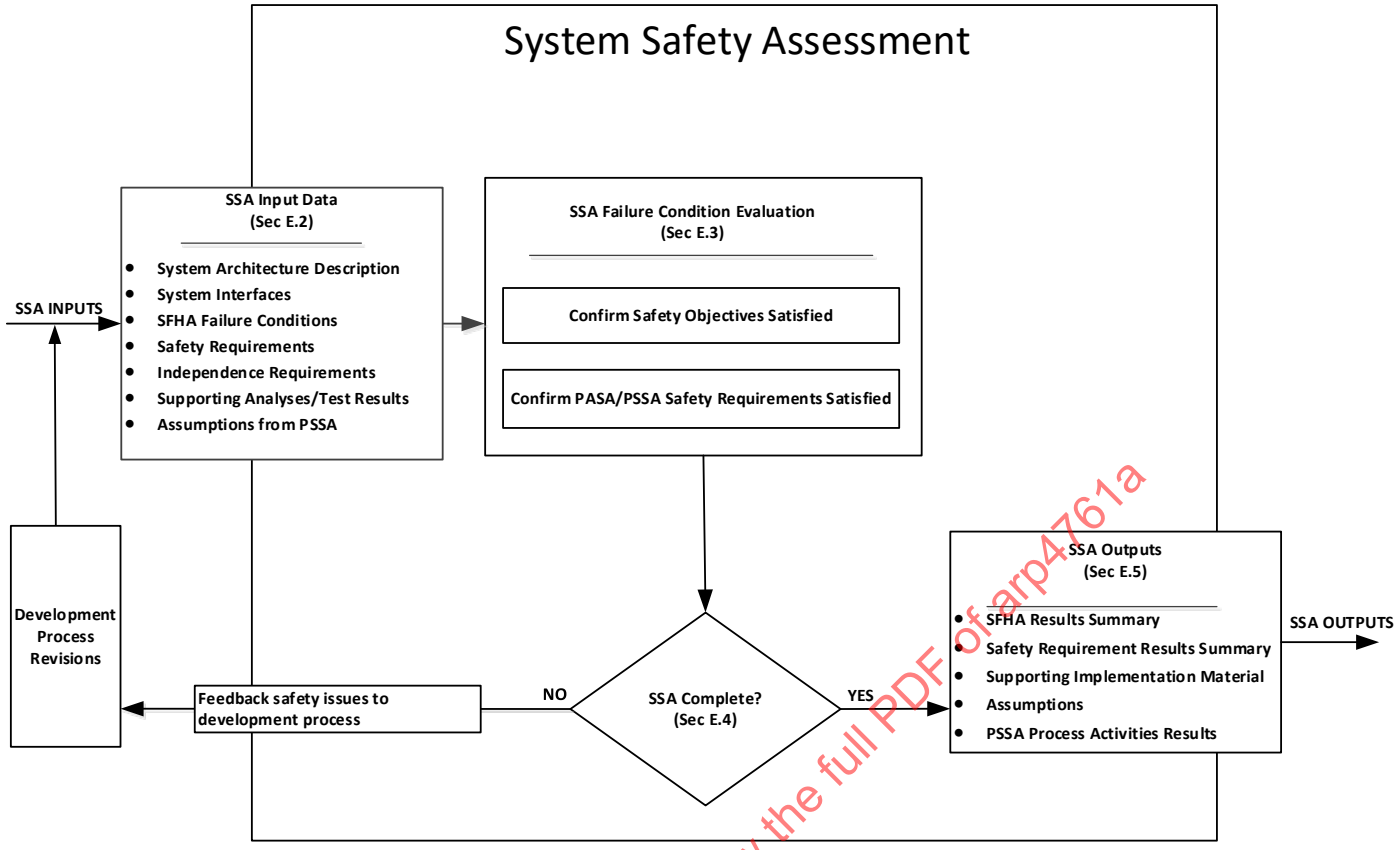


Figure E1 - System Safety Assessment process

E.2 GATHER SSA INPUT DATA

Since the SSA may be performed at any level, the specific inputs applied will depend on the level at which the SSA activity is performed. Inputs to the SSA process include:

a. Implemented architecture description and the associated design rationale documented in the design process (e.g., requirements documents including derived requirements, open problem reports, system definition document, detailed design description, models).

b. Implemented interfaces and their interactions with the equipment of the systems documented in the system design process (e.g., requirements documents, interface control document).

c. Failure conditions, their associated classifications and objectives from the SFHA.

d. Safety requirements allocated to the system, identified during the PASA and PSSA processes.

e. Independence requirements from PASA and PSSA.

f. Results of supporting analyses and tests including:

   1. Analyses from the subsystem or equipment suppliers (e.g., subsystem SSAs, FTA, or FMEA).

   2. Assumptions from the subsystem or equipment supplier SSAs that are necessary for their SSA to be valid.

   3. System functional verification results.

   4. Assumptions from the PSSA to evaluate for applicability in the SSA.

SAENORM.COM : Click to view the full PDF of arp4761a

E.3 EVALUATE SAFETY OBJECTIVES AND REQUIREMENTS

Safety objectives and requirements are evaluated by qualitative analyses and supported by quantitative analyses where appropriate to:

a. Confirm that the safety requirements identified in the PSSA process are met.

b. Confirm that the safety objectives based on the failure condition classifications established in the SFHA and safety requirements allocated to the system are satisfied.

An SSA may be performed at any level. The specific evaluation activities to be applied will depend on the level at which the SSA activity is performed.

Verification of safety objectives and requirements may require the results of safety assessments from lower-level subsystem and equipment suppliers. Analysis assumptions used in lower-level analysis should be either confirmed during the SSA process or escalated to a higher level for confirmation.

E.3.1 Confirm Safety Requirements Established in PSSA Processes are Satisfied

The safety evaluation in the SSA process relies on the safety requirements established in the PSSA process being verified. The SSA process relies on the system development process (e.g., ARP4754B/ED-79B) for verification that Function and Item Development Assurance Levels (FDAL and IDAL) have been achieved and that safety requirements (e.g., requirements of monitors, redundancies, protection mechanisms, self-test/tests) are satisfied. Issues identified during these verification activities may impact the analysis performed as part of the SSA process.

Independence requirements and quantitative requirements are two examples of safety requirements that the SSA process verifies have been satisfied.

In addition, analysis assumptions used in lower-level analysis should be either confirmed as part of the SSA process, or they should be escalated to a higher level for confirmation.

E.3.1.1 Confirm Independence Requirements are Satisfied

Independence requirements were identified during the PSSA process (see D.4.2.2). If changes to the design have occurred, the PSSA process (see Appendix D) should be iterated to identify potential changes to the independence requirements.

The analyst uses common cause methods to verify that the independence requirements identified during the PSSA process have been implemented. As part of the SSA process, the Common Mode Analysis (CMA) is the primary method used to verify the independence requirements (see Appendix M). The results of any lack of independence identified in the CMA are evaluated by the analyst for acceptability in the context of the SSA. If not already addressed during the verification of the independence requirements, the analyst should confirm the common cause methods provide supporting evidence to confirm the independence implied through the use of AND-gates in the quantitative analysis.

Additional independence requirements may be verified by the ZSA (see Appendix K) and PRA (see Appendix L).

E.3.1.2 Confirm Quantitative Requirements are Satisfied

The PSSA process may result in the identification of quantitative safety requirements. These requirements are in addition to the safety objectives identified based on the failure condition classifications in the SFHA and to quantitative safety requirements decomposed from higher-level failure conditions evaluated in the PASA or higher-level PSSA.

An FTA (or other quantitative analysis) may be used, similarly to that described for verification of failure condition safety objectives (see E.3.2.7), to verify that the safety requirements have been satisfied.

SAENORM.COM : Click to view the full PDF of arp4761a

E.3.2 Confirm Safety Objectives and Requirements are Satisfied

For each failure condition in the SFHA an analysis is performed to show that the safety objectives are met. The main body of this document summarizes the type (qualitative or quantitative) of safety analysis that should be performed for each failure condition (see main body 3.8). This analysis includes:

a. Understanding the system implementation of functions associated with the failure condition.

b. Understanding the implemented design features that aid in mitigating the failure condition (e.g., redundancy monitoring).

c. Understanding the fault detection and crew awareness features.

d. Understanding the crew or maintenance action necessary to mitigate the effects of the condition.

e. Qualitative and quantitative analysis, as necessary.

The analyst uses the details of the system implementation to identify how the failures of the system elements contribute to the failure condition being analyzed. The results of these analyses should verify whether the design as implemented satisfies the objectives established by the failure condition's severity classification. The analysis should also verify whether the design as implemented satisfies the safety requirements allocated to the system.

E.3.2.1 Understanding System Implementation of Functions Associated with Failure Condition

The analyst should understand the implemented operation of the system to begin the safety assessment process. Details of the implemented system may be obtained from system drawings, wire diagrams, or lower-level safety analyses. Requirements are another source for data about the intended operation of the implemented system. However, the analyst should be aware that some requirements may not be fully satisfied.

E.3.2.2 Understanding Implemented Design Features Mitigating Failure Condition

A review of the implemented design should identify those design features that were established to mitigate the failure condition being evaluated. Wherever these design features support the failure condition evaluation, details of these features and their associated rationale should be documented with the safety analysis as discussed in E.5.1. Things to consider in this review include:

a. Architectural features (e.g., redundancy, signal selection or voting, fault detection strategies, and fault responses) which have been implemented to mitigate failure conditions. This could include appropriate block diagrams depicting the architectural features, and their independence attributes.

b. Failure detection mechanisms (e.g., monitors) which have been implemented to mitigate unintended or erroneous function. This includes monitor cycle times, limitations of monitor coverage, fault response, and independence between the monitor and function being monitored.

c. Tests (e.g., built-in test, maintenance tests) which have been implemented, including coverage of the function, test cycle times, and fault response. This may include independence of the test and the function being tested.

E.3.2.3 Understanding Crew Awareness Features

The analyst should confirm that an assessment of the appropriateness and effectiveness of crew awareness features (e.g., timeliness, level of alerting), particularly those necessary to mitigate the severity of a failure condition, has been performed. For example, for 14 CFR Part 25/CS-25 aircraft, this would be planned and executed in the corresponding human factors' certification process following FAA AC 25.1302-1/EASA AMC 25.1302; FAA AC 25.1322-1/EASA AMC 25.1322.

E.3.2.4 Identify Significant Latent Failures

For each Catastrophic and Hazardous failure condition, the analyst should analyze the fault tree to identify all latent failures that have a latency period longer than one flight of average duration. These latent failures are significant latent failures.

SAENORM.COM : Click to view the full PDF of arp4761a

E.3.2.5 Identify Wear Out Failures

For systems with mechanical equipment, the analyst should identify any wear out failures that contribute to the failure conditions as these may indicate a need for a periodic maintenance task.

E.3.2.6 Understanding Crew or Maintenance Action Mitigating Effects of Failure Condition

Crew action may have been credited to mitigate the effects of a particular failure condition. The SSA should identify any crew procedures or other crew actions necessary to mitigate the effects of failure conditions listed in the SFHA. A review of the aircraft flight manual procedures should confirm the necessary crew action is defined and that the action mitigates the effects.

Scheduled maintenance tasks may be used to limit exposure to certain failure modes. The SSA process at the aircraft manufacturer (or design approval holder) level should confirm that all scheduled maintenance tasks for which safety credit has been taken are captured in the maintenance documentation.

Where the SSA determines that scheduled maintenance tasks are necessary to meet the safety objectives related to a failure condition, the associated tasks should be identified and the “not to exceed intervals” determined. These maintenance tasks and intervals are evaluated at the next higher level as assumptions. At the highest SSA level, the SSA process should confirm that these “not to exceed intervals” are captured in the aircraft flight manuals or Instructions for continued airworthiness. For example, for 14 CFR Part 25/CS-25 aircraft, this would be via the Candidate Certification Maintenance Requirements (CCMR). A separate process determines which CCMR become Certification Maintenance Requirements (CMR). AC 25-19A/AMC 25-19 contain the process for identifying CCMRs and CMRs.

E.3.2.7 Qualitative and Quantitative Analysis as Necessary

Safety requirements and objectives are verified by FTA to show how failures combine to lead to the failure condition. The SSA evaluates the implemented system and, as such, the SSA fault trees may identify additional Independence Principles that should be evaluated by the PSSA process to determine if additional independence requirements are necessary.

E.4 SSA COMPLETION

The SSA is complete when it has verified that the implemented system meets the identified safety objectives and requirements (e.g., qualitative, quantitative, FDAL/IDAL assignment, independence) and/or any deviations to the identified safety objectives and requirements which have been agreed by the higher-level SSA/ASA process.

The system implementation should be assessed against the following points to verify it meets the requirements and safety objectives.

a. Do the analysis results support that the independence requirements have been met by the implementation (e.g., CMA, ZSA, PRA)?

b. Have the safety requirements been implemented for the system (E.3.2)?

c. Have analysis assumptions used in lower-level analysis either been confirmed or escalated to a higher level for confirmation?

d. Have all problem reports that impact the safety assessment been addressed?

If an issue with meeting the requirements is identified, the results are returned to the applicable system, equipment, or item development process to aid in requirements or architecture changes. The PSSA process is repeated to evaluate the impact of any design changes. These changes may warrant a revision to the PSSA process output, but this is left to the discretion of the design organization. As stated in the PSSA (see Appendix D), for design organizations that elect not to revise the PSSA output after the development phase is complete, the PSSA process activity will still need to be repeated and results captured within the SSA output.

SAENORM.COM : Click to view the full PDF of arp4761a

The resulting SSA documentation should provide an output similar to that described in PSSA (see Appendix D) and show the delta between the original safety requirements and the new safety requirements, as well as capturing any necessary justification for the requirement and/or architecture changes. If the issue is associated with a requirement received from a preliminary safety process, the results may be returned to the preliminary processes to determine if a change to the requirement can be made.

If the collective results of the safety objectives and requirements evaluation indicate that the implementation meets the requirements, the SSA results may be captured.

E.5 GENERATE SSA OUTPUTS

E.5.1 Capturing SSA Process Data

The results of the SSA process should be captured so that there is traceability of the steps taken in developing the SSA. The SSA process documentation should be selected from the following information based on the level of analysis being performed (e.g., system, subsystem).

a. Failure condition quantitative analysis result summary - listing of failure conditions from the SFHA with quantitative analysis (i.e., FTA) results comparison.

b. Safety requirement quantitative analysis result summary - listing of safety requirements allocated to the SSA with quantitative analysis (i.e., FTA) results comparison.

c. Results of the qualitative assessments of each failure condition or safety requirement, including narratives of contributing system failures, preventative design features, identified significant latent failures, wear out failures, crew awareness features, or mitigating crew actions.

d. Assumptions used in the assessment (e.g., installation, aircraft flight manual procedures, not-to-exceed intervals) that need to be addressed outside of the system under analysis for the SSA to be valid.

e. Results of PSSA process activities revisited during the SSA process (e.g., new requirements necessary for safety).

f. Reference to system description information that highlights safety features that provide mitigation for integrity and availability (e.g., redundancy, monitoring). These may include block diagrams to depict the architectural features, independence, and methods of configuring the systems to maintain availability.

g. Where a safety objective or requirement is not met, provide a reference to document evidence stating the unsatisfactory result is acceptable to support the overall objective.

h. Provide details of any recommended maintenance actions that result in CCMRs (see E.3.1.5).

E.5.2 Linkage of the SSA to the ASA

The SSA documented results of the analyses of safety requirements from the PASA/PSSA and safety objectives from the SFHA are provided to the ASA process for use in evaluating aircraft-level safety requirements.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX F - AIRCRAFT SAFETY ASSESSMENT (ASA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

F.1 ASA OVERVIEW 105

F.2 ASA INPUTS 106
F.2.1 ASA Inputs from Safety Analyses 106
F.2.2 ASA Inputs from Aircraft and System Development Processes 106

F.3 AIRCRAFT SAFETY ASSESSMENT 107
F.3.1 Confirm Safety Program Plan is Satisfied 108
F.3.2 Confirm Safety Assumptions are Correct 108
F.3.3 Confirm AFHA and PASA Processes are Completed 108
F.3.4 Confirm Supporting Verification Activity is Complete 108
F.3.5 Confirm Concurrence with Open and Deferred Problem Reports 108
F.3.6 Confirm Safety Related Aircraft Operating Procedures 108
F.3.7 Analyze Final Aircraft Architecture 109
F.3.8 Confirm Final FDAL and IDAL Assignments 109
F.3.9 Confirm CMA, PRA, and ZSA Results 110

F.4 ASA COMPLETION 110

F.5 ASA OUTPUTS 111

Figure F1 Aircraft Safety Assessment process 105

SAENORM.COM : Click to view the full PDF of arp4761a

F.1 ASA OVERVIEW

The Aircraft Safety Assessment (ASA) is a systematic, comprehensive evaluation of the aircraft implementation to show that the failure conditions identified in the AFHA have been addressed and that corresponding safety requirements are met. The ASA process results in confirmation that the interactions of system functions, their interdependencies, independence, separation, and their contribution to associated failure conditions have been appropriately identified and assessed. The ASA does not replace the SSAs for showing that failure conditions identified in the SFHA have been addressed and that system-level safety requirements are met. The ASA is intended to be performed when the aircraft architecture is mature.

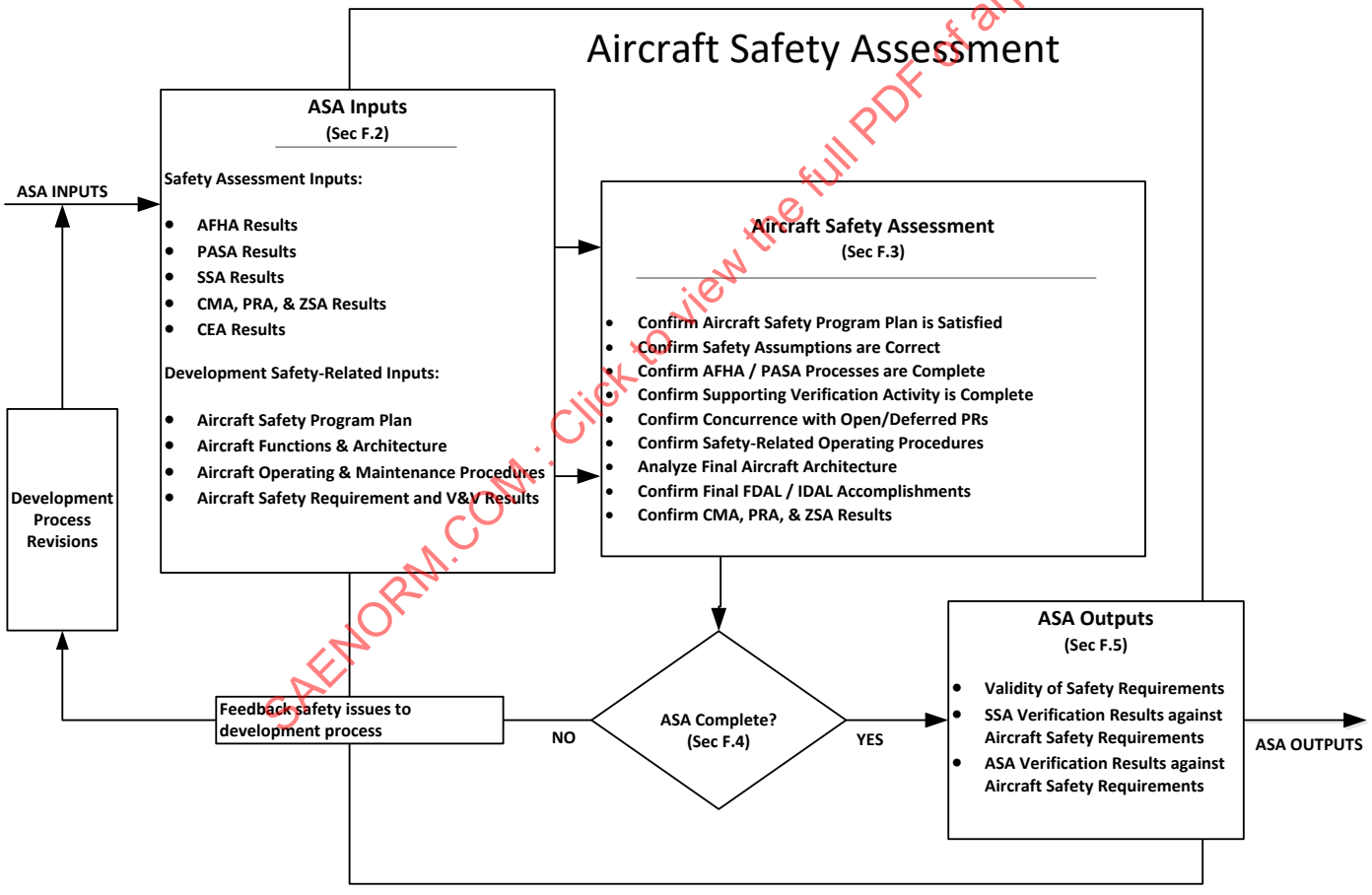
The ASA is conducted as shown in Figure F1 as follows:

a. Gather input data (Section F.2).

b. Conduct safety assessment activities (Section F.3).

c. Determine whether the aircraft has met its safety requirements (Section F.4).

d. Document assessment results (Section F.5).



SAENORM.COM : Click to view the full PDF of arp4761a

Figure F1 - Aircraft Safety Assessment process

F.2 ASA INPUTS

Inputs to the ASA come from the aircraft and system development processes and from the associated PASA and system safety activities, analyses and results described within the other appendices of this document.

F.2.1 ASA Inputs from Safety Analyses

F.2.1.1 AFHA Results

The ASA uses the aircraft-level failure conditions and classifications identified by the AFHA (see Appendix A).

F.2.1.2 PASA Results

The PASA outputs are used as the starting point for initiating the ASA (see Appendix B).

F.2.1.3 SSA Results

The ASA uses the SSA results (see Appendix E) as inputs to the analysis. Because there are many SSAs, it is necessary to identify the system-level information relevant for use in the ASA. The SSAs are the primary source of:

a. Qualitative and quantitative failure information from FMEAs and FTAs, such as failure modes, failure probabilities, failure rates, and exposure times.

b. Development assurance level (both FDAL and IDAL) information including confirmation that the levels have been achieved.

c. Design information demonstrating system-level independence requirements are met.

d. Safety driven maintenance tasks.

e. Crew procedures and associated flight deck alerts.

F.2.1.4 CMA, PRA, and ZSA Results

The ASA uses aircraft-level and system-level Common Mode Analyses (CMA) results (see Appendix M) to confirm the independence requirements are satisfied in the aircraft implementation.

The ASA uses the Particular Risk Analyses (PRA) results (see Appendix L) to confirm that, in the event of a defined threat, the aircraft implementation is such that consequences are minimized at an acceptable level in terms of survivability.

The ASA uses the Zonal Safety Analyses (ZSA) results (see Appendix K) to confirm that the physical interactions of the implemented systems do not violate intended independence assumptions and requirements. The ASA confirms that there is adequate separation of functions or functional channels.

F.2.1.5 CEA Results

The ASA uses the Cascading Effects Analysis (CEA) techniques (see Appendix O) to support the MF&MS analysis to account for detailed system interfaces and possible cascading failure paths between systems in the aircraft implementation. The completed aircraft cascading effect analysis includes the combined aircraft response for the affected aircraft or system functions, including any crew alerts or indications that will be caused by an initiating failure.

F.2.2 ASA Inputs from Aircraft and System Development Processes

F.2.2.1 Aircraft Safety Program Plan

The ASA uses the scope and content of the safety activities that are defined within the aircraft safety program plan (ARP4754B/ED-79B).

SAENORM.COM : Click to view the full PDF of arp4761a

F.2.2.2 Aircraft Functions and Architecture

The ASA uses the implemented aircraft functions and architecture provided in various aircraft and system description data.

F.2.2.3 Aircraft Operating and Maintenance Procedures

The ASA uses the aircraft operating and maintenance procedures. The operational information may take many forms that together capture the normal and abnormal/non-normal procedures, as well as airworthiness limitations to ensure that the aircraft is used in a manner consistent with the intended design and the aircraft and systems safety analyses. These include the Aircraft Flight Manual (AFM), Flight Crew Operations Manual, annunciation checklists, and training materials.

The maintenance procedures needed for the ASA include those used to substantiate constraints on exposure times of latent failures.

F.2.2.4 Aircraft Safety Requirements and Their Validation and Verification Results

The ASA uses:

a. Aircraft requirements management process to establish and validate safety requirements developed from the AFHA/PASA and verify that the implementation satisfies them.

b. Assumption validation results from the PASA and related SSA, CMA, PRA, and ZSA activities.

c. Open and deferred problem reports from the development process.

F.3 AIRCRAFT SAFETY ASSESSMENT

The ASA is used to confirm that safety activities from the aircraft safety program plan (see F.2.2.1) have been completed and that the aircraft architecture satisfies safety requirements. To provide this assessment, the ASA evaluates the aircraft-level activities described in the safety program plan in relation to the aircraft-level failure conditions from the AFHA and the outputs from the PASA.

The ASA provides a means of showing that AFHA failure conditions and the safety requirements originating from those failure conditions have been satisfied by the aircraft architecture.

The ASA should be conducted in two steps:

a. Initial ASA evaluation confirms which AFHA failure conditions are satisfied by analysis conducted for a single system in its SSA or identify if further analysis is needed at the aircraft-level in the ASA.

b. Once any further aircraft-level analysis in the ASA is complete, the ASA re-evaluates the AFHA failure conditions with the complete set of analyses to ensure that the aircraft-level failure conditions and their associated safety requirements have been adequately satisfied.

The following sections describe specific activities which may be used to show that these safety requirements have been satisfied by the aircraft architecture. These activities can be categorized into three groups:

a. Activities confirming the applicable aircraft safety requirements are valid and considered stable: F.3.1 through F.3.6 describe assessment of these requirements through review of the aircraft development and safety data.

b. Activities which confirm that results from other analyses (e.g., SSA, PRA) used to satisfy aircraft-level safety requirements are completed: F.3.7.1 and F.3.9 describe activities intended to ensure completeness of any analysis outside of the ASA.

c. Analysis activities conducted within the ASA which are an extension from the PASA to show the aircraft-level safety requirements are satisfied. This is described in F.3.7.2 and F.3.8.

SAENORM.COM : Click to view the full PDF of arp4761a

F.3.1 Confirm Safety Program Plan is Satisfied

The ASA is used to confirm that the aircraft safety program plan is satisfied through the activities described in F.3.2 through F.3.9.

F.3.2 Confirm Safety Assumptions are Correct

Assumptions, including those from the PASA, PSSA, SSA, ASA, CMA, PRA, and ZSA, if not already validated, should be assessed to confirm their validity including the effect that they have on aircraft-level safety.

Each ASA assessment should address assumptions that capture interactions across multiple systems, for example, assumptions of the response to a fault by the systems and crew. In some cases, simulation or testing may be necessary to validate the effects of failures and their contribution to top events.

F.3.3 Confirm AFHA and PASA Processes are Completed

The ASA confirms that the PASA and the AFHA have been completed. The AFHA should be reviewed to confirm that all of its failure conditions have been validated. Any activity (e.g., analysis, test) needed to validate those failure conditions should be identified.

Instances may arise where the PASA requires re-evaluation which may alter or generate safety requirements and can lead to changes in the architecture. New safety requirements or architecture changes may need to be assessed against the PASA process (see Appendix B). These changes may warrant a revision to the PASA documentation, but this documentation revision is left to the discretion of the program. For the program that elects not to revise the PASA, the PASA process activity will need to be captured in the program's documentation.

This provides an output that shows the differences between the original safety requirements and the new safety requirements as well as capturing any necessary justification for the requirement and/or architecture changes.

F.3.4 Confirm Supporting Verification Activity is Complete

The ASA confirms that the testing and analysis used to meet the safety requirements have been completed. Safety requirements allocated to systems can refer to the SSA in which the completion of that activity is documented. Safety requirements at the aircraft-level should confirm that the necessary testing and analysis has been completed. Typically, this aircraft-level activity is used to support either the verification of the appropriate use of AFM procedures or the verification of common cause findings. The ASA process also confirms that any SFHA safety objectives that are not mapped to safety requirements are appropriately dispositioned.

F.3.5 Confirm Concurrence with Open and Deferred Problem Reports

Open and deferred problem reports are reviewed during the development process to see whether they have a safety impact. Problem reports that have a safety impact that are open or deferred are assessed for their impact on the ASA results. A large program may have a process to identify a subset of significant open problem reports for the ASA review.

Open problem reports at an equipment-level are normally assessed for an impact at the system-level. Corresponding system problem reports are raised to track any system effects. Open problem reports at the system-level are normally assessed for an impact at aircraft-level. Corresponding aircraft problem reports are raised to track any aircraft effects.

The analysis performed in support of the ASA confirms that open or deferred problem reports that affect the aircraft architecture, aircraft-level functionality, or aircraft-level requirements have been assessed for potential changes that can affect the configuration.

F.3.6 Confirm Safety Related Aircraft Operating Procedures

Operating procedures captured in the Aircraft Flight Manual supporting the safety assessments should be reviewed to confirm that they achieve their intended purpose at the aircraft-level. Inputs may also be made to the Flight Crew Operations Manual, aircraft Maintenance Manual and training materials.

SAENORM.COM : Click to view the full PDF of arp4761a

F.3.7 Analyze Final Aircraft Architecture

The confirmation activities of F.3.1 through F.3.6 provide a stable basis for assessing the final aircraft architecture. The ASA analyzes the final aircraft architecture relative to each aircraft-level failure condition in the AFHA. Some of the methods used in the PASA are also used to conduct the ASA, except that the final aircraft architecture is the subject of the analysis instead of the proposed architecture(s). The interactions between system functions and between systems identified in the PASA and the safety data for the individual systems obtained from the SSAs are used to verify that the aircraft as a whole meets the aircraft-level safety requirements.

F.3.7.1 Confirm Failure Conditions Allocated to a System

The ASA confirms that AFHA failure conditions allocated to a system through the PASA have been addressed in their respective SSAs.

F.3.7.2 Multifunction and Multisystem Analysis

For AFHA failure conditions with contributions from more than one system to be analyzed in the ASA, the Multifunction and Multisystem (MF&MS) analysis verifies that the associated safety requirements and objectives are met. The PASA Interdependence Analysis may need to be updated depending on the degree of change in the final aircraft architecture. For the purpose of the ASA, the MF&MS analysis is typically performed on aircraft-level failure conditions classified as Catastrophic and Hazardous, depending on the needed depth of analysis (see 3.8), and include the following inputs:

a. Fault tree data (or equivalent analysis data) from the pertinent SSAs across the aircraft with sufficient fidelity and depth to explain the aircraft-level failure condition, and to reveal any additional failure combinations that might not have been considered in the PASA or in the individual SSAs. The fault tree data should reflect:

    1. How failures from across the aircraft combine to lead to the aircraft-level failure condition under consideration.

    2. Availability and integrity results from SSAs as necessary to support the aircraft-level failure condition classification.

    3. Factors such as the final intended flight profiles and operations (e.g., Extended-Range Operations (ETOPS) and non-ETOPS, airport environments), reliability data, and operational constraints developed after PASA was completed.

b. Results of Cascading Effects Analysis for consistency with the MF&MS analysis.

c. Common resource systems contribution to aircraft-level hazards for consistency with the MF&MS analysis.

The MF&MS analysis results may also be used to identify and show:

a. That no single failures in the aircraft systems can result in Catastrophic failure conditions.

b. That single failures resulting in Hazardous failure conditions are visible and their acceptability has been substantiated, including adequacy of associated maintenance procedures, crew procedures, and flight deck alerts.

c. The adequacy of maintenance tasks and intervals for significant latent failures and life-limited equipment.

F.3.8 Confirm Final FDAL and IDAL Assignments

The PASA process assessed aircraft-level failure conditions and assigned FDALs to the system functions. The ASA ensures that IDAL assignments are commensurate with AFHA failure condition classifications whenever the item is involved in multisystem combinations identified in the PASA. The ASA confirms that the assigned FDALs and IDALs satisfy each of the aircraft-level failure conditions and adhere to the development assurance level assignment principles as described in Appendix P.

SAENORM.COM : Click to view the full PDF of arp4761a

F.3.9 Confirm CMA, PRA, and ZSA Results

The CMA, PRA, and ZSA support the ASA by investigating the aircraft capability from a number of perspectives using the safety requirements captured throughout the program. These include architectural design constraints such as separation, segregation, survivability and functional independence (e.g., implementation in common resource system like Integrated Modular Avionics mitigated by independent backup function).

The CMA assesses the aircraft susceptibility to common cause error and common cause failures (see Appendix M). The PRA assesses the aircraft susceptibility to threats that have the potential to violate independence of redundant elements or identify possible vulnerabilities (see Appendix L). The ZSA assesses the physical installation relative to separation and segregation requirements and the potential for undesirable interference between equipment (see Appendix K).

Confirmation of these analyses are documented in the ASA.

F.3.9.1 Common Mode Analysis

The ASA uses the CMA to confirm that functional and item development independence is maintained per each of the applicable independence requirements.

F.3.9.2 Particular Risk Analysis

The ASA confirms that particular risk will not defeat the intended independence to the extent that aircraft survivability is compromised. Also, the ASA dispositions residual safety-related effects discovered by PRA. A summary of the PRAs performed on the aircraft should be included as part of the ASA process.

F.3.9.3 Zonal Safety Analysis

The ASA uses the ZSA to confirm that physical installation of equipment and systems does not compromise safety and, in particular, that intended physical independencies have not been compromised.

F.4 ASA COMPLETION

The ASA determines that the requirements related to or originating from the AFHA and PASA have been met. The ASA also demonstrates that for the certification baseline aircraft architecture, the relationships between aircraft functions and systems are acceptable.

The ASA also confirms that the interdependencies between the aircraft functions and systems have been properly identified. The ASA documents that AFHA safety objectives have been met considering the aircraft architecture, cascading failure effects, and external events. The certification baseline aircraft architecture is assessed to demonstrate that the activities necessary to ensure the aircraft requirements and, where applicable, the system-level safety requirements have been satisfied and are complete. The ASA is considered correct and complete when the following analysis and topics have been addressed:

a. Have the aircraft safety program plan objectives been achieved and any deviations accepted?

b. Are the evaluated safety requirements valid and stable based on review of the status of the assumptions, problem reports (open or deferred), and PASA process?

c. Does the aircraft architecture meet the safety requirements (qualitative and quantitative) commensurate with the classifications of all the aircraft-level failure conditions?

d. Do the results of the ZSA, PRA, and CMA verify aircraft independence requirements from the safety assessments are met?

e. Was each assigned FDAL and IDAL requirement appropriately applied throughout development?

f. Does the aircraft architecture meet the development assurance level allocation requirements commensurate with the classifications of all the aircraft-level failure conditions?

SAENORM.COM : Click to view the full PDF of arp4761a

g. Does the aircraft architecture embody the appropriate independence between the members of the Functional Failure Sets (FFS) necessary to support the development assurance level allocation based on CMA?

h. Have assumptions regarding crew actions or responses along with their safety context been compiled and accepted by the relevant stakeholders?

F.5 ASA OUTPUTS

The results of ASA process are documented. As described in Section F.3, these results can be categorized into three groups:

a. Evidence confirming the applicable aircraft safety requirements are valid and stable: F.3.1 through F.3.6 describe assessment of these requirements through review of the aircraft development and safety data. This information is for the analysts' confirmation and only needs to be linked or referenced by the ASA, since many of them may have been documented through other means.

b. Evidence that other analyses (e.g., SSA) used to satisfy aircraft-level safety requirements are completed and reflect the certification configuration. F.3.7.1 and F.3.9 describe activities which are intended to cause the analyst to trace the source of any analysis outside of the ASA. Such data may include:

    1. A status for each validation and verification activity performed. This would include the verification for assigned FDAL/IDAL and aircraft operating procedures.

    2. The status of open/deferred problem reports, their consequences on the aircraft, and their acceptability.

    3. The final list of AFHA failure conditions with references to the evidence addressed in other analyses (e.g., SSA) demonstrating compliance with qualitative and quantitative objectives.

c. Analysis results conducted within the ASA to show the aircraft-level safety requirements are satisfied. This is described in F.3.7.2 and F.3.8 and includes:

    1. The final list of AFHA failure condition addressed within the ASA with the evidence that they are satisfied (i.e., compliance with qualitative and quantitative objectives).

    2. Evaluations for failure conditions assessed in the ASA (see F.3.7.2), including:

        i. MF&MS analysis updated with the final aircraft systems architecture.

        ii. The CMA, PRA, and ZSA results and systems FMEA/FMES or FTAs to the extent they might become ASA artifacts if embodied in the ASA.

        iii. As needed, updates to supporting analyses started in the PASA (e.g., Interdependence Analysis, Combined Functional Failure Effects Analysis).

    3. Assigned FDAL/IDAL updated with results for systems FDAL/IDAL and FFS independence verification activity (see F.3.8).

    4. The status of open/deferred problem reports, their consequences on the aircraft, and their acceptability.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX G - FAULT TREE ANALYSIS (FTA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

G.1 INTRODUCTION ... 114

G.2 SCOPE ... 115

G.3 ROLE OF FTA IN SAFETY ASSESSMENT ... 115

G.4 FAULT TREE SYMBOLS AND DEFINITIONS ... 115

G.5 OVERVIEW OF PERFORMANCE OF FAULT TREE ANALYSIS ... 118

G.6 FTA ANALYSIS DEFINITION ... 118

G.7 UNDESIRED TOP-LEVEL EVENT DETERMINATION ... 120

G.8 SYSTEM INFORMATION COLLECTION ... 121
G.8.1 Review the System Functional Flow Block Diagram ... 121
G.8.2 Review Design Description/Requirement Documentation ... 121

G.9 FAULT TREE CONSTRUCTION ... 121
G.9.1 State the Fault Tree Undesired Top-Level Event ... 121
G.9.2 Develop the Upper and Intermediate Tiers of the Fault Tree ... 122
G.9.3 Extend the Top Event Branches Down to the Primary Events ... 124
G.9.4 Evaluate the Fault Tree for Compliance with Safety Objectives ... 128

G.10 QUALITATIVE FAULT TREE EVALUATION ... 129
G.10.1 Fault Tree Minimal Cut Set Determination ... 129
G.10.2 Qualitative Importance Determination ... 133
G.10.3 FTA Supporting FDAL/IDAL Assignment ... 133

G.11 QUANTITATIVE FAULT TREE EVALUATION USING UNAVAILABILITY METHOD ... 134
G.11.1 Numerical Probability Calculations ... 134
G.11.2 Quantitative Sensitivity Evaluation ... 153

G.12 QUANTITATIVE FAULT TREE EVALUATION BASED ON FAILURE FREQUENCY ... 154
G.12.1 Assumptions Used in Failure Frequency FTA ... 154
G.12.2 Failure Frequency ... 154
G.12.3 Comparison to Unavailability Method ... 157
G.12.4 Sequencing in Fault Trees Using Failure Frequency ... 161
G.12.5 Conversion from Failure Frequency FTA to Unavailability FTA ... 163
G.12.6 Conversion from Unavailability FTA to Failure Frequency FTA ... 164

G.13 ANALYZE AND SUMMARIZE THE FTA RESULTS ... 165
G.13.1 Fault Tree Data Analysis—Normalizing the FTA Numerical Calculation ... 165
G.13.2 Summarizing Fault Tree Analysis Results During SSA/ASA Process ... 165

Figure G1 Fault tree symbols ... 117
Figure G2 Typical FTA undesired event sources ... 120
Figure G3 Upper tier of fault tree-based single versus multiple ... 122
Figure G4 Upper tier of fault tree without single thread in the system ... 123
Figure G5 Upper tier of fault tree considering failure sequence ... 123

SAENORM.COM : Click to view the full PDF of arp4761a

Figure G6 Expanding a fault tree event with respect to fail-safe system elements 124
Figure G7 Example of a fault tree structure when two failures cause a loss of a function 125
Figure G8 Example of a fault tree structure when two failures cause a loss of a function where one could fail latent 126
Figure G9 Example of a fault tree structure when two failures cause a loss of a function where each could fail latent 127
Figure G10 Example of a fault tree structure when two failures cause a top event and one can fail latent and failures are order dependent 128
Figure G11 Fault tree to demonstrate direct analysis techniques 130
Figure G12 Fault tree to demonstrate Boolean reduction techniques 131
Figure G13 Reduced fault tree 132
Figure G14 Error FTA example 134
Figure G15 Potential FTA failure rate data sources 136
Figure G16 Example FTA failure rate units 137
Figure G17 An example of a fault tree structure when the monitor detects 90% of Function “X” Failures 140
Figure G18 An example of a fault tree structure when the monitor detects 90% of Function “X” Failures and the monitor verification is 95% 141
Figure G19 Fault tree model SEE to protected data 142
Figure G20 Fault tree model of persistent SEE with corrective action 143
Figure G21 An example of a fault tree structure which includes Priority AND-gates with ROF 144
Figure G22 Fault tree calculation example when two failures cause a loss of a function 146
Figure G23 Fault tree calculation example when two failures cause a loss of a function where one could fail latent 148
Figure G24 Fault tree calculation example when two failures cause a loss of a function where each could fail latent 149
Figure G25 Fault tree calculation example when failures cause a top event and one can fail latent and failures are order dependent 150
Figure G26 Equation G15 graphical representation 151
Figure G27 Example of a three event AND-gate 156
Figure G28 Example of a fault tree with OR and AND gates 156
Figure G29 Three event fault tree example 157
Figure G30 Fault tree for combination of three events with two having latency 158
Figure G31 Potentially overly simplistic fault tree for a hazardous turbine disc burst 161
Figure G32 Assigning enablers in a combination of failure events 162
Figure G33 FF FTA example where the result of P_f is used when converting to unavailability FTA 163

Table G1 Examples of FTA boundaries 119
Table G2 Sources of top-level events 120
Table G3 Examples of undesired event statements 122
Table G4 Summary of qualitative versus quantitative FTA evaluation techniques and results 129
Table G5 Pictorial representation of average probability calculation for a two failure case—one latent and one active 147
Table G6 Comparison of effect of failure event latency on unavailability FTA (P_f /t) rate and failure frequency 160
Table G7 Comparison of P_f/t results from unavailability and FF fault trees 164
Table G8 Comparison of failure frequency results from unavailability and FF fault trees 165
Table G9 Example of a system indenture level FTA data summary chart 166
Table G10 Example of an LRU indenture level FTA data summary chart 166

SAENORM.COM : Click to view the full PDF of arp4761a

G.1 INTRODUCTION

A Fault Tree Analysis (FTA) is a deductive failure analysis which focuses on one particular undesired event and provides a method for determining causes of this event. In other words, an FTA is a top-down system evaluation procedure in which a qualitative model for a particular undesired event is formed and then evaluated. The analyst begins with an undesired top-level hazard event and systematically determines all credible single failures and failure combinations of the system functional blocks at the next lower level which could cause this event. The analysis proceeds down through successively more detailed (i.e., lower) levels of the design until a primary event is uncovered or until the fault tree shows support of the undesired event under evaluation. A primary event is defined as an event which for one reason or another has not been further developed (i.e., the event does not need to be broken down to a finer level of detail in order to show that the system under analysis complies with applicable safety requirements). A primary event may be internal or external to the system under analysis.

The fault tree graphical representation is hierarchical and takes its name from the branching that it displays. It is this analysis format which enhances the reviewability by both engineering and the Certification Authority. As one of a family of safety assessment techniques for assuring that the system/equipment will accomplish its intended safety functions, FTA is concerned with ensuring that design safety aspects are identified and controlled.

FTA usage includes:

a. Facilitation of technical/Certification Authority assessments and reviews. (The completed fault tree displays only the failure events which could individually or collectively lead to the occurrence of the undesired top event.)

b. Assessment of a design modification with regards to its impact on safety.

c. Quantification of the top event probability of occurrence.

d. Allocation of probability budgets to lower-level events.

e. Identification of Functional Failure Sets showing development errors to support allocation of FDAL/IDAL.

f. Identification of single failures and failure combinations that result in the failure condition under evaluation.

g. Assessment of exposure intervals, latency, and “at risk” intervals with regard to their overall impact on the safety of the system.

h. Visibility of potential common cause boundaries.

i. Assessment of common cause failure sources.

j. Assessment of fail-safe design attributes (fault-tolerant and error-tolerant).

This appendix describes two FTA methodologies: unavailability and failure frequency. Sections G.1 through G.10, G.11.1.1 to G11.1.4, and G.13 are aspects of FTA common to both methodologies. Section G.11 describes performing an FTA evaluation using the unavailability method while Section G.12 describes FTA evaluation using the failure frequency method.

There may be occasions when a fault tree has been performed by one company (e.g., supplier) using one of the two methods (i.e., unavailability or failure frequency) and this fault tree is then provided to another company (e.g., customer) for use in a higher-level fault tree. It is important to understand the mathematical relationships when extracting and integrating quantitative values between the two methods. G.12.5 and G.12.6 discuss this in more detail.

SAENORM.COM : Click to view the full PDF of arp4761a

G.2 SCOPE

This Fault Tree Analysis appendix contains the background information and procedural guidelines necessary for an experienced engineer to perform an FTA for the first time. Although this appendix contains the basic information on FTAs, the reader may also wish to refer to NUREG-0492, Fault Tree Handbook, U.S. Nuclear Regulatory Commission, and other published material for a detailed discussion of FTA structure and mathematical evaluation techniques.

G.3 ROLE OF FTA IN SAFETY ASSESSMENT

Fault Tree Analysis may be performed during system conception in support of the PASA/PSSA process as described in the main body 3.3 and 3.5. An FTA may also be performed in support of the safety verification effort as part of the SSA/ASA process described in main body 3.6 and 3.7. A top-down analysis like FTA allows for its level of detail to match the proposed or current level of design detail respectively.

FTA can be used throughout the design process to evaluate the ability of the proposed system to meet the safety objectives and requirements. This can be high-level fault trees during conceptual design to final fault trees to support certification.

FTA revisions after a design freeze are dictated by the level of the design change. Since ASA/SSA fault trees represent the implemented hardware, the FTA may require updating if a hardware design change causes a change in the failure rate for the hardware. The FTA may also require updating if a design change impacts how hardware failures may contribute to the failure condition under evaluation. The FTAs should be reviewed again during the latter stages of the aircraft flight program. FTAs which include any equipment design changes resulting from the aircraft test program are usually required as part of the equipment certification supporting documentation.

For example, an early FTA may be performed to qualitatively model a failure condition and the combined events that can cause it to occur. As the design progresses, iterations may include fault tree updates due to rework or clarification of some of the analyst's initial assumptions as the result of the requirement capture and validation process. In support of the PSSA/PASA process, allocation of probability budgets to lower-level events may be included in these fault trees. As the design progresses and more knowledge is gained during preliminary hardware or software detailed design, preliminary failure rate information may be inserted into the fault tree primary events and the top-level event failure probability calculated and compared to the applicable safety requirement as part of the equipment design review process. Iterations can be made to evaluate hardware or software changes due to problems uncovered during prototype or verification testing. A "final tree" can be made that represents the implemented system including changes resulting from remaining verification testing or flight test, based on the corrective actions applied to the implementation. This version of the fault tree then becomes part of the SSA documentation used to support the certification program milestone.

G.4 FAULT TREE SYMBOLS AND DEFINITIONS

All fault trees are composed of two kinds of symbols: logic and event. The general rule with regard to symbols is keep it simple; the fewer the different symbol types used, the easier it will be for a person reviewing the fault tree to understand it. Logic symbols are used to tie together the various branches of the fault tree.

The two main logic symbols used are the Boolean logic AND-gates and OR-gates. The analyst selects an AND-gate when the upper-level event can only occur when all the next lower conditions are true. The OR-gate is used when the event can occur if any one or more of the next lower conditions are true. The analyst may also use other Boolean logic gates if the system architecture warrants the use of these gate types.

Event symbols most commonly used include a rectangle, triangle, oval, circle, house, and diamond (see Figure G1). A rectangle contains the description of a logic symbol output or an event. A triangle indicates a transfer of information and is composed of two types. A triangle with a vertical line from its top represents a fault tree section (events and their corresponding probability of occurrence) which is "transferred in." A triangle with a horizontal line from its side indicates that the event the triangle is tied to is "transferred out" to another branch of the tree. The oval represents a conditional event which defines a necessary condition for a failure mode to occur (usually used in conjunction with Priority AND and Inhibit gates). For example, "monitor fails first" is a conditional event because it is necessary before corrupt data can be propagated through the system undetected.

SAENORM.COM : Click to view the full PDF of arp4761a

The circle, house, and diamond all represent types of primary events (i.e., basic events, external events, and undeveloped events). A circle signifies a basic event. A basic event is defined as an event which is internal to the system under analysis, requires no further development (i.e., has the capability of causing a fault to occur), and for hardware elements only, can be assigned a failure rate budget or an actual failure rate from an FMES or other source necessary for quantitative evaluation.

A house event is an event which is normally expected to occur. This house event has the following two possible states:

a. The event has occurred.

b. The event will not occur during the period under investigation.

A house event functions like a switch and is used to include or exclude parts of the fault tree, which may or may not apply to certain situations.

A diamond signifies an undeveloped event. An undeveloped event is defined as an event which is not developed further because it has negligible impact on the top-level event or because the details necessary for further event development are not readily available. Often these types of events are added to a fault tree in order to make the fault tree “complete” from a qualitative model point of view.

Many FTA computer software packages also have additional symbols which are usually unique to that particular FTA software package. The analyst may use other symbols which do not appear in Figure G1 if the symbols are properly defined.

Mathematical symbols that are used in this appendix include:

λ = failure rate per hour

T = check interval (units of time)

t = the exposure time or “at risk” time associated with the particular primary event (units of time)

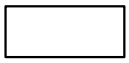
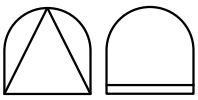
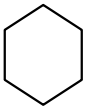
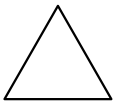
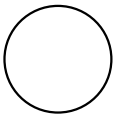
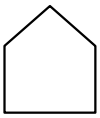
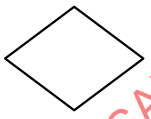
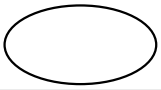
P or P_t = probability of the event or failure occurring during the time t or T

w or w(t) = failure frequency per hour

“At risk” time is the period of time during which the aircraft may be subject to the failure effect under analysis.

Exposure time is the period of time between when a system or equipment was last known to be operating properly and when it will be known to be operating properly again.

SAENORM.COM : Click to view the full PDF of arp4761a

Symbol	Name	Definition
	Description Box	Description of an output of a logic symbol or of an event
	AND-Gate	Boolean Logic gate – event can occur when all the next lower conditions are true
	Priority AND-Gate	Boolean Logic gate – event can occur when all the next lower conditions occur in specific sequence (sequence is usually represented by a conditional event)
	OR-Gate	Boolean Logic gate – event can occur if any one or more of the next lower conditions are true
	Inhibit	Output fault occurs if the (single) input fault occurs in the presence of an enabling conditional event
	Transfer	Indicates transfer of information
	Basic Event	Event which is internal to the system under analysis, requires no further development
	House	Event which is external to the system under analysis, it will or will not happen (P_f=1 or P_f=0)
	Undeveloped Event	Event which is not developed further because it has little impact on the top level event or because the details necessary for further event development are not readily available
	Conditional Event	A condition which is necessary for a failure mode to occur

SAENORM.COM : Click to view the full PDF of arp4761a

Figure G1 - Fault tree symbols

G.5 OVERVIEW OF PERFORMANCE OF FAULT TREE ANALYSIS

Performing an FTA requires six basic steps.

a. Define the goal and depth of analysis for the FTA.

   Be specific: Will the fault tree be used to determine failure event budgets or for FDAL/IDAL assignments (part of a PASA/PSSA process)? Will it be used to verify system design compliance with established safety requirements (part of the SSA/ASA process)? Will the fault tree be evaluated qualitatively, quantitatively, or both? Defining the FTA goal helps the analyst determine the scope of the FTA.

b. Define the analysis boundaries required.

   Will the system be subdivided in order to perform multi-level FTAs? Knowing the boundaries of the analysis is important for determining the scope of the FTA and for defining how the FTA results will be reported (i.e., tie in closely with step e). Section G.6 contains more information on the analysis definition.

c. Define the undesired event.

   An undesired event includes a statement of the failure condition being evaluated and any context in which the undesired event results directly in the specific effects associated with the severity identified in the FHA. This undesired event can either be tied directly to an FHA or it can be tied to a primary event in another fault tree if the system has been subdivided into multiple levels (i.e., alignment of boundaries in multi-level FTAs). If the undesired event is a subdivision of a larger event, then take care when combining the sub-trees back together. All sub-trees so combined need to be reviewed for independence before combining them in a new fault tree. A probability of failure budget for the undesired event may also be stated. Section G.7 contains more information on defining undesired events.

d. Gather the most complete system data available at the time and analyze it to determine the possible fault and failure events and event combinations which lead to the top event.

   Section G.8 contains more information on this step.

e. Construct the fault tree associated with the undesired event from step c.

   Section G.9 contains information on fault tree construction.

f. Analyze and summarize the FTA results.

   Sections G.10 through G.13 contain more information on analyzing fault trees and summarizing their results.

G.6 FTA ANALYSIS DEFINITION

The fault tree can be used to accomplish these main goals:

a. In the PASA/PSSA process:

   1. Allocate the probability of failure (P_f) (also known as P_f budgeting) when working with P_f quantitative objectives. Budgeted failure probabilities in a PASA/PSSA fault tree can be tighter (i.e., a lower probability) than the probability number required to meet the top event probability objective.

   2. Identify safety requirements to support mitigation of failure conditions.

   3. Identify Functional Failure Sets as part of the FDAL/IDAL assignment.

b. In the SSA/ASA process:

   1. Verify that safety objectives and/or requirements are achieved.

SAENORM.COM : Click to view the full PDF of arp4761a

The analyst can create fault trees for any development indenture level (i.e., aircraft, system, equipment). An indenture level is defined as any one level within a multi-level FTA. The analyst will need to determine the boundary for the FTA. The boundary will be subjectively based on what the analyst wants or needs to accomplish by performing the FTA. Table G1 lists several possible indenture levels and their potential boundaries. Note that the information presented in the "FTA Boundary" column indicates one potential boundary of the analysis (i.e., the lowest level of design detail that the analyst will consider when performing the top-down FTA). The analyst should choose the boundaries based on the scope of analysis. The following elements may be considered:

a. What are the system inputs and outputs?

b. What external system contributions are to be included?

The selected FTA boundary ties in closely with how the fault tree evaluation results are reported.

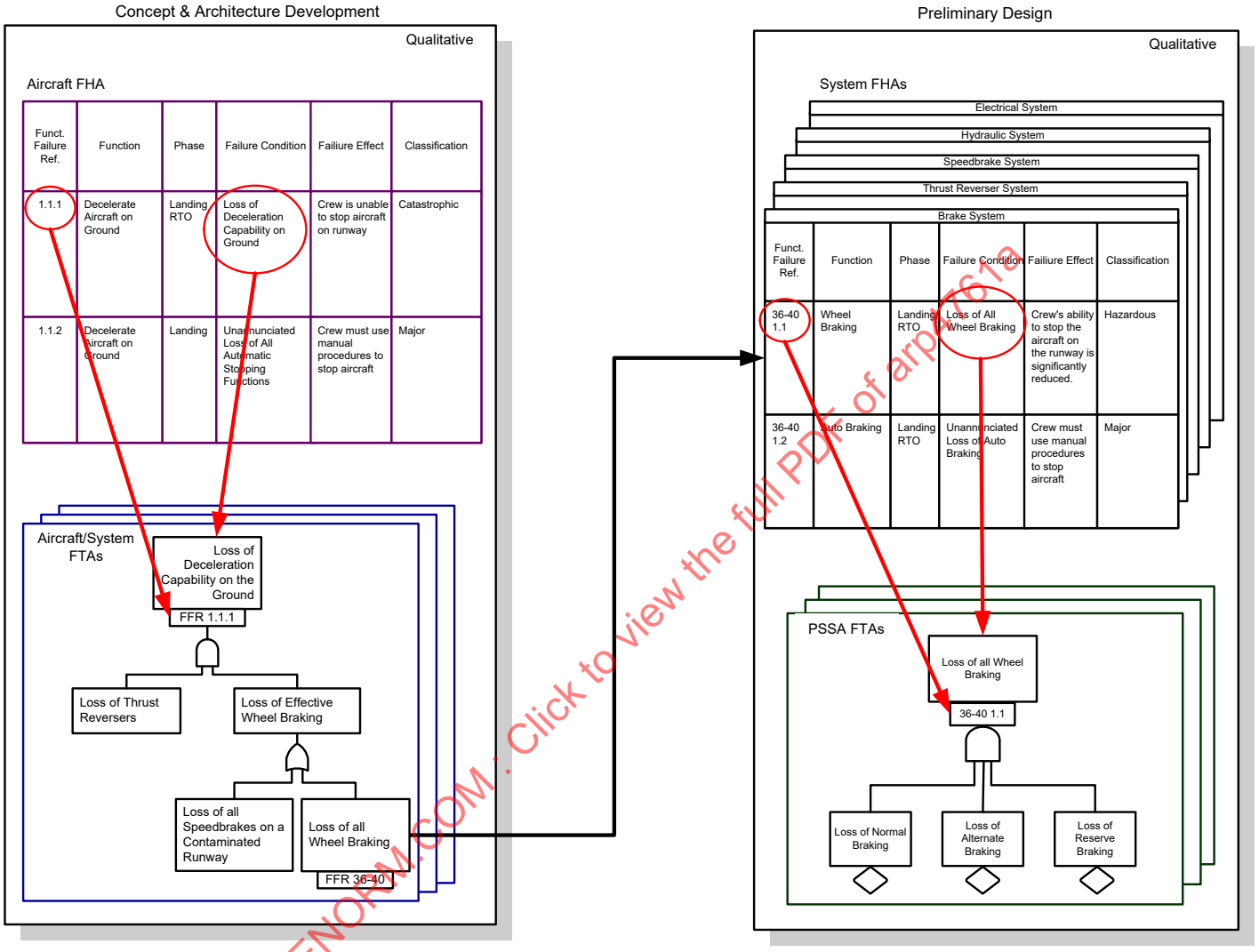
Table G1 - Examples of FTA boundaries

FTA Indenture Level	FTA Boundary	Characteristics of FTA at This Indenture Level
Aircraft	Aircraft block diagram	AFHA/PASA: P_f budgeting to the various major systems composing an A/C level function.
		ASA: Identification of failure effects and probabilities from SSAs causing or contributing to A/C level failure conditions.
System	System block diagram	SFHA/PSSA: P_f budgeting to the subsystems within the system and interface systems with the system under consideration.
		SSA: Use of subsystem failure rates (taken directly from reliability prediction analysis, equipment-level safety assessment or an FMEA/FMES) and interface system failure rates for primary event quantitative evaluation.
Subsystem (i.e., equipment)	Subsystem functional block diagram	PSSA: P_f budgeting to the various blocks within the subsystem (i.e., allocation to hardware and software functions).
		SSA: Use of failure rates for specific groups of circuitry of interest (e.g., failure rate of core processor function—CPU, oscillators, memory) when the entire failure rate is too large to demonstrate compliance with safety requirements during quantitative evaluation. Failure rates from an FMEA or FMES may also be used.
Subsystem Functional Block	Hardware schematics	PSSA: P_f budgeting to the various functional circuitry and their respective monitors, within the subsystem functional blocks. Allocation of IDAL to software functional elements.
		SSA: Use of failure rates for specific components of interest (e.g., failure rate of ARINC 429 receiver) when the failure rate for a group of circuitry causes non-compliance with safety requirements during a quantitative evaluation. The analyst is able to take advantage of hardware component failure modes and their percentage of occurrence. Failure modes and rates from an FMEA or FMES may also be used.

SAENORM.COM : Click to view the full PDF of arp4761a

G.7 UNDESIRED TOP-LEVEL EVENT DETERMINATION

The analyst compiles a list of undesired events. Each undesired event will become the top-level event in a fault tree. Depending on the system indenture level the analyst is dealing with, these top-level events can have different origins. Figure G2 highlights two typical sources of undesired events, the AFHA and the SFHA, and the linkages into FTA structures.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure G2 - Typical FTA undesired event sources

Table G2 describes some of the other top-level event sources based on the safety assessment process diagram presented in the main body of this document.

Table G2 - Sources of top-level events

FTA Indenture Level	Origin of Top-Level Events
Aircraft	AFHA
System	SFHA and/or PASA and/or AFHA (when the aircraft function is implemented by only the system under assessment)
Subsystem	System FTA
Subsystem Functional Block	Subsystem FTA

G.8 SYSTEM INFORMATION COLLECTION

The analyst should gather the most complete and current system data available. The analyst should analyze the data to determine the possible failure events and combinations which lead to the top event. The analyst obtains the information from two main sources:

a. System functional flow block diagrams.

b. Design description documentation or design requirement documentation.

G.8.1 Review the System Functional Flow Block Diagram

The analyst should review the system functional flow block diagram. The system functional flow block diagram includes information on flight success criteria and system inter-dependencies. The word “system” in this context can refer to any grouping of aircraft or support equipment; e.g., propulsion system, engine subsystem, or autopilot Line Replaceable Unit (LRU). The analyst should have detailed knowledge of the system to be analyzed in order to determine the single failures and combinations of failures which could cause the top-level event for that particular tree to occur.

G.8.2 Review Design Description/Requirement Documentation

The analyst should gather all existing system data and analyze it to determine the possible failure events and combinations which could lead to the top-level event for that particular tree. Possible sources include the system architecture description documents, the various system, hardware, and software design specifications and description documents, and the designer/analyst’s own intimate knowledge of the system.

G.9 FAULT TREE CONSTRUCTION

The following four steps should be followed for constructing a fault tree.

a. State the undesired top-level event (and its probability of failure objective or failure rate objective, if applicable) in a clear, concise statement.

b. Develop the upper and intermediate tiers of the fault tree, determine the intermediate failures and combinations which are minimum, immediate, necessary, and sufficient to cause the top-level event to occur and interconnect them by the appropriate fault tree logic symbols. Extend each fault event to the next lower level.

c. Develop each fault event down through successively more detailed levels of the system design until the root causes are established or until further development is deemed unnecessary.

d. Either:

   1. Establish probability of failure budgets or failure rate budgets, including potential impact of Single Event Effects (SEE) susceptible devices if including SEE in the fault tree, evaluate the ability of the system to comply with the safety objectives, and initiate a redesign the system if deemed necessary (PASA/PSSA process).

      or

   2. Evaluate the fault tree in either a qualitative and/or quantitative manner (SSA/ASA process).

G.9.1 State the Fault Tree Undesired Top-Level Event

This section addresses the first fault tree construction step: State the undesired top-level event (and its probability of failure objective if applicable) in a clear, concise statement.

The analyst enters the fault tree top-level event into a description box. This statement identifies what the undesired event is and when it occurs. For a majority of the fault trees, this top-level event is already identified in an FHA or in another higher-level fault tree and just needs to be copied into the rectangular event symbol. In other cases, the analyst needs to clarify the undesired event statement before placing it into the description box.

SAENORM.COM : Click to view the full PDF of arp4761a

The undesired top-level event should be clearly and concisely stated because it sets the tone for the series of questions the analyst asks when constructing the various fault tree levels. Table G3 provides some examples of poorly worded and revised top-level event statements for SSA/ASA FTAs. During PASA/PSSA, the type of information stated in the "Revised Statement" column may not be available.

Table G3 - Examples of undesired event statements

Poorly Worded Statement	Problem with Statement	Revised Statement
Loss of airspeed indication.	Too vague as to "what" the fault is—does it mean loss of primary airspeed, loss of secondary airspeed, or loss of both?	Loss of all airspeed display in the flight deck.
Display of misleading approach data without annunciation of failure.	Too vague as to where the fault occurs—is it on both navigation displays or only one?	Display of misleading approach data on both navigation displays without annunciation of failure.
Display of misleading attitude on a single pilot's primary flight display, without annunciation of failure.	States "what" but not "when"—if considered during cruise, this event has a failure condition classification of Major. If considered during takeoff after rotation, this event has a failure classification of Hazardous. "When" defines the time period used with respect to P_f during a quantitative evaluation.	Display of misleading attitude on a single pilot's primary flight display, without annunciation of failure during takeoff after rotation.

G.9.2 Develop the Upper and Intermediate Tiers of the Fault Tree

This section addresses the second fault tree construction step: Develop the upper and intermediate tiers of the fault tree, determine the intermediate failures and combinations of failures which are necessary and sufficient to cause the top-level event to occur and interconnect them by the appropriate, conventional fault tree logic symbols. Extend each fault event to the next lower level.

Each fault tree will start with a top-level event for that particular fault tree which is a previously defined event (see G.9.1). If there are known single failures, the fault tree can be constructed as shown in Figure G3.

SAENORM.COM : Click to view the full PDF of arp4761a

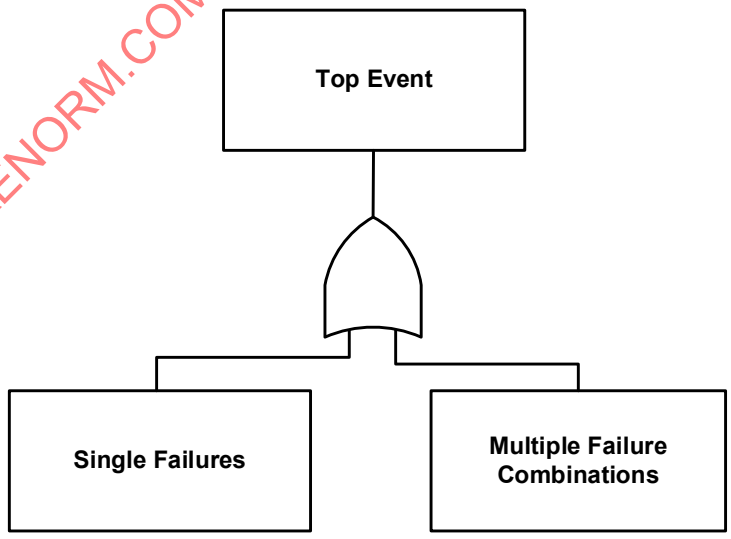


Figure G3 - Upper tier of fault tree-based single versus multiple

If there are no known single failures, the fault tree first tier might be drawn like Figure G4.

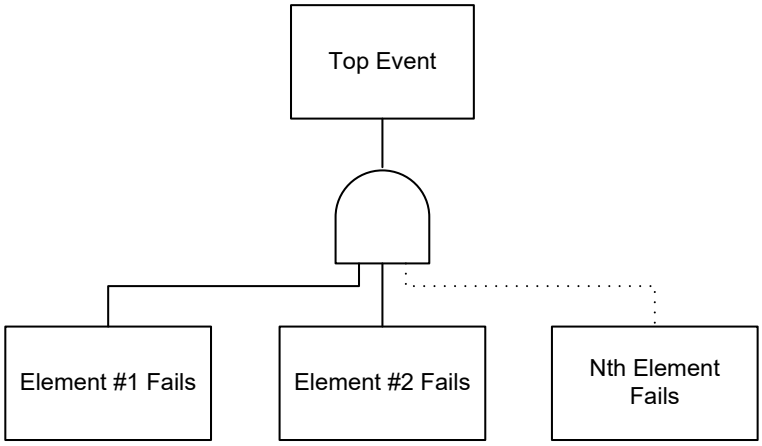


Figure G4 - Upper tier of fault tree without single thread in the system

Multiple failure combinations may be dependent on a specific order in which they fail. These events are then defined as failure order dependent events (also known as sequential events). Failure order dependent events should be drawn as inputs into an AND-gate from left to right in the order in which they must fail. If, in Figure G4, the first and second elements of the system must fail prior to the Nth element in order for the event to occur, then the AND-gate may include another undeveloped event input which represents the probability that the “n” elements will fail in that order. Another way to represent failure order events dependent events is to use a Priority AND-gate along with a conditional event. For details and limitations, see also G.11.1.4.

For example, assume the above system has three elements (N = 3). The fault tree first tier would be drawn as in Figure G5.

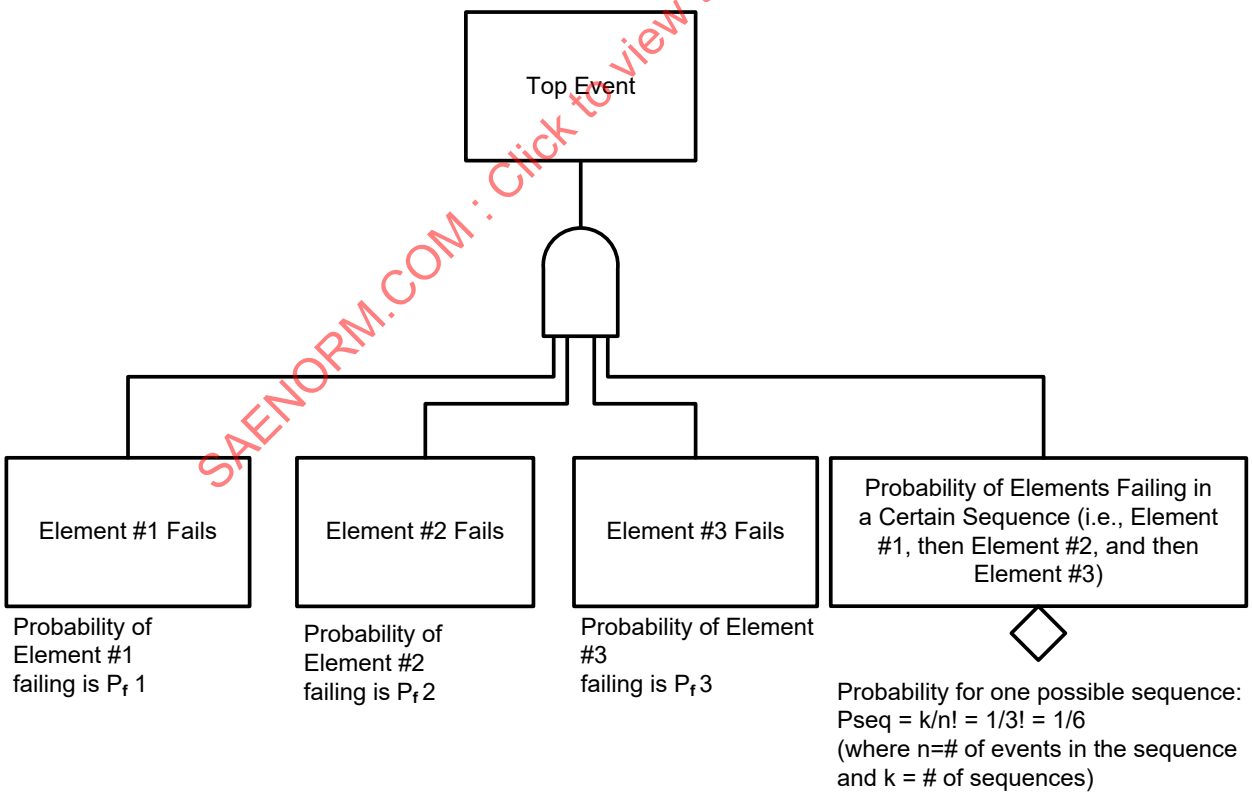


Figure G5 - Upper tier of fault tree considering failure sequence

SAENORM.COM : Click to view the full PDF of arp4761a

The n! (factorial) term represents the number of event sequences which could occur. For this example, the possible event sequences are $P_f1P_f2P_f3$, $P_f1P_f3P_f2$, $P_f2P_f3P_f1$, $P_f2P_f1P_f3$, $P_f3P_f1P_f2$, and $P_f3P_f2P_f1$. See G.11.1.4 for further discussion of required order factors (ROF).

Next, the analyst will expand the tree by working top-down while considering the above questions for the event or failure effect, as it is also referred to, at each new level. When considering events based on multiple failures, the analyst should consider contributions from incorrect outputs and inoperative protective or reconfiguration mechanisms as shown in Figure G6.

Throughout the fault tree construction effort, the analyst should make sure that a pre-defined naming convention is followed so everyone working on a given system creates the fault trees in the same manner. When selecting a naming convention, the analyst should keep in mind three things.

a. The naming convention should prevent conflicts between events; i.e., no two different events can have the same name and identical events must have the same name. This is crucial for proper Boolean algebra reduction.

b. The naming convention should not be too cryptic or someone looking at the tree will have to constantly refer to some sort of table in order to decipher the name.

c. The naming convention should be maintainable. For example, set up the naming convention with ample growth potential so that you do not have to go back and re-name all events because your convention does not allow you to add several new events at a later date.

SAENORM.COM : Click to view the full PDF of arp4761a

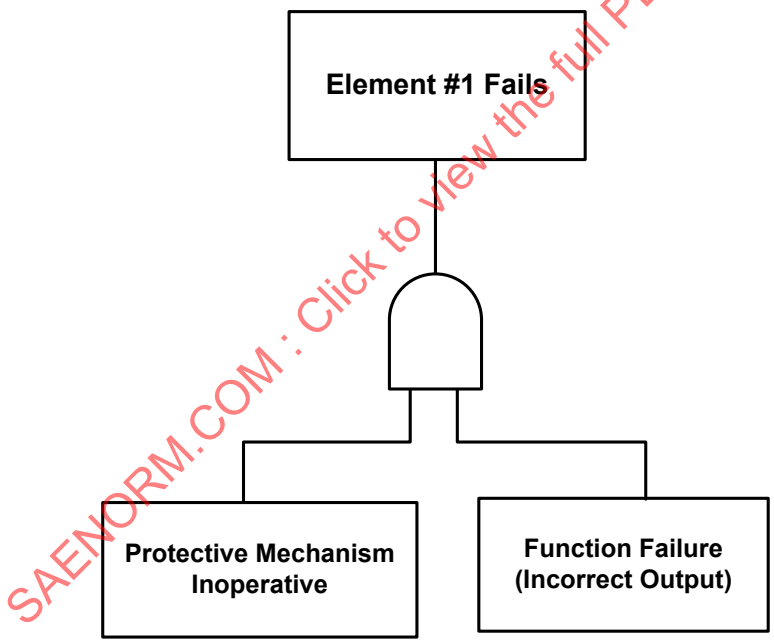


Figure G6 - Expanding a fault tree event with respect to fail-safe system elements

If a software FTA package is used to construct the trees, this pre-defined naming convention must be compatible with the software package. Some software packages require gates to be named in order to identify the intermediate events which are outputs of logic gates.

G.9.3 Extend the Top Event Branches Down to the Primary Events

This section addresses the third fault tree construction step: Develop each fault event down through successively more detailed levels of the system design until root causes are established or until further development is deemed unnecessary.

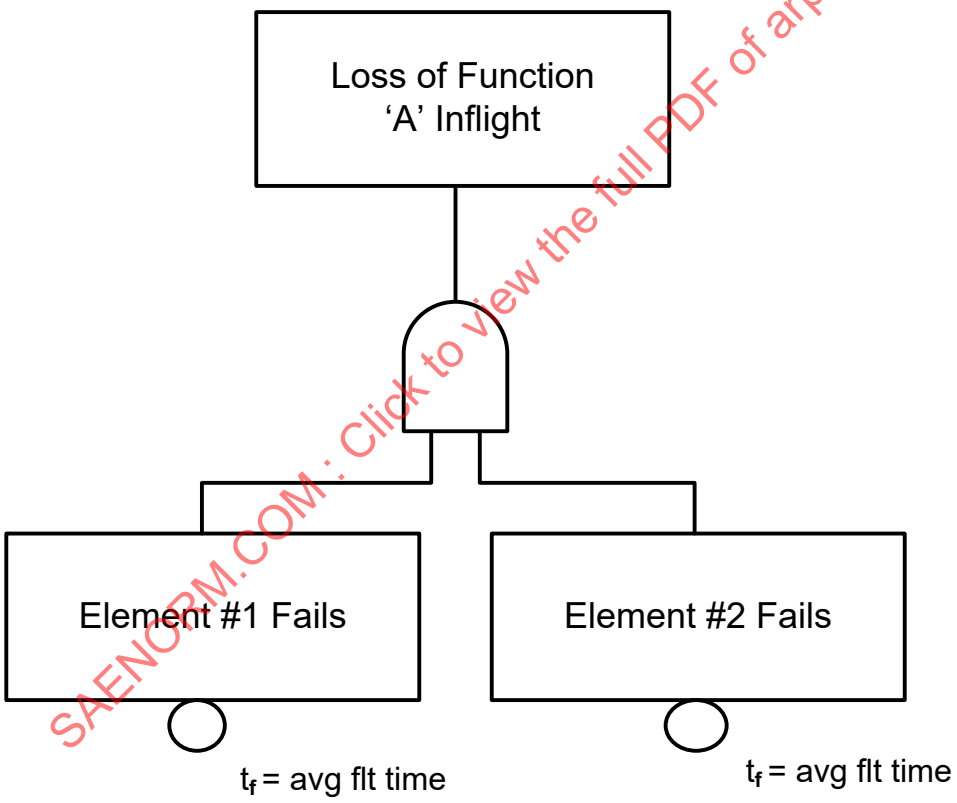
The analyst should further develop and complete the fault tree by extending the fault tree branches down to the primary events. These primary events are the root causes of the first level fault events. The fault tree should be developed such that repeated primary events are identified across multiple branches.

The root cause will be a hardware failure, external event, or undeveloped event broken down to a level of detail necessary to demonstrate system design compliance with safety objectives. Here is where the goal of the FTA becomes apparent with its impact on the FTA scope. If the FTA goal is a qualitative evaluation, gathering further information on the primary event may not be necessary. If the FTA goal is a quantitative evaluation, the analyst should gather more detailed information on the primary event (hardware failure rates and “at risk” or exposure times). In either case, if the analyst stops developing the tree before all of the recurring events are discovered then the qualitative and quantitative FTA may provide an incorrect result. If the fault tree depth is truncated, the analyst should provide justification for the claim that any resulting loss of accuracy does not affect the analysis result (e.g., due to potential common causes).

In this appendix, four particular examples are developed to show typical fault tree representations which include basic events with or without latency and required order factors. The detailed mathematical calculations are further explained in G.11.1.5.

G.9.3.1 Example When Two Failures Cause a Loss of a Function

The first example fault tree shown in Figure G7 shows the simple failure case where the top event is caused by the loss of both elements during the same flight (note that t_f is the average flight time). Both elements are known to be operating at the start of the flight and neither fail latent. The two failures can occur in either order.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure G7 - Example of a fault tree structure when two failures cause a loss of a function

G.9.3.2 Example When Two Failures Cause a Loss of a Function Where One Could Fail Latent

In the second example, Element #1 can fail at any point between when it is checked (time = zero) and when it is next checked (time = T_1). Element #2 is known to be operating at the start of each flight and never fails latent. The order of failure does not matter. An example fault tree is shown in Figure G8.

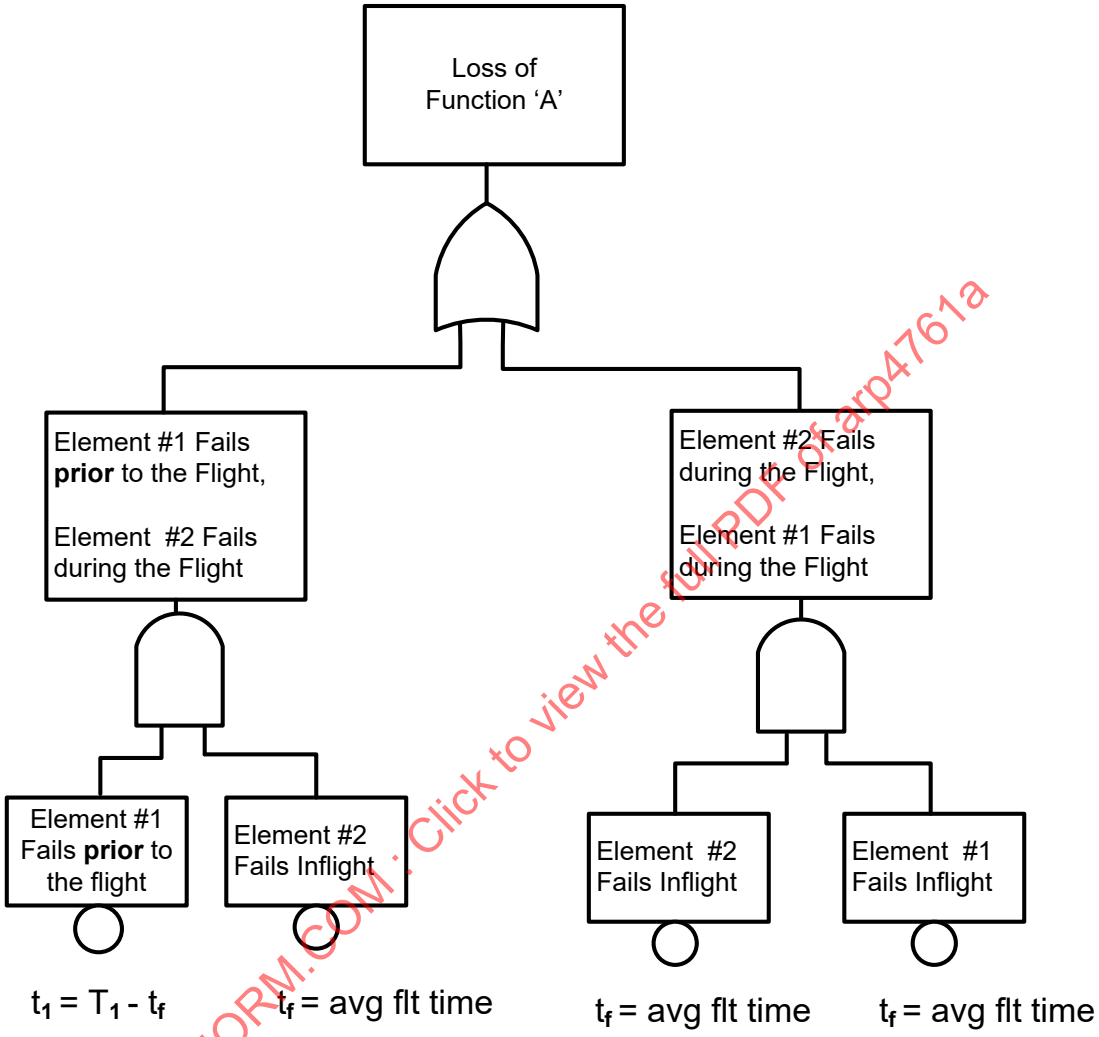


Figure G8 - Example of a fault tree structure when two failures cause a loss of a function where one could fail latent

SAENORM.COM : Click to view the full PDF of arp4761a

G.9.3.3 Example When Two Failures Cause a Loss of a Function Where Each Could Fail Latent

In the third example, either element could fail latent, but if both fail, this would be detected by virtue of it causing the top event. Therefore, at least one of the elements must be operating at the start of each flight. An example fault tree is shown in Figure G9. Three things should be noted about this figure:

a. An undeveloped event for failure order (i.e., ROF = k/n! as shown in Figure G5 and further described in G.11.1.4) is not required because failure order dependence is built into the tree structure via the latency period (Equation G1). This is representative of a failure during the latency period before the flight.

$$\text{Latency period: } t_n = T_n - t_f \qquad \text{(Eq. G1)}$$

Where T_n = check interval (T_1 and T_2)

t_f = exposure time

b. The right-most AND-gate is necessary to cover the case that both elements fail during the flight without a required sequence.

c. The right-most AND-gate in Figure G9 is often omitted and the exposure times set equal to the inspection intervals, for cases where t_f is much less than the inspection intervals.

SAENORM.COM : Click to view the full PDF of arp4761a

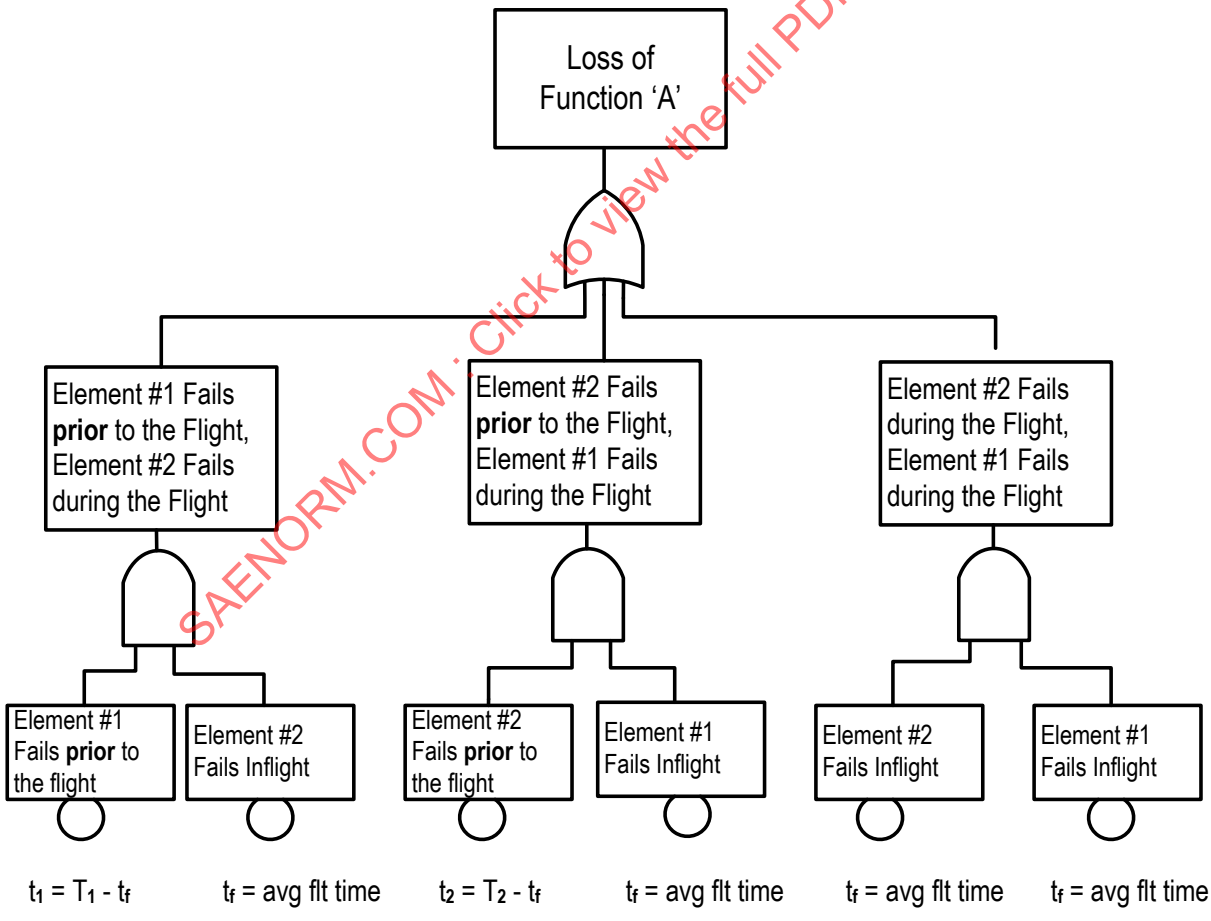


Figure G9 - Example of a fault tree structure when two failures cause a loss of a function where each could fail latent

G.9.3.4 Example When Two Failures Cause a Top Event and One Could Fail Latent and Failures are Order Dependent

In the fourth example, Element #1 (the latent one) must fail prior to Element #2 or the top event does not result. Element #2 is known to be operational at the start of the flight. This is typical of a failure/monitor situation where the top event is an erroneous output rather than a loss of function. An example involving the transmission of incorrect data is provided in Figure G10.

The required order factor is used per G.11.1.4.

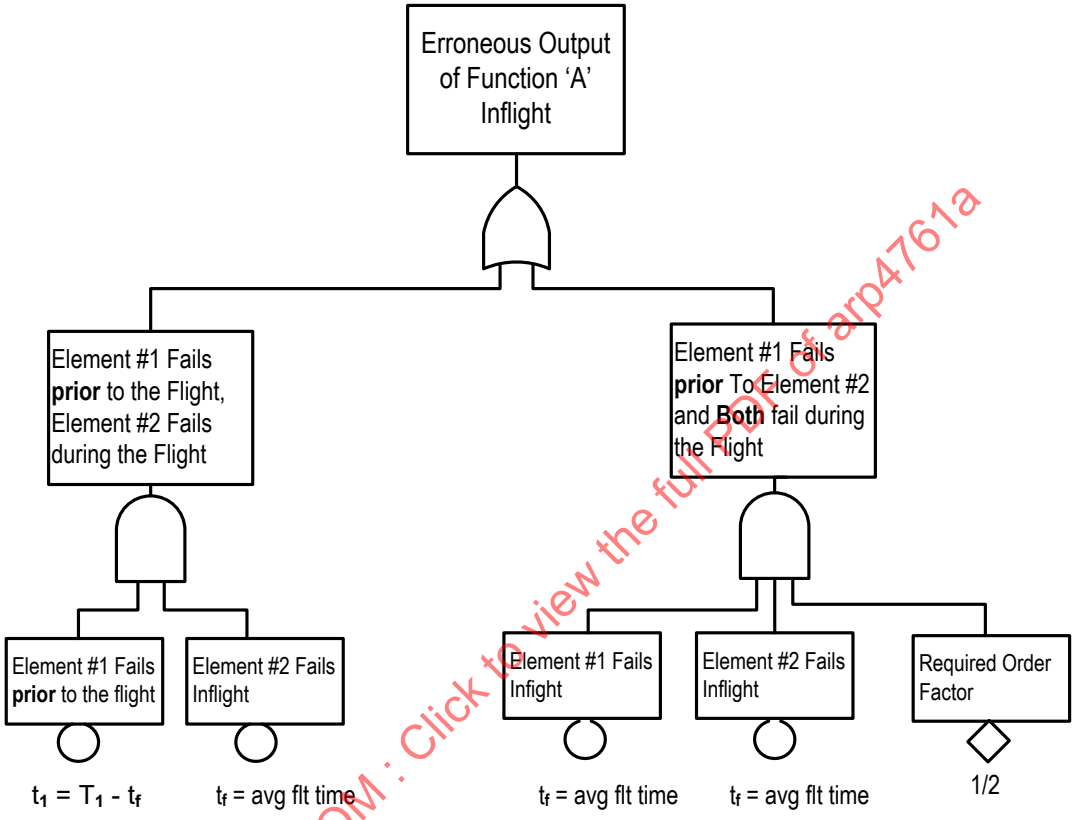


Figure G10 - Example of a fault tree structure when two failures cause a top event and one can fail latent and failures are order dependent

SAENORM.COM : Click to view the full PDF of arp4761a

G.9.4 Evaluate the Fault Tree for Compliance with Safety Objectives

This section addresses the fourth fault tree construction step: Evaluate the fault tree in either a qualitative or quantitative manner.

Fault trees are qualitative models by nature of their construction. Depending on the goal of the FTA, the analyst will evaluate the fault tree in a qualitative or qualitative and quantitative fashion. Table G4 summarizes the results of the two evaluation methods. The analyst may find this table useful when determining the FTA goal. Qualitative evaluation and quantitative evaluation are further described in Sections G.10 and G.11, respectively.

Table G4 - Summary of qualitative versus quantitative FTA evaluation techniques and results

Qualitative	Quantitative
Minimal cut sets (MCSs): Minimal combination of primary events causing the top event	Numeric probabilities: Probabilities of system and cut set failures
Qualitative importance: Qualitative ranking of contributions to system failures, direct cause versus contributory via fail-safe	Quantitative importance: Quantitative ranking of contributions to system failure
Common cause potentials: MCSs potentially susceptible to a single failure cause	Sensitivity evaluations: Effects of changes in models and data on numerical probability

G.10 QUALITATIVE FAULT TREE EVALUATION

The qualitative fault tree evaluation produces minimal cut sets (MCSs). These can be used to determine the qualitative importance and to evaluate common cause potentials.

The following sections provide the minimal amount of information needed to understand the subject matter. For a more detailed and complete explanation of these techniques, refer to NUREG-0492 or one of many similar books on the subject of fault tree evaluation.

G.10.1 Fault Tree Minimal Cut Set Determination

A fault tree MCS is a set of primary events where removing any single primary event no longer results in the top event.

The analyst should be aware of the potential lack of independence between two or more primary events in order to avoid serious errors in qualitative and quantitative analysis. This lack of independence can occur whenever the same event appears in more than one location in the fault tree or when certain single failures can result in more than one failure event simultaneously. When dependence is known, it is modeled by the same event (or the same gate) appearing at more than one place in the fault tree and is handled correctly by the application of Boolean algebra to generate the cut sets. Take care when in a high-level tree (where the primary events are derived as top-level events from separate FTAs), an event can appear in more than one of those separate fault trees. If this happens, the dependence will not be visible in the high-level tree and the probability calculation for the high-level tree will be incorrect. To obtain accurate calculations in this case, it is necessary to replace the derived primary events with their corresponding detailed fault tree structure. Accuracy can also be obtained by an adding an OR-gate with the common events above the AND-gate. This allows the common events to be correctly modeled throughout the high-level fault tree so that accurate cut set listings and probability calculations can be obtained.

The analyst may use “direct analysis” on the fault tree when the various primary events only appear once in that given tree. However, for most civil airborne systems, this is not the case. The logic symbol dictates how the calculation will be performed based on the following probability calculus basic rules. (NUREG-0492 addresses this subject in greater detail.)

a. The probability of obtaining an outcome A is denoted by P(A), outcome B by P(B), and so on for other outcomes.

b. The probability that A AND B occur is denoted by P(AB).

c. The probability that A OR B occurs is denoted by P(A+B).

d. If A and B are two independent events with the probabilities P(A) and P(B), then the probability that both events will occur is the product:

   P(AB) = P(A) * P(B) — applies to two input AND-gates.

e. If A, B, and C are three independent events with the probabilities P(A), P(B), and P(C), then the probability that all three events will occur is the product:

   P(ABC) = P(A) * P(B) * P(C) — applies to three input AND-gates

f. The same logic can be carried to four or more independent events.

SAENORM.COM : Click to view the full PDF of arp4761a

g. If the two independent events can occur simultaneously, the probability that either A OR B or both A AND B will occur is:

P(A+B) = P(A) + P(B) - [P(A) * P(B)] — applies to two input OR-gates.

h. If the three independent events can occur simultaneously, the probability that A OR B OR C, or any combination of these three will occur is:

P(A+B+C) = P(A) + P(B) + P(C) - [P(A) * P(B)] - [P(A) * P(C)] - [P(B) * P(C)] + [P(A) * P(B) * P(C)] — applies to three input OR-gates.

The same logic can be carried to four or more independent events.

i. If the two events are mutually exclusive so that when one occurs the other cannot occur, the equation for a two input OR-gate simplifies to:

P(A+B) = P(A) + P(B) — furthermore, P(AB) = 0

This equation is also good approximation for two non-mutually exclusive events with low probabilities, which errs on the conservative side.

For a “direct analysis” example, consider the fault tree in Figure G11.

SAENORM.COM : Click to view the full PDF of arp4761a

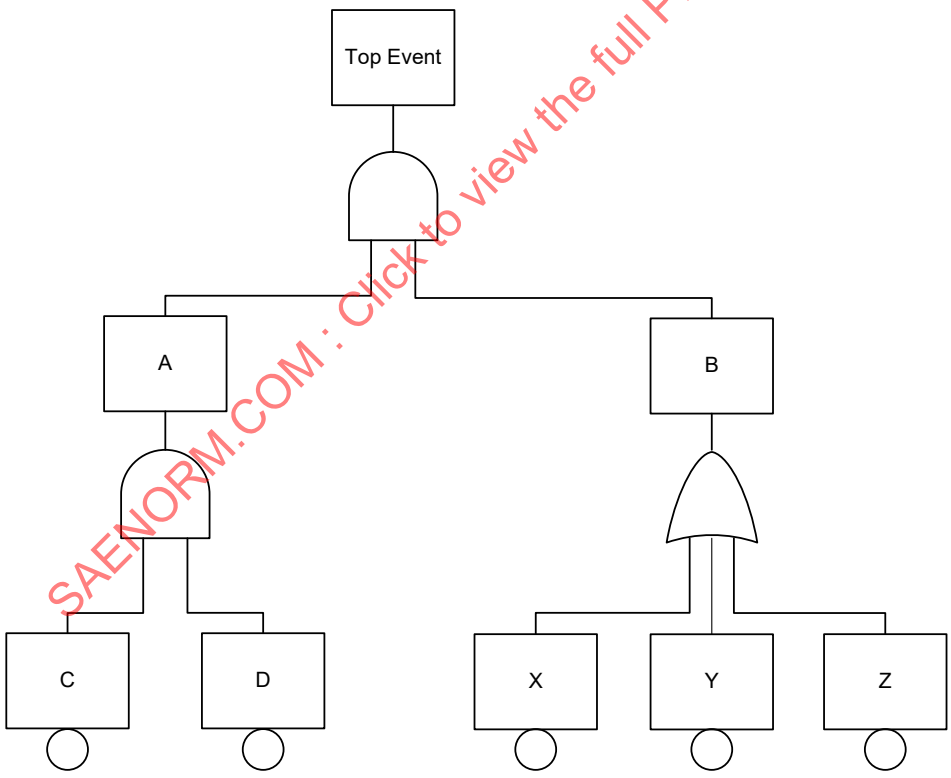


Figure G11 - Fault tree to demonstrate direct analysis techniques

From Figure G11:

P(A) = P(C) * P(D) [C and D are independent events]

P(B) = P(X) + P(Y) + P(Z) [X, Y, and Z are mutually exclusive events]

P(top) = P(A) * P(B) = [P(C) * P(D)] * [P(X) + P(Y) + P(Z)]

The analyst should perform Boolean analysis on the tree structure if primary events occur more than once in that given tree. Based on the location of these identical primary events within the tree, “direct analysis” without first reducing the tree via Boolean analysis will lead to an incorrect top-level event probability which is either greater than or less than the event’s true probability.

As an example of fault tree reduction via Boolean analysis, consider the tree structure in Figure G12.

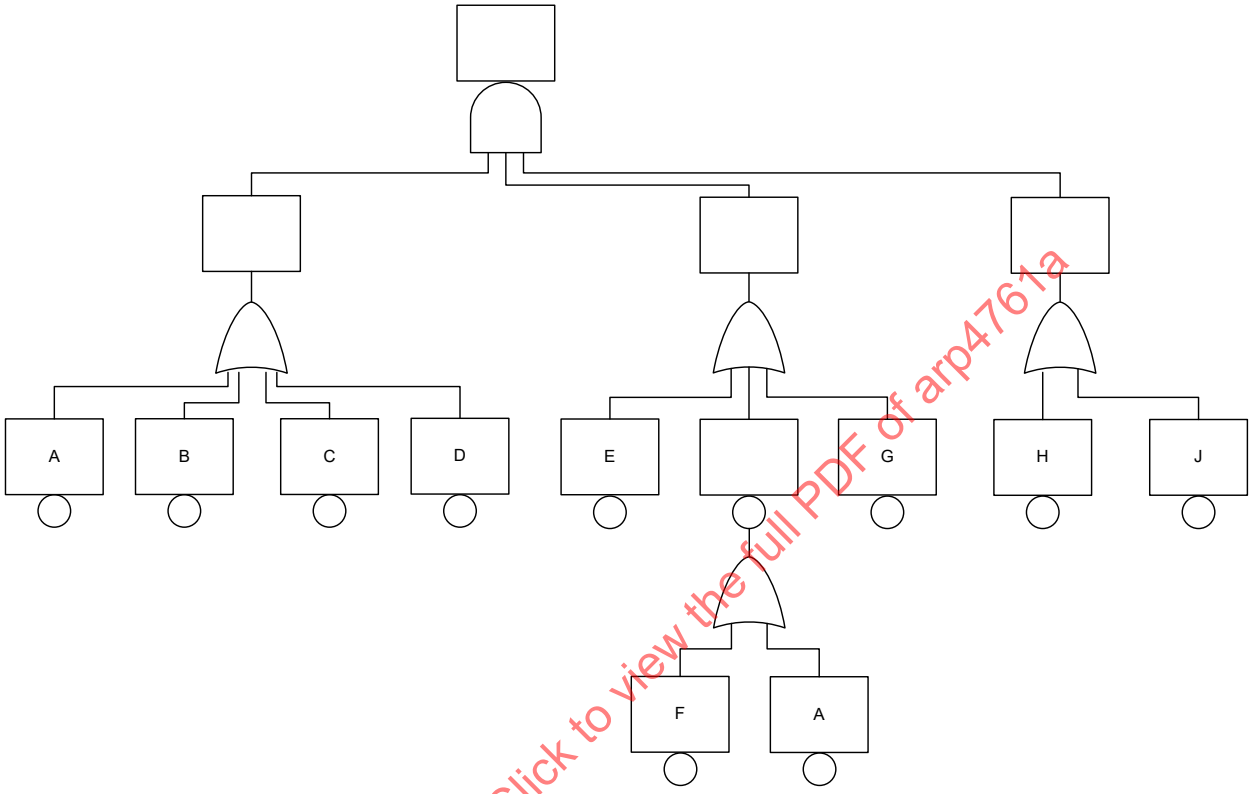


Figure G12 - Fault tree to demonstrate Boolean reduction techniques

SAENORM.COM : Click to view the full PDF of arp4761a

The Boolean reduction follows the following steps.

a. Use “direct analysis” to determine the apparent top. The term apparent is used because event A is located in two branches of the fault tree.

   top = (A+B+C+D) * (E+F+A+G) * (H+J)

b. Multiply out the above equation in order to get terms separated by “+” signs.

   top = AEH + AFH + AAH + AGH + BEH + BFH + ABH + BGH + CEH + CFH + ACH + CGH + DEH + DFH + ADH + DGH + AEJ + AFJ + AAJ + AGJ + BEJ + BFJ + ABJ + BGJ + CEJ + CFJ + ACJ + CGJ + DEJ + DFJ + ADJ + DGJ

c. Apply the following Boolean logic rules to the expanded FTA equation:

   (1) A + A = A, (2) A * A = A, (3) A + AK = A, (4) AAK = AK

   By applying the above logic, the fault tree MCS is determined by reducing the number of elements in a term and reducing the number of total terms. Applying Boolean logic to the equation from step b:

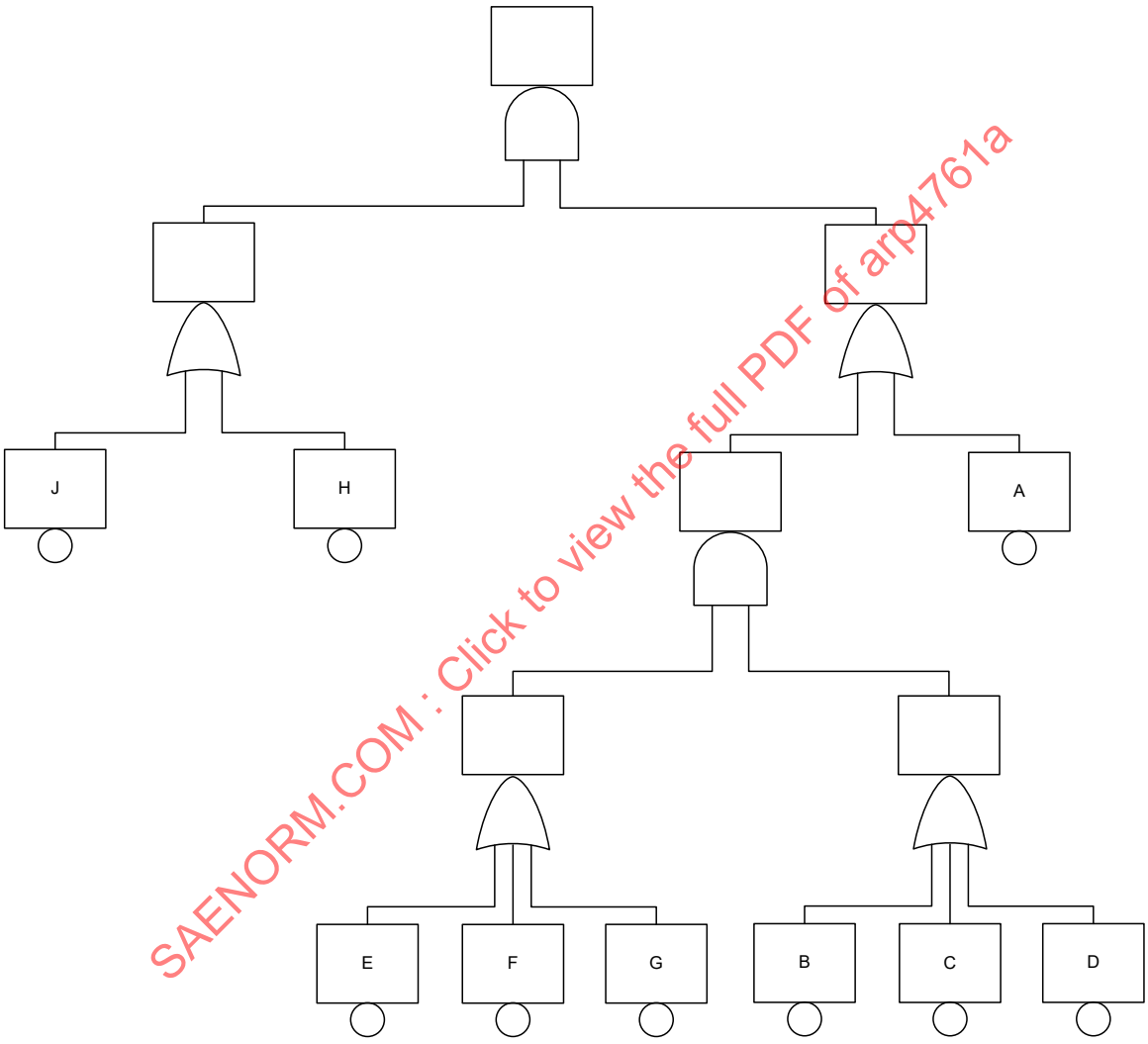
   top = ~~AEH~~ + ~~AFH~~ + AAH + ~~AGH~~ + BEH + BFH + ~~ABH~~ + BGH + CEH + CFH + ~~ACH~~ + CGH + DEH + DFH + ~~ADH~~ + DGH + ~~AEJ~~ + ~~AFJ~~ + AAJ + ~~AGJ~~ + BEJ + BFJ + ~~ABJ~~ + BGJ + CEJ + CFJ + ~~ACJ~~ + CGJ + DEJ + DFJ + ~~ADJ~~ + DGJ

Rewriting the above equation results in the fault tree MCS. Notice that twelve terms were eliminated and two terms went from three to two elements within the term.

top = AH + BEH + BFH + BGH + CEH + CFH + CGH + DEH + DFH + DGH + AJ + BEJ + BFJ + BGJ + CEJ + CFJ + CGJ + DEJ + DFJ + DGJ

d. Draw the reduced fault tree by first combining terms within the MCS equation (optional step). The reduced fault tree is shown in Figure G13.

top = (J+H) * [A + (E+F+G) * (B+C+D)]



SAENORM.COM : Click to view the full PDF of arp4761a

Figure G13 - Reduced fault tree

Many commercially available FTA software packages will generate the cut sets automatically when given the proper commands.

Once the reduced tree is drawn, the analyst should confirm that all AND-gates indicate a true combination of independent events. This step is very important before performing the FTA numerical calculations. A Common Mode Analysis (see Appendix M) may assist in evaluating the event independence. In the event that an issue with independence is identified, the fault tree model should be re-evaluated.

G.10.2 Qualitative Importance Determination

In order to get some idea of how the various cut sets impact the undesired top-level event, the analyst can evaluate the fault tree using a method known as qualitative importance. Qualitative importance is simply ranking the cut sets in ascending order based on the number of primary events in the cut set. This method allows the analyst to see the various primary events relative importance with respect to top-level event occurrence based on how many times the primary event appears in the cut sets and in what combination with other primary events. This FTA evaluation technique works well with hardware failure, function development error or hardware/software development error.

Assume that the analyst wants to evaluate a fault tree via qualitative importance. First, the cut set is ranked as described in the previous paragraph. This ranking gives the analyst knowledge of whether the top-level event has any associated single point failures and how often any one primary event helps cause the top event to occur.

Furthermore, by assuming a standard failure rate value (e.g., 1.0E-06) and a standard exposure time (e.g., 100 hours) for all hardware failure related basic events, the analyst can get a gross estimate of a cut set's relative importance. For example, using the values provided in the previous sentence, a cut set with two basic events has a probability of failure (P_f) of 1.0E-08, a cut set of three basic events has a P_f of 1.0E-12. Using this gross estimating technique, the analyst can quickly conclude that cut sets with five or more basic events have very little relative impact on the top-level event probability of failure.

The drawbacks associated with this evaluation method are as follows.

a. If the analyst has hardware related basic event at indenture levels higher than the piece-part level, an additional reliability analysis should be performed in order to get a failure rate number for the P_f estimate.

b. Basic event exposure times can vary greatly from one basic event to another because of such factors as monitor cycle times, monitor exposure times, and maintenance intervals. Consequently, the estimated failure probabilities used to weigh relative importance of one cut set to another are no better than gross estimates. Exposure time variations can mean two or three orders of magnitude difference between the estimated failure probabilities and quantitatively obtained failure probabilities.

G.10.3 FTA Supporting FDAL/IDAL Assignment

An FTA may be used to support FDAL and IDAL assignment activities (see Appendix P). When supporting the FDAL/IDAL assignment process, the FTA is constructed of potential error sources rather than failure mechanisms. An example of a fault tree which includes the consideration of errors is presented in Figure G14.

Figure G14 illustrates the potential error sources which when combined could cause the top undesired failure condition event. For the Figure G14 example, two independent functions (F_1 and F_2) must contain errors for the failure condition (FC2) to occur. The sources of function error may be either in the development of the functions (F_1, F_2) or in the development of the items (I_1, I_3). This FTA is a model of the planned development environment associated with the two functions. The minimum number of errors which will cause the FTA result to be true is called a Functional Failure Set.

The FDAL/IDAL assignment activity may now use the FTA qualitative presentation, in combination with all other failure conditions error FTAs to derive an appropriate assignment.

SAENORM.COM : Click to view the full PDF of arp4761a

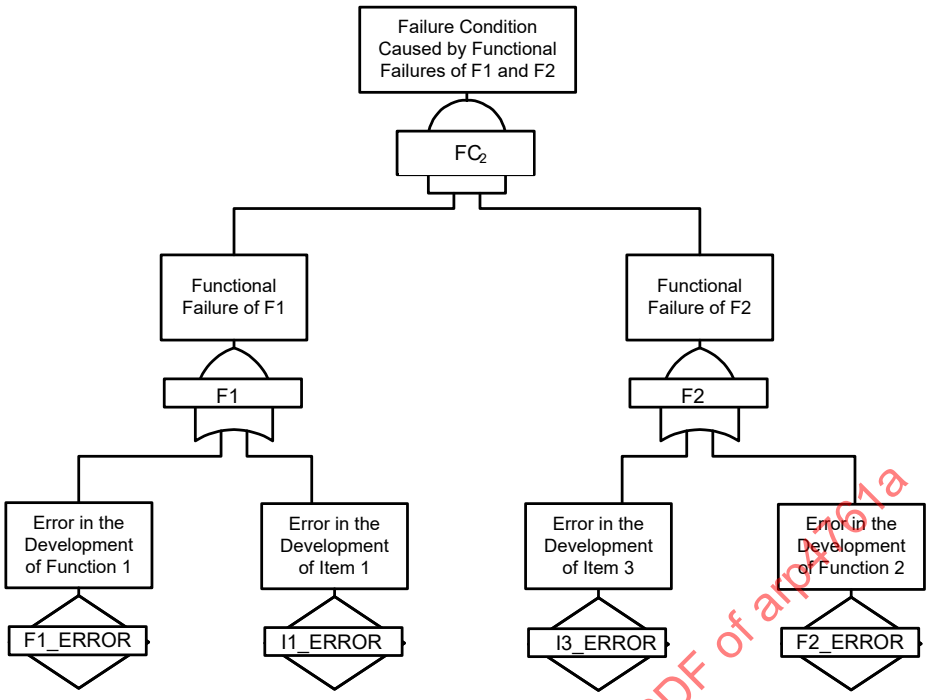


Figure G14 - Error FTA example

G.11 QUANTITATIVE FAULT TREE EVALUATION USING UNAVAILABILITY METHOD

Quantitative fault tree evaluation techniques produce three types of results: (1) numerical probabilities, (2) quantitative importance, and (3) sensitivity evaluations. All three results can be obtained from MCSs as described in Section G.10. Other methods exist which may be more efficient for some fault trees. This section provides the minimal amount of information needed to understand the subject matter and has been restricted to elementary examples which are based on the assumption of constant failure rates and small λt. For a more detailed and complete explanation of these techniques, refer to NUREG-0492 or one of many similar books on the subject of fault tree evaluation.

The methods of fault tree quantification other than those described in this section, which can be shown to be logically and mathematically correct, may be used at the discretion of the analyst. When using software tools to perform fault tree calculations, some random manual cross checks should be performed to show the reasonableness of the results generated by the tool.

G.11.1 Numerical Probability Calculations

The quantitative evaluation technique for determining a fault tree level event probability of failure (P_f) using cut sets has five major steps.

a. Determine the fault tree MCSs.

b. Determine the failure/SEE rates of the basic events.

c. Determine the exposure times and “at risk” times of the basic events.

d. Establish any relevant required order factors.

e. Perform the FTA numerical calculations.

These five steps are described in the following sub-sections. The analyst cannot perform quantitative analysis on MCSs containing development errors. Fault trees containing development errors can be evaluated using a qualitative evaluation method described in Section G.10.

SAENORM.COM : Click to view the full PDF of arp4761a

G.11.1.1 Determine the Fault Tree Minimal Cut Sets

The process of determining MCSs for quantitative FTA evaluation is the same as the process used for qualitative evaluation discussed in G.10.1. The MCSs may be different for a qualitative FTA than a quantitative FTA. For a quantitative FTA, the lack of independence between two or more primary events should be evaluated against failure independence while a qualitative fault tree may include errors or failures.

G.11.1.2 Determine the Rates of the Basic Events

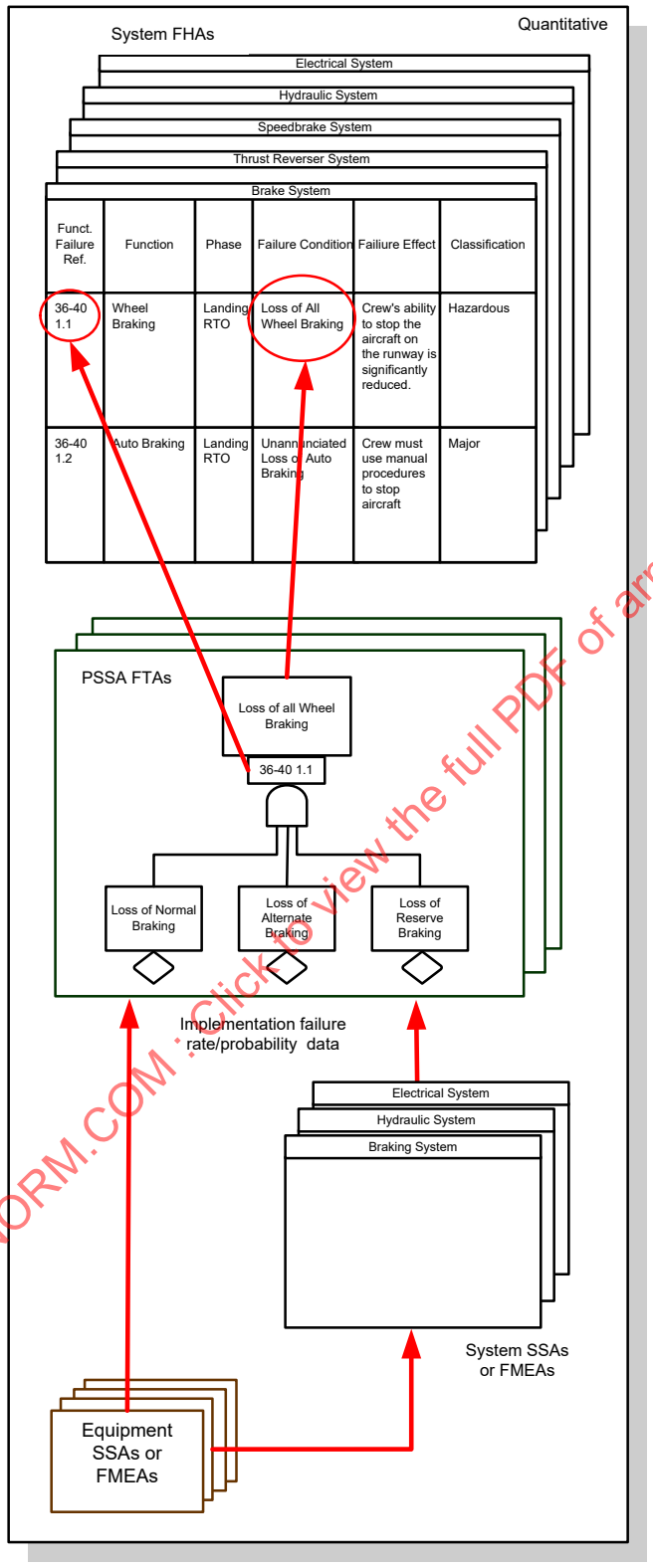
G.11.1.2.1 Hardware Failure Rates

A failure rate for each hardware related basic event in the fault tree should be determined. Failure rates should be determined whenever possible from failure rate data of similar equipment already in field use. Other industry-wide sources of failure rates and/or mode distributions may be found in U.S. military handbooks, reliability analysis references, and industry reliability data exchange references. While these reference documents provide a basis for failure rate prediction of some component types, there will be many device types that are not included in these documents. This is especially true for complex digital integrated circuits (ICs) which need to be considered on a part by part basis. Determining the failure modes of digital devices generally require engineering judgment and it is unlikely that all of the failure modes can be determined for a complex digital IC.

The entire failure rate of the device can be conservatively assumed to cause the failure mode of concern in the fault tree. When the entire failure rate of a component or function is too conservative, the FMEA/FMES can be used to identify failure modes and associated rates for components or functions. Figure G15 summarizes other potential failure rate and probability data sources. These failure rates can then be used as basic event failure rates in the FTA supporting an SSA. References to failure rate sources may be explicitly made in each basic event for traceability purposes.

Care should be taken when using the failure rates from an FMEA/FMES as the analysis may have included mitigation methods which erroneously reduce or eliminate the failure mode rate. This mitigation in the FMEA/FMES is in effect an “AND” gate in fault tree terms which needs to be appropriately modeled in the fault tree to avoid masking potential common causes. Therefore, when using failure rates from an FMEA/FMES for a fault tree basic event, the failure rate for failure modes before any monitoring is considered should be used. This allows the failure mode and the appropriate mitigations to be accurately modeled.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure G15 - Potential FTA failure rate data sources

Failure rates may be on either a per flight hour or per operating hour basis. Whether using failure per operating or per flight hour, the same units are used for the entire fault tree.

Using failure rates based on hours of operation is most appropriate for safety analysis because there are latent failures with an exposure time greater than an average flight that could occur outside the actual flight time. Though fault tree results are normally expressed in the units per flight hour, the event failure rates in units per flight hour may not be accurate due to differences in latency of each event. For example, if there is a latent failure that is only detected during a periodic test window greater than an average flight time, the failure rate used should be representative for the entire period between checks. This period could include operating time on ground and operating time during flight, and—in some cases—non-operating time. Using failure rate per hour during flight is also acceptable and conservative.

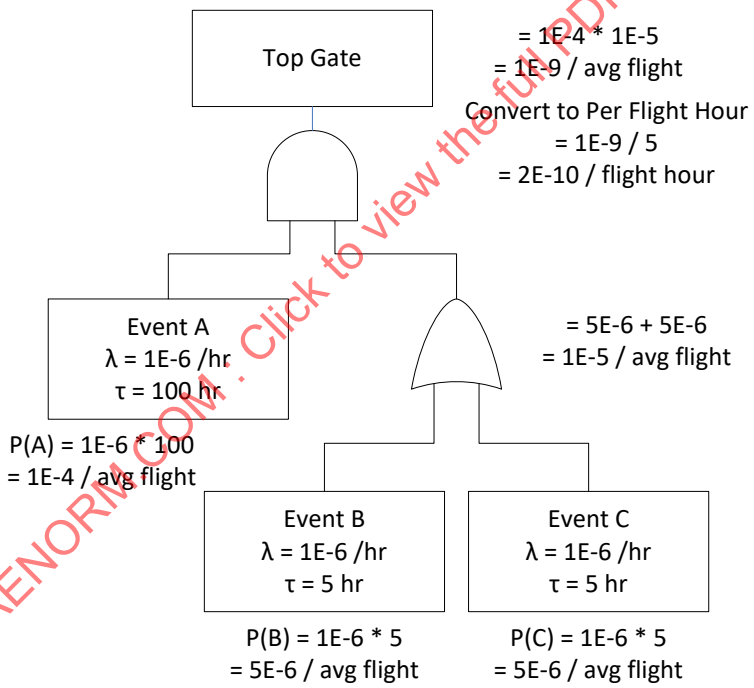
The fault tree example in Figure G16 shows how events with failure rates from a reliability prediction in units of failures per hour of operation give a top gate result in units per flight hour.

Assumptions:

a. Average flight time = 5 hours.

b. Event A latent for 100 operating hours.

c. Events B and C are active failures.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure G16 - Example FTA failure rate units

G.11.1.2.2 Single Event Effects Rates

In addition to hardware failures, some electronic hardware may be susceptible to Single Event Effects (SEE) which can cause effects that may be included in the fault tree.

Single Event Effects are random and may be addressed in the safety analysis in a similar manner to hardware failures. The contribution of SEE at the component level may be considered based on the sensitivity of the component and the ability for the SEE to contribute to the failure condition. An example of determining the sensitivity of components to SEE is contained in AIR6219/ER-008. If SEE is being included in a fault tree, mitigations to prevent SEE from contributing to the fault tree top event may be included as an AND-gate in the fault tree similar to monitors protecting against hardware failures.

G.11.1.3 Determine the Exposure Times and “At Risk” Times of the Basic Events

The analyst determines the exposure time or “at risk” time associated with each basic event in the fault tree. Some of the different types of basic events are:

a. Basic event associated with loss or malfunction of a function of equipment which is used throughout the entire flight.

b. Basic events associated with loss or malfunction of a function of equipment used only during particular phases of the flight.

c. Basic events associated with latent failure of equipment that performs a function.

d. Basic events associated with loss or malfunction of a protective element (e.g., fault monitors).

e. Basic events associated with SEE where corrupted data is refreshed before the corrupted data can contribute to the fault tree top event.

f. Basic events associated with SEE where corrupted data is not refreshed.

Paragraphs G.11.1.3.1 through G.11.1.3.5 describe how to determine the exposure times or “at risk” times associated with each of these types of events.

G.11.1.3.1 Loss or Malfunction of a Function of Equipment Used Throughout the Entire Flight

In this case, the equipment being analyzed is used throughout the entire flight. When the equipment fails or malfunctions, it results in the undesired failure effect. The “at risk” time for this case is equal to the estimated average flight duration.

G.11.1.3.2 Loss or Malfunction of a Function Used Only During a Particular Phase of a Flight

There are two main subcases associated with the loss or malfunction of equipment which is used only during particular phases of flight. In the first subcase, the “at risk” time is equal to the time elapsed from the beginning of the flight to the end of the phase in question. For example, assume the phase in question is “gear down” and the equipment used to lower the gear is known to be operating properly via on-ground test. The “at risk” time for the equipment required to lower the landing gear is the time period from the ground test to the end of the “gear down” phase of the flight.

In the second subcase, the equipment is known to be working just prior to using it and is again only used during a particular phase of the flight. For this subcase, the “at risk” time and exposure time are equal to the time elapsed from the function checkout to the end of the phase in question. For example, assume the phase in question is “autoland” and the equipment used to automatically land the plane is known to be operating properly via an initiated test run at “autoland” mode engagement. The “at risk” time for this scenario is the time period from the initiated test to when the aircraft touches the ground.

G.11.1.3.3 Latent Failures

Latent failures disable protective mechanisms or reduce safety margins thereby increasing the risk of hazards due to subsequent conditions or failures. Latent failures, by themselves, do not constitute a hazard (i.e., the latent failure has no failure effect which would make them noticeable, otherwise they would not be latent). Usually, latent failures affect only functions which are not relied upon in normal operation, but which provide fail-safe coverage and/or protection against abnormal conditions.

Latent failures can persist for a time interval which is either greater than or shorter than the flight time. This time interval is known as exposure time and is defined as the time between when equipment was last known to be operating properly and when it will be known to be operating properly again. Proper operation may be confirmed during acceptance tests, maintenance checks, monitor cycle times, power-up tests, etc. The key to latent failure management is to detect and repair the applicable failed state quickly in order to reduce the exposure time.

SAENORM.COM : Click to view the full PDF of arp4761a

In the case where a function is being monitored, the exposure time of the function is linked to the monitor exposure time (e.g., a monitor scrubbed during power-up would have exposure time equal to interval between power-ups, a monitor scrubbed at initiation of a flight phase would have exposure time equal to interval between scrub initiation and end of flight).

Latent failures which are only detectable during system/equipment production and return-to-service testing may use the predicted system/equipment MTBF for detectable failures as the exposure time for these events. Latent failures which are only detectable during system/equipment production and for which no detection means are available in service use the design life of the aircraft as the exposure time for these events. The analysis should ensure that the testing for the latent failures is implemented and accomplishes the credit taken in the FTA. If predicted MTBF is used, a conservative exposure time should be allocated to allow for the possibility that the in-service MTBF will be greater than initial predictions. Coordination with Certification Authorities is recommended when MTBF is intended to be used as an exposure time.

G.11.1.3.4 Failure Detection Coverage and Exposure Times

Failure detection may be accomplished through dedicated hardware circuitry, software code, or various test methods. For the purposes of this section, these failure detection methods and associated mitigating action are referred to as monitors.

There are two subtle assumptions typically made when monitors are included in fault trees. They are:

a. The monitor provides 100% failure detection and mitigation coverage of the equipment performing the function, and

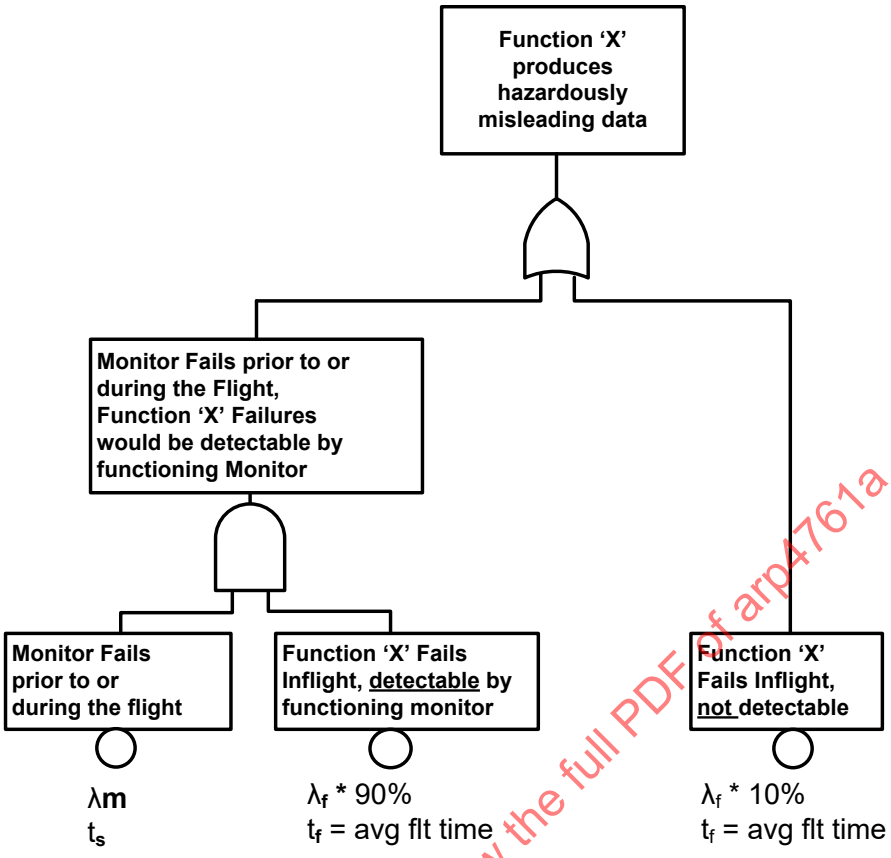
b. The monitor verification (i.e., scrub) operation confirms that the monitor is fully operational and provides 100% coverage of the monitor.

Unfortunately, real life monitors may not provide 100% coverage. The analyst should consider fine tuning the FTA to account for imperfect coverage.

Figure G17 models a system where a monitor detects only 90% of Function “X” circuitry failures whenever the monitor is exercised. In this fault tree, 100% verification of monitor operation is achieved. The remaining 10% of Function “X” circuitry failures are not detected until a return to service test is performed on the equipment. This simplified tree provides a conservative result because the left branch of the tree does not consider required failure order between monitor and function failures in the same flight.

Figure G18 models the above system when it is only possible to achieve 95% verification of monitor operation.

SAENORM.COM : Click to view the full PDF of arp4761a

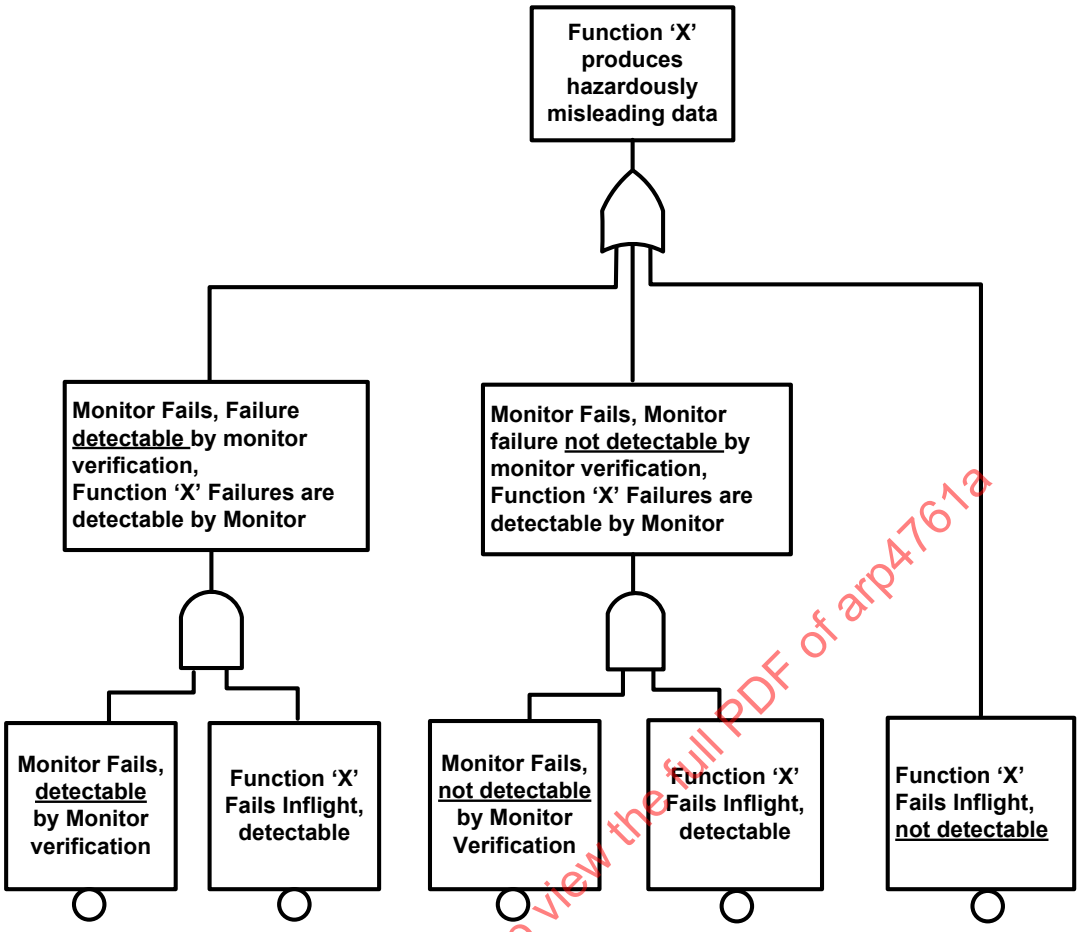


t_s = Monitor 'scrub' (verification) time

$Pf = 0.9\lambda_m\lambda_f t_s t_f + 0.1\lambda_f t_f$

Figure G17 - An example of a fault tree structure when the monitor detects 90% of Function 'X' Failures

SAENORM.COM : Click to view the full PDF of arp4761a



t_s = Monitor 'scrub' (verification) time

$P_{f\,(flight)} = 0.9*0.95\lambda_m\lambda_f t_s t_f + (0.9*0.05)\lambda_m\lambda_f t_m t_f + 0.1\lambda_f t_f$

$P_{f\,(hour)} = P_{f\,(flight)} / t_f$

Figure G18 - An example of a fault tree structure when the monitor detects 90% of Function 'X' Failures and the monitor verification is 95%

SAENORM.COM : Click to view the full PDF of arp4761a

Many methods of failure detection may be required to effectively confirm proper operation of a function, test, or monitor. Each of these detection layers may have different exposure times and should be accounted for accordingly. Some of the more common detection methods include the following:

a. Real time self-test.

b. Power up self-test.

c. Preflight self-test.

d. Scheduled maintenance testing.

e. Initial production test.

f. Return to service test.

G.11.1.3.5 Single Event Effects Inclusion in Fault Trees

SEE can have effects that are either transient in nature (refreshed) or persistent (remain until a corrective action such as power-up or reconfiguration of the affected device). This section presents fault tree structures and exposure times to model these effects when SEE is modelled by FTA.

G.11.1.3.5.1 Loss or Malfunction Due to SEE Where Corrupted Data is Refreshed

Single Event Effects that corrupt data that are refreshed can be ignored by the safety analysis if the refresh occurs at a rate such that the corruption does not persist long enough to cause or contribute to the event being modeled. This would include scenarios such as data stored in RAM that will be updated before each use when the use of a single instance of bad data does not cause the event being modeled. In this case, the corrupted data will be used once but since an SEE does not permanently affect the RAM, when new data is written, the event is cleared.

If corruption of a single piece of data results in the top event, then the fault tree should account for the SEE as shown in Figure G19. Error Detection and Correction (EDAC) is typically used to protect data when it is not refreshed at a rate sufficient to allow corruption of data to be ignored.

Depending on the EDAC algorithm, multi-bit upsets may result in loss of the data instead of correction and design implementations to exclude the use of the corrupted data until corrective action would then need to be modeled in the fault tree.

For failure conditions that are only applicable during a particular phase of flight (see G.11.1.3.2), the exposure time for the SEE basic events may consider any data refresh that occurs prior to starting the phase of flight. In addition, the SEE rate based on the environment for the phase of flight may also be considered if the potential SEE that may have occurred prior to that phase of flight have been mitigated (e.g., refreshed prior to the particular phase of flight).

SAENORM.COM : Click to view the full PDF of arp4761a

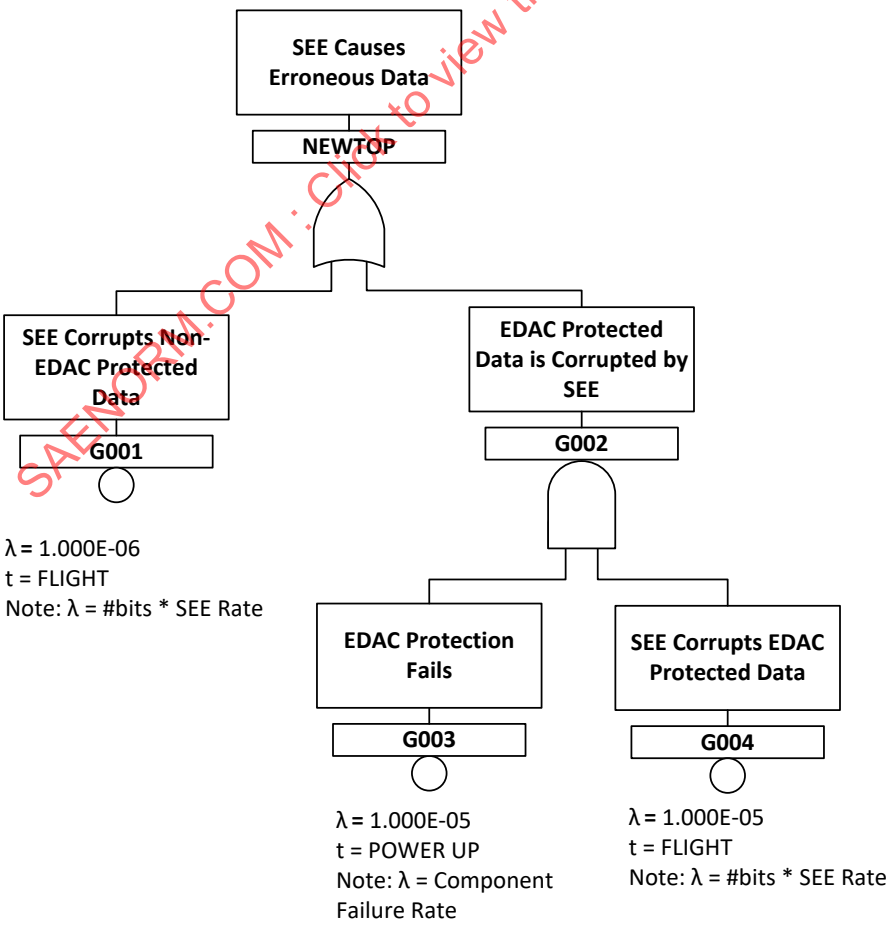


Figure G19 - Fault tree model SEE to protected data

G.11.1.3.5.2 Loss of Function or Malfunction Due to SEE where Corrupted Data is Not Refreshed

Persistent SEE related effects (e.g., SEE to unrefreshed RAM location, latchup) can be dealt with in much the same way as hardware failures. The exception is that the “failure” due to SEE can usually be corrected if desired by power reset or device reconfiguration. Malfunction or loss of function due to these effects could potentially have mitigation that allows the affected device to be reset or re-loaded as shown in Figure G20.

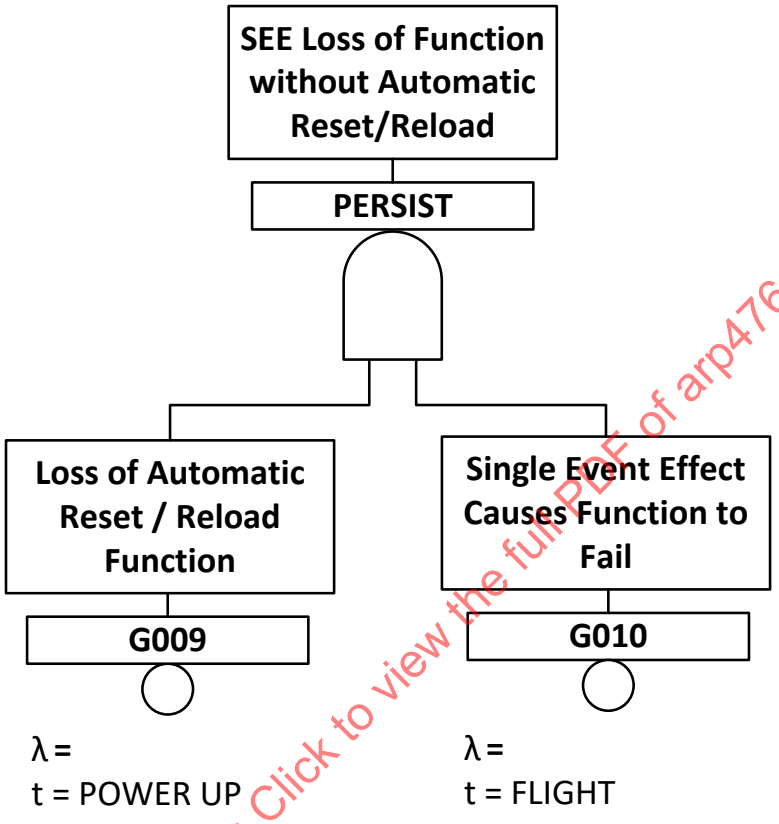


Figure G20 - Fault tree model of persistent SEE with corrective action

SAENORM.COM : Click to view the full PDF of arp4761a

G.11.1.4 Establish any Relevant Required Order Factors

An AND-gate in a fault tree implies no specific order of the faults present. In some cases, this may be unrealistic. An example is a failure combination where a monitor is used to detect failures of functional circuitry that can cause the top-level event. If the monitor fails first, the failure may remain latent until the monitor is next checked. If the Function “X” circuitry fails first, the top-level event does not occur because the monitor mitigates the failure.

When dealing with failure order dependent events, a factor may be incorporated into the fault tree to make the calculated probabilities less conservative. This factor is known as the required order factor or the sequencing factor. For small λt, ($\lambda t < 0.1$), the probability of the two events occurring in either order (given that they both fail) is approximately 1/2 of the total probability and therefore the ROF for each order is 1/2. In general, if there are n events in an AND-gate there are n! possible orders in which they could fail. If only k of those possible orders lead to the top event, then ROF = k/n!.

This approximation is only valid for events with the same exposure time or events with different exposure times where $(\lambda_1 + \lambda_2)T_{(Max)}$ is less than 0.2. For all other cases, ROF should be calculated. An example using ROF is shown in Figure G10.

When a fault tree contains multiple ROFs, it is more accurate to apply the ROF to the MCSs when performing probability calculations. An example is shown in Figure G21.

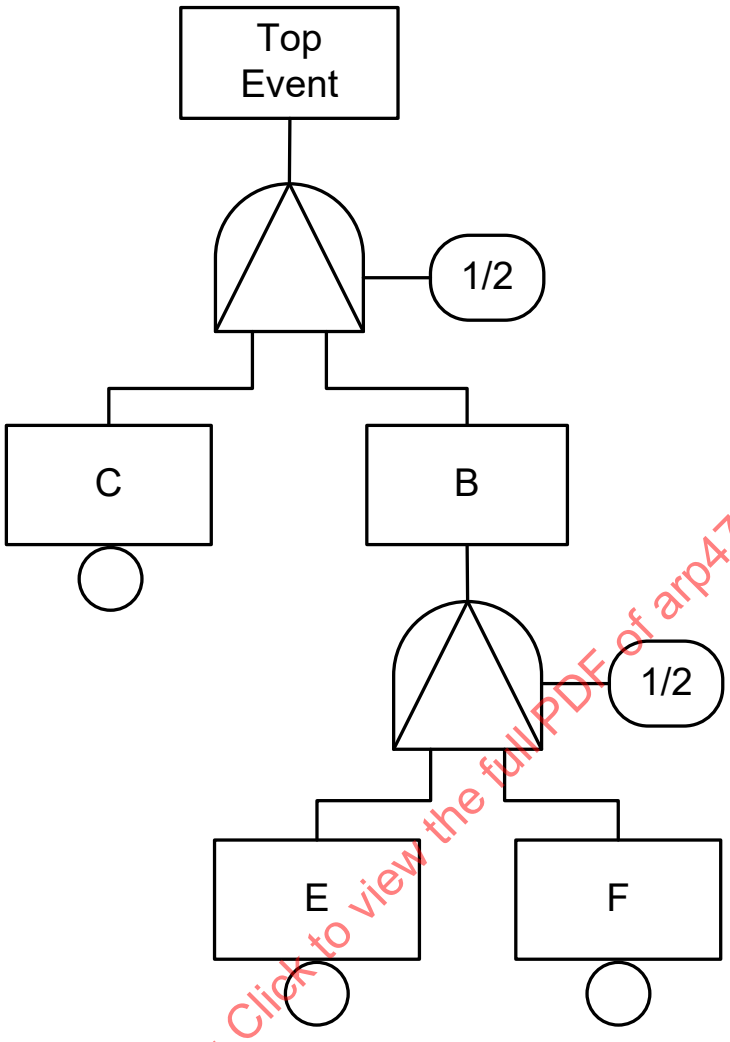


Figure G21 - An example of a fault tree structure which includes Priority AND-gates with ROF

SAENORM.COM : Click to view the full PDF of arp4761a

From Figure G21, one MCS would be 1/2(P_fC*1/2*P_fE*P_fF) = 1/4* P_fC*P_fE*P_fF. However, this answer is incorrect.

The analyst should generate the same cut set from Figure G21 ignoring the ROFs (i.e., P_fC*P_fE*P_fF). Next, it is necessary to calculate k/n! by considering how many of the possible combinations would satisfy the required orders. There are 3! (i.e., six) possible orders which are CEF, CFE, ECF, EFC, FCE, and FEC. The order CEF clearly satisfies the required order and ECF may also satisfy it. More knowledge of the actual system is required to establish this. Therefore, k could equal 1 or 2 and k/n! may equal 1/6 or 1/3. The complete and most correct mathematical solution for the probability of this cut set is therefore either 1/6 P_fC*P_fE*P_fF or 1/3 P_fC*P_fE*P_fF. This illustrates that care must be taken when multiple ROFs exist with a fault tree cut set.

G.11.1.5 Perform the FTA Numerical Calculations

After the steps in G.11.1 are completed, the probability of failure for the top-level event [P_f(top)] is calculated by performing the Boolean algebra mathematics. The methods used for combining probabilities in AND-gates and OR-gates are described in G.10.1.

When dealing with constant failure rates (i.e., the equipment is operating in the flat portion of the reliability bathtub curve), the basic event probability of success (also referred to as basic event reliability) is given by the Equation G2:

$$P_s = R = e^{-\lambda t} \quad \text{(Eq. G2)}$$

where:

P_s = Probability of Success

R = Reliability

e = natural logarithm base

λ = base event failure rate

t = base event exposure or “at risk” time

In reliability terms, we know survival and failure are complementary and mutually exclusive. Consequently, for any given time period:

$$P_s + P_f = R + Q = 1 \quad \text{(Eq. G3)}$$

or

$$P_f = Q = 1 - e^{-\lambda t} \quad \text{(Eq. G4)}$$

where:

P_f = Probability of Failure

Q = Unreliability

When $\lambda t \leq 0.1$, Equation G4 can be simplified to $P_f = Q = \lambda t$.

The FTA numerical calculations are performed using P_f because the electronic based systems of today have such high reliability (R = 0.9999...) that Q is less sensitive to round-off errors and thus produces a more accurate P_f(top). In other words, FTA numerical calculations should deal with the probability of failure terms instead of probability of success terms.

The case in which two latent failures cause system failure is approximately correct providing $n\lambda t_f$ is small for both failure mechanisms, but is inaccurate if $n\lambda t_f$ is large. The reason is that if both equipment in a dual equipment system fail latent, then the failure must be manifest. Therefore, there is an implicit assumption that both equipment have not failed at the beginning of the mission. Since this case is not included in the calculations, the result may be higher than necessary when $n\lambda t_f$ is large (n is the number of missions between maintenance periods). A correct mathematical result can be obtained by the use of Boolean algebra or Markov Analysis.

In G.11.1.5.1 through G.11.1.5.4, the four particular examples in G.9.3 are developed further to show typical fault tree calculations which include basic events with or without latency and required order factors. The methodology presented here shows the probability for the worst-case flight as well as the average probability per flight of the top event, for double failures. Different methods could be applied to calculate the average probability per flight in cases where the problem is straightforward. Distinct formulas would need to be developed to deal with more than two failures or where some of the assumptions are not correct. To calculate the probability per flight hour, see Section G.13. A conservative analysis using the worst-case flight probabilities may be submitted to show compliance without the complication of computing the average probability. Caution is required with the use of fault tree software packages which may automatically select either worst-case or average probabilities.

SAENORM.COM : Click to view the full PDF of arp4761a

G.11.1.5.1 Fault Tree Calculation When Two Failures Cause a Loss of a Function and Neither Failure is Latent

This is the simple failure case where the top event is caused by the loss of both elements during the same flight. Both elements are known to be operating at the start of the flight and neither fail latent. Since neither failure is latent, the average and worst-case probability calculations are identical. The two failures can occur in either order. An example is shown in Figure G22.

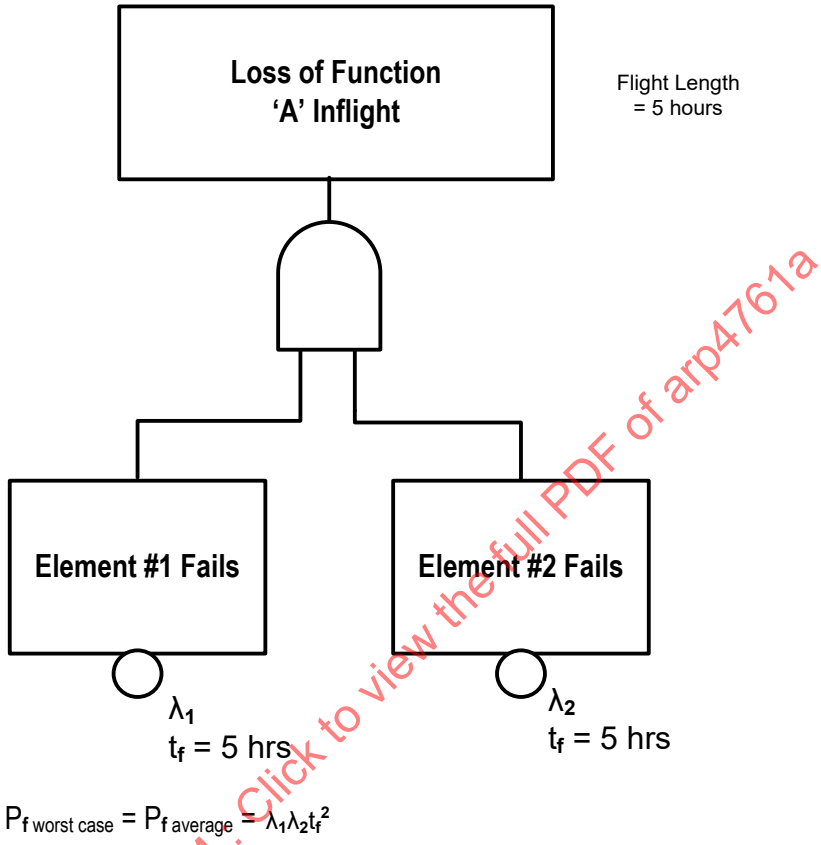


Figure G22 - Fault tree calculation example when two failures cause a loss of a function

G.11.1.5.2 Fault Tree Calculation When Two Failures Cause a Loss of a Function and One Can Fail Latent but the Other Cannot Fail Latent, No Sequencing

In this case, Element #1 can fail at any point between when it is checked (time = zero) and when it is next checked (time = T). Element #2 is known to be operating at the start of each flight and never fails latent. The order of failure does not matter. In this case there is a difference between the average probability of the top event per flight and the probability of the top event for the worst-case flight. Consider that there are n flights of t_f hours, i.e., $T = nt_f$. (this example assumes no failures occur during ground operating time). The failure rate, λ, is the failure rate per hour during flight.

Using the approximation of $P_f = \lambda t$ for small λt, gives the following which is shown pictorially in Table G5.

a. Probability of both failures occurring in the first flight after the inspection check = $\lambda_1\lambda_2 t_f^2$.

b. Probability of element one failing in either of the first two flights after the inspection check and element two failing in the second flight = $2\lambda_1\lambda_2 t_f^2$.

c. Probability of element one failing in any of the first i flights and element two failing in the i^{th} flight = $i\lambda_1\lambda_2 t_f^2$.

SAENORM.COM : Click to view the full PDF of arp4761a

d. Probability of element one failing in any of n flights and element two failing in the final (n^{th}) flight = $n\lambda_1\lambda_2 t_f^2$. (This is the probability for the worst-case flight.)

e. The average probability per flight equals the sum of the probabilities for each flight, divided by n, the number of flights in the latency period.

$$P_{f\,Average} = 1/n * \Sigma i\lambda_1\lambda_2 t_f^2 \text{ for } i = 1 \text{ to } n \qquad \text{(Eq. G5)}$$

$$= (\lambda_1\lambda_2 t_f^2)/n * \Sigma i \text{ for } i = 1 \text{ to } n$$

$$= ((\lambda_1\lambda_2 t_f^2)/n * (n * (n+1))/2$$

$$= 1/2 * \lambda_1\lambda_2 t_f(nt_f + t_f)$$

$$= 1/2 * \lambda_1\lambda_2 t_f(T + t_f)$$

The factor of 1/2 appears in Equation G5 as a result of calculating the average probability that the function will fail on any single flight within the latency period and not from using a mean exposure time of T/2.

Table G5 - Pictorial representation of average probability calculation for a two failure case—one latent and one active

Case #	Current Flight	A Non-Latent Failure on Current Flight And a Latent Failure on 1st Flt of Latency Period	A Non-Latent Failure on Current Flight And a Latent Failure on 2nd Flt of Latency Period	A Non-Latent Failure on Current Flight And a Latent Failure on ith Flt of Latency Period	A Non-Latent Failure on Current Flight And a Latent Failure on Next to Last Flt of Latency Period	A Non-Latent Failure on Current Flight And a Latent Failure on Last Flt of Latency Period	Total Probability for This Case
1	1st Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$					$\lambda_1\lambda_2 t_f^2$
2	2nd Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$				$2\,\lambda_1\lambda_2 t_f^2$
i.	ith Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$			$i\,\lambda_1\lambda_2 t_f^2$
n-1	Next-to Last Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$		$(n-1)\,\lambda_1\lambda_2 t_f^2$
n	Last Flight of Latency Period	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$n\lambda_1\lambda_2 t_f^2$

An example is shown in Figure G23. In the Figure G23 example, T_1 (flight time for Element #1 at end of last flight before next inspection) has been assumed to be 1000 hours.

SAENORM.COM : Click to view the full PDF of arp4761a

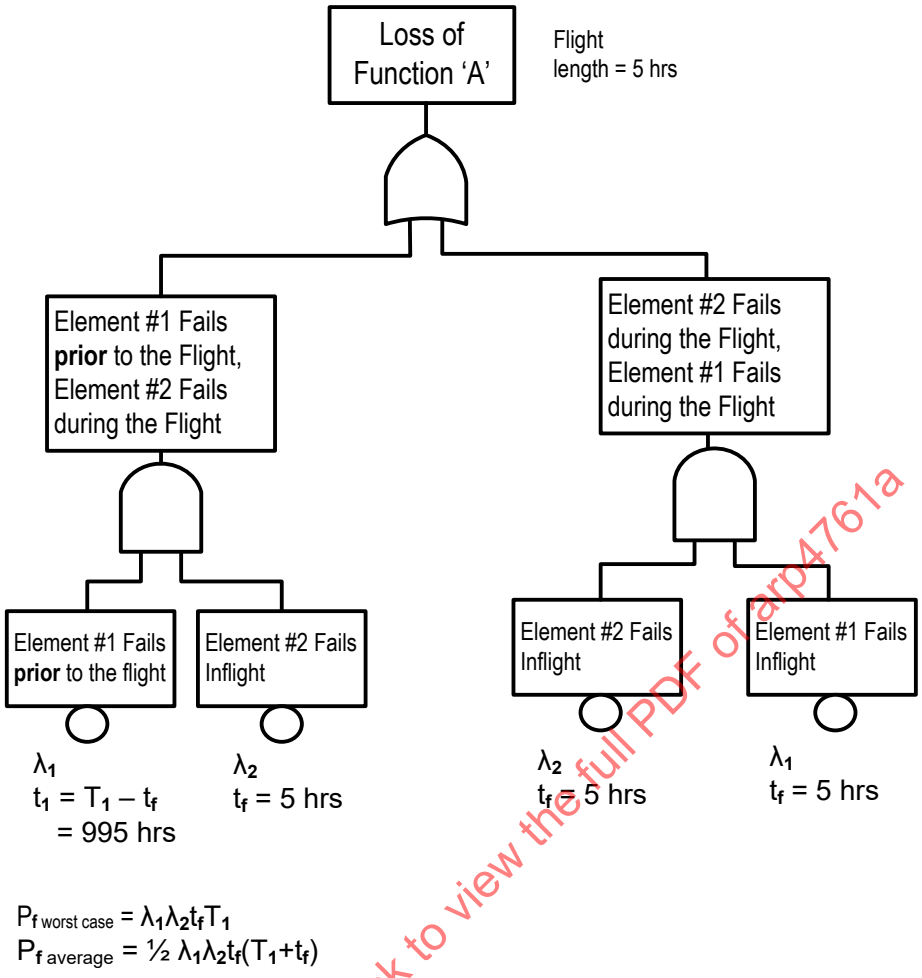


Figure G23 - Fault tree calculation example when two failures cause a loss of a function where one could fail latent

G.11.1.5.3 Fault Tree Calculation When Two Failures Cause a Loss of a Function and Each Could Fail Latent, No Sequencing

In this case, either element could fail latent, but if both fail, this would be detected by virtue of it causing the top event. Therefore at least one of the elements must be operating at the start of each flight. An example is shown in Figure G24. In Figure G24, T_1 has an assumed value of 1000 hours and T_2 an assumed value of 2000 hours (flight time at end of last flight before next inspection for each element). The failure rate for each element, λ, is the failure rate per hour during flight.

SAENORM.COM : Click to view the full PDF of arp4761a

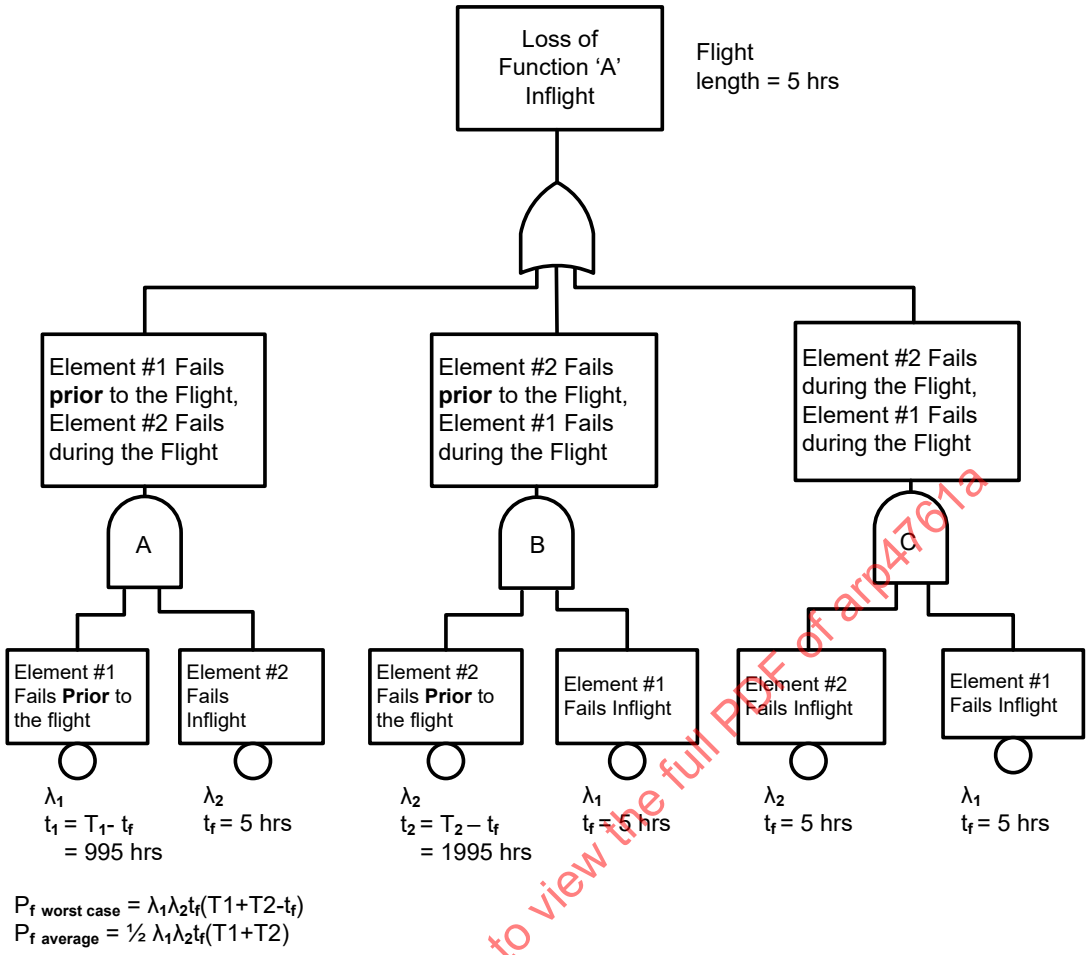


Figure G24 - Fault tree calculation example when two failures cause a loss of a function where each could fail latent

Three things should be noted about Figure G24. First, an undeveloped event for failure order (i.e., ROF = k/n! as described in G.11.1.4) is not required because failure order dependence is built into the tree structure via the latency period ($t_n = T_n - t_f$), which is representative for a failure before the flight. Second, the rightmost AND-gate is necessary to cover the case that both elements fail during the flight without a required sequence. Third, the rightmost AND-gate (C) is often omitted and the exposure times of paths A and B are set equal to the inspection intervals, for the case where t_f is much less than the inspection intervals.

The probability of the worst-case flight is calculated as below, with reference to Figure G24:

$$P_fA = \lambda_1(T_1 - t_f)\,\lambda_2 t_f \qquad \text{(Eq. G6)}$$

$$P_fB = \lambda_2\,(T_2 - t_f)\,\lambda_1 t_f \qquad \text{(Eq. G7)}$$

$$P_fC = \lambda_1 t_f \lambda_2 t_f \qquad \text{(Eq. G8)}$$

$$P_{fworst\text{-}case} = P_fA + P_fB + P_fC \qquad \text{(Eq. G9)}$$

$$= \lambda_1\lambda_2 t_f\,(T_1 - t_f + T_2 - t_f + t_f)$$

$$= \lambda_1\lambda_2 t_f (T_1 + T_2 - t_f)$$

For the average probability calculation as described in G.11.1.5.5, the result is:

$$P_f \text{ average} = 1/2\lambda_1\lambda_2 t_f(T_1 + T_2) \qquad \text{(Eq. G10)}$$

SAENORM.COM : Click to view the full PDF of arp4761a

G.11.1.5.4 Fault Tree Calculation When Two Failures Cause a Top Event and One Can Fail Latent and a Required Order is Needed

In this case, Element #1 (the latent one) must fail prior to Element #2 or the top event does not result. Element #2 is known to be operational at the start of the flight. This is typical of a failure/monitor situation where the top event is an erroneous output rather than a loss of function. An example loss of function with latent failures is provided in Figure G25. T_1 is the flight time at end of last flight before next inspection. The failure rate for each element, λ, is the failure rate per hour during flight.

The required order factor is used per G.11.1.4.

The probability of the worst-case flight is calculated as below with reference to Figure G24:

$$P_fA = \lambda_1(T_1-t_f)\lambda_2 t_f \quad \text{(Eq. G11)}$$

$$P_fB = 1/2\ \lambda_1\lambda_2 t_f^2 \quad \text{(Eq. G12)}$$

$$P_{f\text{-worst-case}} = P_fA + P_fB \quad \text{(Eq. G13)}$$

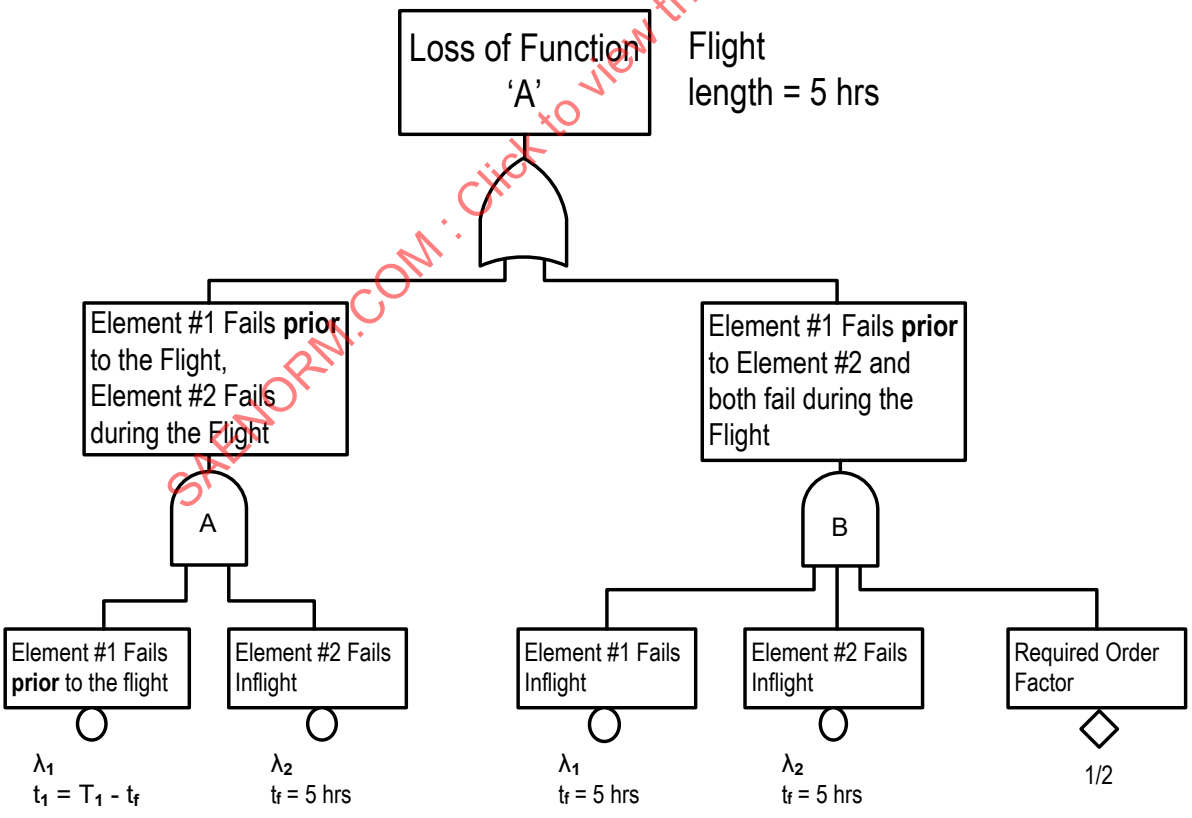
$$= \lambda_1(T_1-t_f)\lambda_2 t_f + (\lambda_1\lambda_2 t_f^2)/2$$

$$= \lambda_1\lambda_2 t_f(T_1-t_f/2)$$

For the average probability calculation, as described in G.11.1.5.5, the result is:

$$P_{f\text{-average}} = 1/2\lambda_1\lambda_2 t_f T_1 \quad \text{(Eq. G14)}$$

SAENORM.COM : Click to view the full PDF of arp4761a



$P_{f\ worst\ case} = \lambda_1\lambda_2 t_f(T_1.(t_f/2))$
$P_{f\ average} = ½\ \lambda_1\lambda_2 t_f T_1$

Figure G25 - Fault tree calculation example when failures cause a top event and one can fail latent and failures are order dependent

G.11.1.5.5 Examples of Calculation of the Average Occurrence Probability of a Double Failure for an Average Flight Time

The following example considers the general case of a double failure F_1 and F_2 with two different failure rates, λ_1 and λ_2, and two latencies, T_1 and T_2, with the assumptions:

$$T_1 \leq T_2,\ T_2 = NT_1, \text{ and } t_f \text{ is the average flight time} \qquad \text{(Eq. G15)}$$

This results in Figure G26.

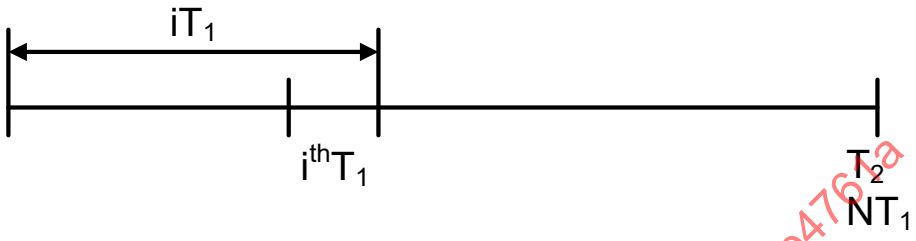


Figure G26 - Equation G15 graphical representation

G.11.1.5.5.1 Probability of Occurrence for the i^{th} T_1

This probability is composed of two cases, Case A and Case B

a. Case A: F_2 occurs before F_1.

1. This case is composed of two subcases:

i. A1: F_2 occurs before the i^{th} T_1 and F_1 occurs during T_1.

ii. A2: F_2 occurs before F_1 during the i^{th} T_1.

$$P_A = P_{A1} + P_{A2} = \lambda_2(i\text{-}1)T_1\lambda_1T_1 + (\lambda_1T_1\lambda_2T_1/2) \qquad \text{(Eq. G16)}$$

(NOTE: /2 term for sequencing F_2 before F_1 during T_1.)

$$P_A = \lambda_1\lambda_2T_1^2(i\text{-}1+1/2) = \lambda_1\lambda_2T_1^2(i\text{-}1/2)$$

b. Case B: F_1 occurs before F_2.

1. In this case the latency of F_1 is T_1, and the double failure occurs if F_1 occurs before F_2 during T_1.

$$P_B = (\lambda_1T_1\lambda_2T_1)/2 \qquad \text{(Eq. G17)}$$

(NOTE: /2 term for sequencing (F_1 before F_2) during T_1.)

The total probability of occurrence for the i^{th} T_1 is:

$$P = P_A + P_B = \lambda_1\lambda_2T_1^2[(i\text{-}1/2) + 1/2] = \lambda_1\lambda_2T_1^2i \qquad \text{(Eq. G18)}$$

SAENORM.COM : Click to view the full PDF of arp4761a

G.11.1.5.5.2 Probability of Occurrence for the T_2 Periods

The global occurrence probability for the T_2 period is:

$$P_G = \Sigma (P_A + P_B); \text{ for } i = 0 \text{ to } i = N \quad \text{(Eq. G19)}$$

$$P_G = \lambda_1\lambda_2T_1^2[(N(N+1)/2 - N/2) + (N/2)]$$

$$P_G = \lambda_1\lambda_2T_1^2[(N^2/2 + N/2 - N/2) + N/2]$$

$$P_G = \lambda_1\lambda_2T_1^2[N^2/2 + N/2]$$

Replace NT_1 by T_2

$$P_G = 1/2\lambda_1\lambda_2T_2(T_1 + T_2)$$

G.11.1.5.5.3 Probability of Occurrence per Flight

P_G is the average occurrence probability for a period of T_2 hours. To have the average occurrence probability per flight, it is necessary to divide P_G by T_2 to have the average occurrence probability per hour of flight and to multiply by t_f, which is the average time of a flight.

This results in the general formula of Equation G20:

$$P_{ft} = P_G * t_f/T_2 \quad \text{(Eq. G20)}$$

$$P_{ft} = 1/2\lambda_1\lambda_2t_f(T_1+T_2)$$

Where:

P_{ft} = probability per flight of the double failure

G.11.1.5.5.4 Derivation of Current Cases

From the P_{ft} general formula of Equation G20, one can derive several current cases of double failures:

a. Two latent failures, F_1 and F_2, with two different latency periods, T_1 and T_2.

$$\text{No sequence: } P_{ft} = 1/2\lambda_1\lambda_2t_f(T_2 + T_1) \quad \text{(Eq. G21)}$$

$$\text{Sequence } F_2 \text{ before } F_1\text{: } P_{ft} = 1/2\lambda_1\lambda_2t_fT_2$$

$$\text{Sequence } F_1 \text{ before } F_2\text{: } P_{ft} = 1/2\lambda_1\lambda_2t_fT_1$$

b. Two latent failures, F_1 and F_2, with the same latency periods, $T_1 = T_2 = T$.

$$\text{No sequence: } P_{ft} = \lambda_1\lambda_2t_f[(T + T)/2] = \lambda_1\lambda_2t_fT \quad \text{(Eq. G22)}$$

$$\text{Sequence } F_2 \text{ before } F_1\text{: } P_{ft} = 1/2\lambda_1\lambda_2t_fT$$

$$\text{Sequence } F_1 \text{ before } F_2\text{: } P_{ft} = 1/2\lambda_1\lambda_2t_f\ T$$

SAENORM.COM : Click to view the full PDF of arp4761a

c. One latent failure, F_2 and one active failure, F_1, with latency periods, $T_2 = T$ and $T_1 = t_f$.

$$\text{No sequence: } P_{ft} = 1/2\lambda_1\lambda_2 t_f(T + t_f) \quad \text{(Eq. G23)}$$

$$\text{Sequence } F_2 \text{ before } F_1: P_{ft} = 1/2\lambda_1\lambda_2 t_f T \text{ (case of command and monitoring system)}$$

$$\text{Sequence F1 before F2: } P_{ft} = 1/2\lambda_1\lambda_2 t_f t_f = 1/2\lambda_1\lambda_2 t_f^2$$

d. Two active failures, F_1 and F_2, $T_1 = T_2 = t_f$.

$$\text{No sequence: } P_{ft} = \lambda_1\lambda_2 t_f[(t_f + t_f)/2] = \lambda_1\lambda_2 t_f^2 \quad \text{(Eq. G24)}$$

$$\text{Sequence } F_2 \text{ before } F_1: P_{ft} = 1/2\lambda_1\lambda_2 t_f t_f = 1/2\lambda_1\lambda_2 t_f^2$$

$$\text{Sequence } F_1 \text{ before } F_2: P_{ft} = 1/2\lambda_1\lambda_2 t_f t_f = 1/2\lambda_1\lambda_2 t_f^2$$

G.11.2 Quantitative Sensitivity Evaluation

Sensitivity evaluations can be broken into two categories. Refer to NUREG-0492 for a detailed discussion of this subject.

a. Variations of models or data.

b. Formal error analysis.

The analyst can use data or fault tree model variations to determine how sensitive a system design is to a particular aspect of individual primary events. By inserting different failure rates in a particular primary event, the analyst can decide whether a higher reliability equipment/component is worth the additional cost. By inserting different exposure times, the analyst provides input to help establish equipment maintenance intervals.

The analyst can use formal error analysis to determine how sensitive the FTA result is to primary event variability, i.e., variability in failure rates and maintenance intervals. The Monte Carlo method is one such technique which is adaptable to FTA. Since error analyses are based on statistical and probabilistic techniques which are beyond the scope of this appendix, the reader should refer to textbooks on this subject matter.

Quantitative Importance is similar to qualitative importance (see G.10.2) in that both evaluation methods simply rank the cut sets for determining their relative importance with respect to top-level event occurrence.

Quantitative importance can take various forms. Several methods are provided here. The analyst receives a different type of information from each method.

G.11.2.1 Method #1: Cutset Ranking

A simple ranking of cut sets in descending order based on each cut sets actual probability of failure (i.e., highest to lowest P_f).

This method is closely related to qualitative importance. The analyst can accurately determine cut set ranking as opposed to only being able to get a gross estimate of cut set ranking using the qualitative importance method.

G.11.2.2 Method #2: i^{th} Cut Set Importance

Provides a percentage of cut set failure probability with respect to the top-level event failure probability.

$$\%(i) = \frac{P_f(i)}{P_f(top)} \quad \text{(Eq. G25)}$$

SAENORM.COM : Click to view the full PDF of arp4761a

G.11.2.3 Method #3: Fussell-Vesely (FV) Importance

Provides the risk associated with an individual primary event (i.e., provides a relative indication on how much a primary event is contributing to the top-level event P_f).

$$FV = \frac{P_f(top) - P_f(top \mid A = 0)}{P_f(top)} \quad \text{(Eq. G26)}$$

where P_f (top | A=0) is defined as the probability that the top event occurs given event A never occurs; i.e., P_f (A) = 0.

G.11.2.4 Method #4: Birnbaum Importance

Provides the increase in risk associated with a primary event. That is, this method provides the difference in top-level event P_f when a primary event occurs (i.e., P(A) = 1) and when a primary event does not occur (i.e., P(A) = 0).

$$Birnbaum = P_f(top \mid A = 1) - P_f(top \mid A = 0) \quad \text{(Eq. G27)}$$

G.12 QUANTITATIVE FAULT TREE EVALUATION BASED ON FAILURE FREQUENCY

The failure frequency method is an alternative to the unavailability method which may be used if desired by the analyst or customer. As with the unavailability method, the top event probability is calculated from the MCSs. Using failure frequencies (w) of the basic events in fault trees produces failure frequency of the system effect occurring during the flight. The result is already a “per hour of flight” rate so it can be compared directly with a requirement or objective that is expressed in those units. The alternative method explained in this section is based on NUREG-0492 and is an approach that the analyst may select to calculate probability of failure. Fault Tree Analysis software packages generally provide an option to calculate a fault tree by the failure frequency method.

The failure frequency method has the potential to reduce the complexity of the fault tree representation of the failure condition. For example, the failure frequency method allows a single basic event to be used to represent both an active and a latent failure.

Complex fault trees, constructed for failure frequencies, cannot be integrated into unavailability method fault trees however without rebuilding the structure of the unavailability method fault tree (see G.12.5). It is therefore important that the method of calculation is agreed upon by all analysts who are contributing fault trees to a safety analysis, before the analysis commences.

G.12.1 Assumptions Used in Failure Frequency FTA

The following assumptions are established for use in this section:

a. Failures are not repairable until the end of the flight or latency period.

b. Failure rates are constant.

c. Rare event approximation is applicable.

G.12.2 Failure Frequency

Failure frequency (w) is the probability per unit time that the component or system experiences a failure at time t, given that the component or system was operating at time t = 0. (This is also referred to as the unconditional failure intensity.) Equation G28 is from NUREG-0492, Page XI-13:

$w(t)\Delta t$ = the probability that the component fails in time t to $t+\Delta t$ (Eq. G28)

In the definition of w(t), it is not given that the component has operated without failure to time t as was the case for the instantaneous failure rate definition λ(t). If the component is repairable, then it can have failed many times previously; the quantity $w(t)\,\Delta t$ is the probability that it fails in time t to $t + \Delta t$, irrespective of history.

SAENORM.COM : Click to view the full PDF of arp4761a

The failure frequency, w(t), is applicable for both non-repairable and repairable equipment. For both repairable and non-repairable equipment, the expected number of failures in some time interval t_1 to t_2, denoted by $n(t_1, t_2)$, is given by the integral of w(t) from t_1 to t_2 (Equation G29).

$$n(t_1, t_2) = \int_{t_1}^{t_2} w(t)dt \quad \text{(Eq. G29)}$$

For non-repairable component failures, the component can only fail once. Therefore, w(t) is equal to the instantaneous failure rate for the first failure present in Equation G30.

$$w(t) = \lambda e^{-\lambda t} \quad \text{(Eq. G30)}$$

For time t, small compared to 1/λ (such that λt < 0.1), $e^{-\lambda t}$ is approximately 1, and Equation 30 reduces to Equation G31.

$$w \approx \lambda \quad \text{(Eq. G31)}$$

For active failures, the difference between frequency, w, and a rate per flight hour determined from P_f is small. For example, if λ = 1.0E-05/hour.

t = 5 hours → w(t) = 1.00E-05/hour
$P_f(t)/t$ = 1.00E-05/hour

t = 20 hours → w(t) = 1.00E-05/hour
$P_f(t)/t$ = 1.00E-05/hour

When several failure events are combined in a cut set, the failure frequency is calculated from Equation G32 (refer to NUREG-0492 Page XI-17, Equation XI-28).

$$w_{CUT} = \sum_{j=1}^{n} w_j \prod_{i=1, i\neq j}^{n} P_i \quad \text{(Eq. G32)}$$

Where:

P_i = probability of failure of the ith event

w_j = failure frequency of the jth event in the cut set

w_{CUT} = MCS failure frequency

i = number of events ANDed together to produce the cut set, unless enabler or initiators are used (see G.12.6)

j = number of events ANDed together to produce the cut set, unless enabler or initiators are used (see G.12.6).

Note that in the case that enablers or initiators are designated, also i≠j.

The calculation of failure frequency involves one failure occurring at a certain rate (its failure frequency w), while the other failures occur with their respective probabilities based on their “at risk” time (t) or check interval T. This calculation is accomplished for each failure event in an MCS.

SAENORM.COM : Click to view the full PDF of arp4761a

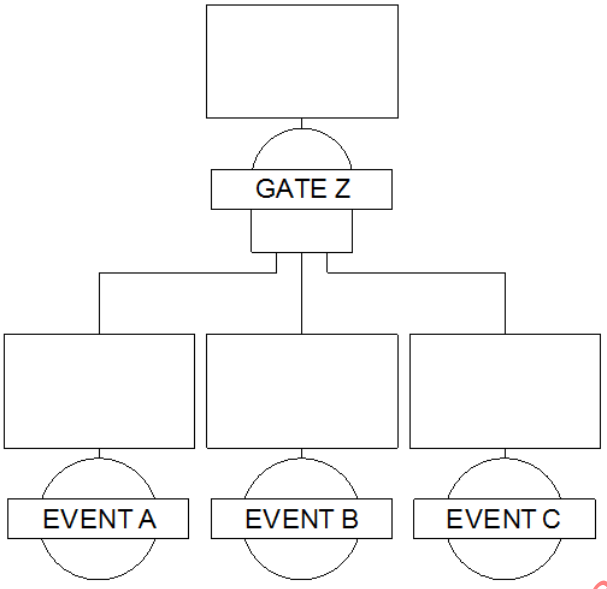


Figure G27 - Example of a three event AND-gate

For Gate Z, in Figure G27, Equation G33 is developed.

$$wCUT = wA * PB * PC + PA * wB * PC + PA * PB * wC \quad \text{(Eq. G33)}$$

For Gate Z and Equation G33, the MCS has three terms (products). This is a consequence of there being three events that combine through an AND-gate to represent Gate Z.

The complete expression for failure frequency of a top event of a fault tree is given by Equation G34.

$$w_{TE} = \sum_{i=1}^{n} w_{CUT\,i} \quad \text{(Eq. G34)}$$

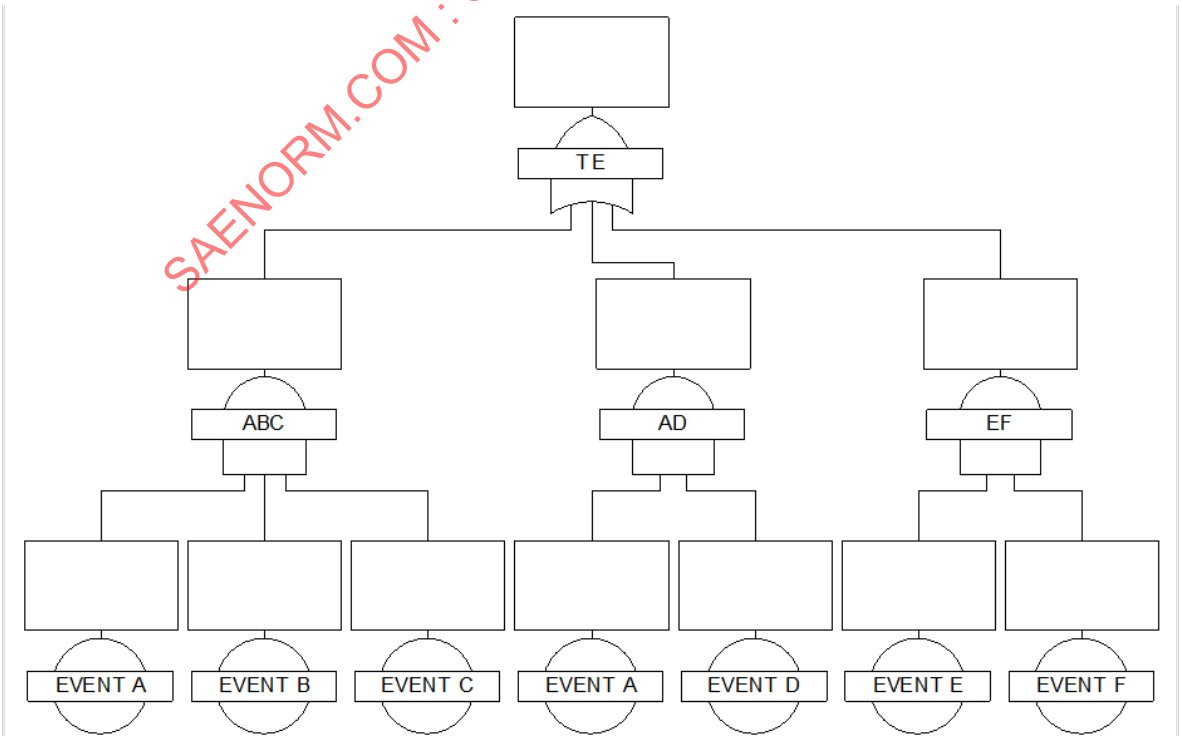


Figure G28 - Example of a fault tree with OR and AND gates

SAENORM.COM : Click to view the full PDF of arp4761a

Using the rare event approximation, the system unavailability represented by the fault tree shown in Figure G28 is:

$$P_{TE} = P_A * P_B * P_C + P_A * P_D + P_E * P_F \quad \text{(Eq. G35)}$$

The resulting w_{TE} is presented in Equation G36.

$$w_{TE} = w_A * P_B * P_C + w_{B*} P_{A.} * P_C + w_C * P_A * P_B + w_A * P_D + w_D * P_A + w_E * P_F + w_F * P_E \quad \text{(Eq. G36)}$$

G.12.3 Comparison to Unavailability Method

Two examples are provided to illustrate and explain the difference in results obtained with the failure frequency analysis versus the rate determined from the unavailability method (P_f/t).

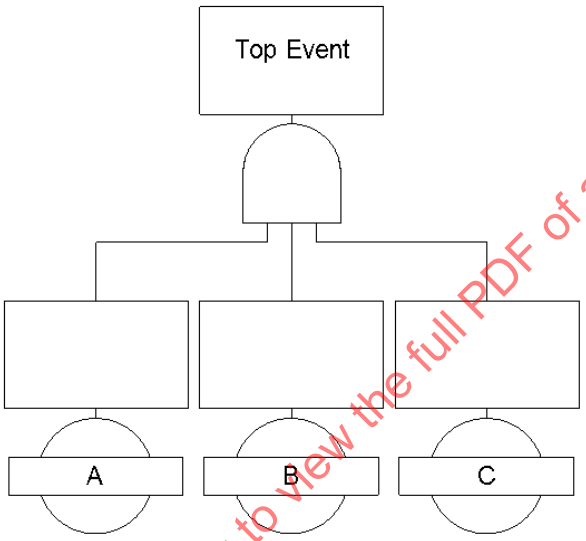


Figure G29 - Three event fault tree example

SAENORM.COM : Click to view the full PDF of arp4761a

Given the following conditions for the FTA shown in Figure G29:

λ_A = 1.00E-05/hour

λ_B = 1.00E-06/hour

λ_C = 5.00E-05/hour

flight time t = 5 hours

The unavailability method probability of the top event is calculated by Equation G37.

$$P_{TE} = P_A * P_B * P_C \quad \text{(Eq. G37)}$$

P_{TE} = (5.00E-05) x (5.00E-06) x (2.50E-04)

P_{TE} = 6.25E-14

Dividing by flight time t = 5 hours results in an unavailability method value of 1.25E-14 per flight hour.

The failure frequency w for the top event is calculated by Equation G38.

$$w_{TE} = w_A * P_B * P_C + P_A * w_B * P_C + P_A * P_B * w_C \quad \text{(Eq. G38)}$$

$$w_{TE} = (1.00E\text{-}05) \times (5.00E\text{-}06) \times (2.50E\text{-}04) + (5.00E\text{-}05) \times (1.00E\text{-}06) \times (2.50E\text{-}04)$$

$$+ (5.00E\text{-}05) \times (5.00E\text{-}06) \times (5.00E\text{-}05)$$

$$w_{TE} = 3.75E\text{-}14/\text{hour}$$

The failure frequency result is three times greater than the result produced by the unavailability method. This illustrates a fundamental difference in the way the numerical result for failure frequency of the top event is calculated. The normalized cut set for unavailability method effectively consists of only one product of a rate and two probabilities:

$$P_{TE} = (P_A/t) * P_B * P_C \text{ (any of the three terms can be divided by t with the same effect)}$$

$$\approx [(\lambda_A * t)/t] * PB * PC \text{ for small values of } \lambda_A t$$

$$= \lambda_A * PB * PC.$$

The cut set for the failure frequency calculation of the same top event has two additional terms:

$$w_{TE} = w_A * P_B * P_C + P_A * w_B * P_C + P_A * P_B * w_C$$

$$\approx \lambda_A * P_B * P_C + (P_A * \lambda_B * P_C + P_A * P_B * \lambda_C) \text{ for small values of } \lambda$$

The frequency method (w_{TE}) has two extra terms ($P_A * \lambda_B * P_C$ and $P_A * P_B * \lambda_C$) which have no equivalent contributions in the unavailability method calculation. This is a consequence of the way in which failure frequency is calculated and produces a conservative result. When only active basic events contribute to the cut set, the ratio between the result of a failure frequency calculation and an unavailability method calculation is equal to the number of basic events constituting the cut set. When there are latent and active failures to consider, the two methods converge.

Consider a second scenario where events A and B have latency and both A and B have active and latent events that need to be considered. An unavailability method FTA would be constructed as shown in Figure G30. Note that for simplicity, the combination of all the active events has been omitted, as explained in G.9.3.3 item c.

SAENORM.COM : Click to view the full PDF of arp4761a

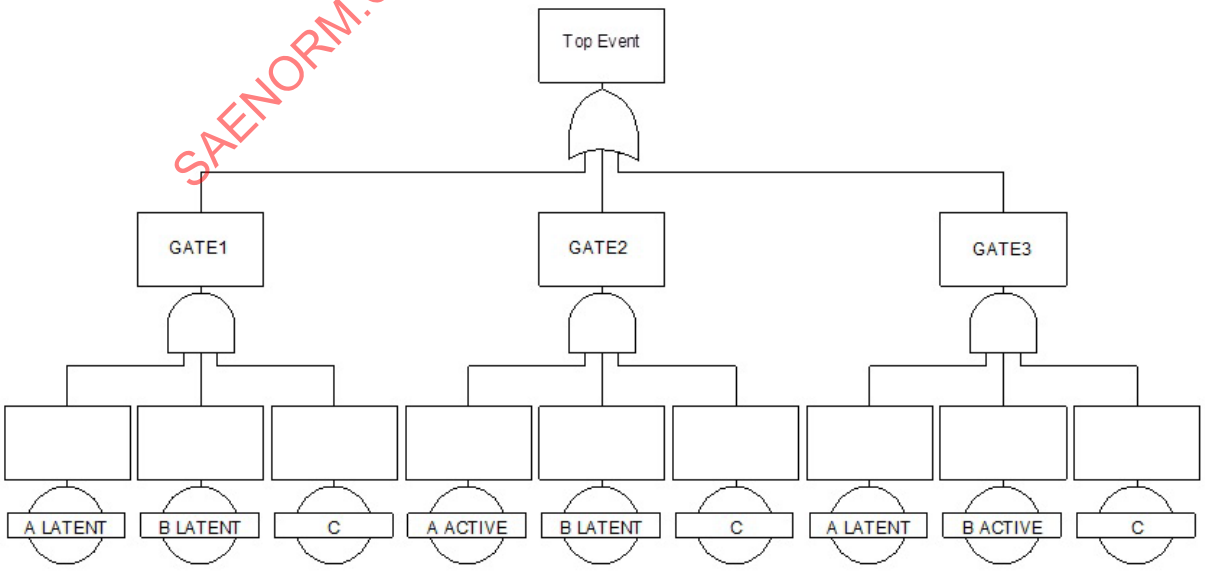


Figure G30 - Fault tree for combination of three events with two having latency

The cut set of Figure G30 for unavailability method effectively consists of the following:

$$P_{TE} = P_{A\text{-}LAT} * P_{B\text{-}LAT} * P_C + P_{A\text{-}ACT} * P_{B\text{-}LAT} * P_C + P_{A\text{-}LAT} * P_{B\text{-}ACT} * P_C$$

If “at risk” times are T_A = 50 hours and T_B = 1000 hours for $P_{A\text{-}LAT}$ and $P_{B\text{-}LAT}$, respectively, then:

$$P_{TE} = (5.00E\text{-}04)(1.00E\text{-}03)(2.50E\text{-}04) + (5.00E\text{-}05)(1.00E\text{-}03)(2.50E\text{-}04)$$

$$+ (5.00E\text{-}04)(5.00E\text{-}06)(2.50E\text{-}04)$$

$$P_{TE} = 1.38E\text{-}10$$

Dividing by flight time t = 5 hours results in an unavailability method result of = 2.76E-11 per flight hour.

The calculation of failure frequency for the same scenario can be based on the simple fault tree structure in Figure G29, since the failure frequency cut set formula contains the terms required to consider the latencies. P_A and w_A are calculated using the latency period T_A, but because w_A is insensitive to T_A, it effectively represents the rate of occurrence of active failures. The same logic applies to event B.

$$w_{TE} = w_A * P_B * P_C + P_A * w_B * P_C + P_A * P_B * w_C$$

$$= (1.00E\text{-}05)(1.00E\text{-}03)(2.50E\text{-}04) + (5.00E\text{-}04)(1.00E\text{-}06)(2.50E\text{-}04)$$

$$+ (5.00E\text{-}04)(1.00E\text{-}03)(5.00E\text{-}05)$$

$$w_{TE} = 2.76E\text{-}11/\text{hour}$$

NOTE: w_{TE} here has been calculated approximately using the λT method. However, a more accurate calculation based on the $\lambda e^{-\lambda t}$ method would produce a w_{TE} of 2.5E-11/hour, which is shown in Table G6.

The similarity in the results and the difference in fault tree structures of Figures G29 and G31 illustrate the advantage of potential simplicity offered by the failure frequency method. In large fault trees, the use of failure frequency instead of the unavailability method can result in a significant reduction in the number of gates and basic events. The effect of latencies on the failure frequency w of a cut set consisting of two to four basic events compared to the unavailability method is illustrated in Table G6. Table G6 entries assume the following failure rates: λ_A = 1.00E-05/hour, λ_B = 1.00E-06/hour, λ_C = 5.00E-05/hour, λ_D = 5.00E-06/hour, and flight duration t_f = 5 hours.

SAENORM.COM : Click to view the full PDF of arp4761a

Table G6 - Comparison of effect of failure event latency on unavailability FTA (P_f /t) rate and failure frequency

Combination (No Order/ Sequence)	Latency of Basic Event (hours)				Unavailability FTA (U-FTA) (Worst-Case Flight) "Unavailability Normalized": $P_{TE}(t_f)/t_f$	FF FTA (FF-FTA) Unconditional Failure Intensity: $w_{TE}(t_f)$	Ratio $w_{TE}/P_{TE}/t_f$ with Their Respective FTA:
	A	B	C	D	(failure/hr)	(failure/hr)	FF-FTA/U-FTA
AB	--	--	--	--	5.00E-11	1.00E-10	2.00
AB	50	--	--	--	5.00E-10	5.50E-10	1.10
AB	50	1000	--	--	1.04E-08	1.05E-08	1.00
ABC	--	--	--	--	1.25E-14	3.75E-14	3.00
ABC	50	--	--	--	1.25E-13	2.62E-13	2.10
ABC	50	1000	--	--	2.50E-11	2.76E-11	1.10
ABC	50	1000	10000	--	4.13E-09	4.14E-09	1.00
ABCD	--	--	--	--	3.12E-19	1.25E-18	4.00
ABCD	50	--	--	--	3.12E-18	9.68E-18	3.10
ABCD	50	1000	--	--	6.24E-16	1.31E-15	2.10
ABCD	50	1000	10000	--	9.83E-13	1.09E-12	1.11
ABCD	50	1000	10000	20000	3.92E-10	3.95E-10	1.01

NOTE: The fault trees used for calculation of combinations of failures used the method described in G.9.3.2 and G.9.3.3, but not using the simplification described in G.9.3.3 item c. Furthermore, calculations are only shown to two decimal places.

To exploit this simplicity without introducing erroneous modelling, the analyst should always be aware of the terms that constitute a failure frequency cut set. This is because the pictorial view of a failure frequency fault tree may not reveal all the products that constitute the cut set. However, this does not detract from the advantages offered by the correct construction of a failure frequency fault tree, but serves to illustrate that simplification compared to unavailability FTA modeling has limits. As an example, Figure G31 shows a fault tree that models an uncontained turbine overspeed event, requiring two electronic protection systems to fail in combination with a turbine shaft failure. Each protection channel has a latency period of 250 hours after which it would be repaired.

SAENORM.COM : Click to view the full PDF of arp4761a

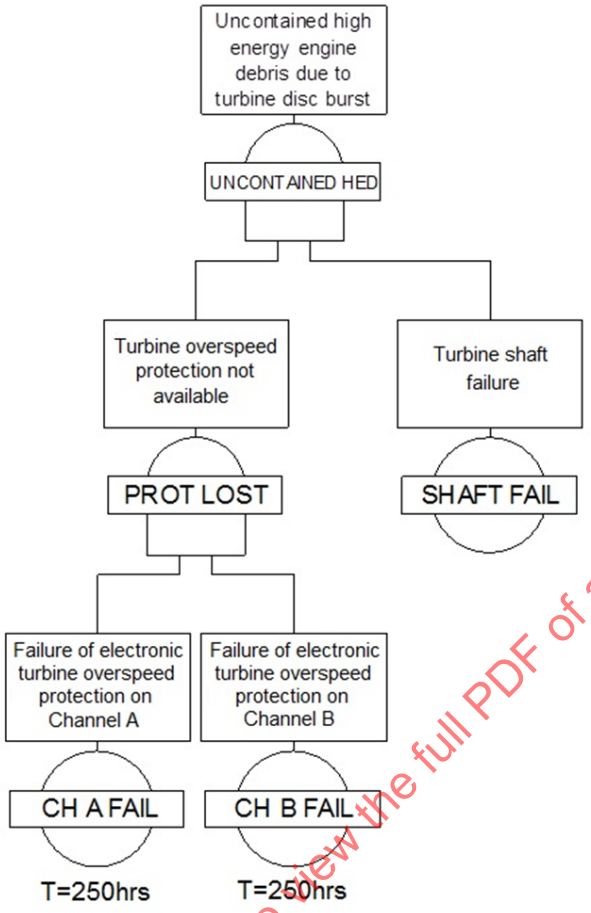


Figure G31 - Potentially overly simplistic fault tree for a hazardous turbine disc burst

The failure frequency cut set for the top event shown in Figure G31 is:

$$W_{UNCONTAINED\ HED} = W_{CH\ A\ FAIL} * P_{CH\ B\ FAIL} * P_{SHAFT\ FAIL} + P_{CH\ A\ FAIL} * W_{CH\ B\ FAIL} * P_{SHAFT\ FAIL}$$

$$+ P_{CH\ A\ FAIL} * P_{CH\ B\ FAIL} * W_{SHAFT\ FAIL}$$

Since the failure frequency calculation would use T for calculation of $P_{CH\ A\ FAIL}$ and $P_{CH\ B\ FAIL}$, the last product of the cut set represents a latent failure of both protection functions and its inclusion would be erroneous if the system does not allow the combination of failure of both protection channels for 250 hours. If only one channel is allowed to fail for 250 hours and failure of the second system would prohibit further operation of the turbine system, then the fault tree structure is overly simplistic and would produce a result that is overly conservative. To prevent this, the analyst needs to construct a more complex fault tree in a way that eliminates combinations of such latent failures.

SAENORM.COM : Click to view the full PDF of arp4761a

G.12.4 Sequencing in Fault Trees Using Failure Frequency

Sequencing of failure events allows the analyst to reduce the conservatism in the fault tree results by eliminating sequences that would not contribute to the top event.

a. Enabler event: An event which must occur at any position other than the last in a sequence to cause a failure.

   The logic is that enablers only have probabilities, either based on the system time or a latency period. An enabling event is considered to have occurred already, cannot fail again and hence, has a probability, not a failure frequency.

b. Initiator event: An event that must be the last event to occur in a sequence to cause the system failure of interest.

   Initiators do not have probabilities, only a failure frequency.

Consider the example of a combination of three events A, B, and C. As before:

$$w_{TE} = w_A * P_B * P_C + P_A * w_B * P_C + P_A * P_B * w_C$$

If the top event would only occur when A and B fail before C, then A and B can be designated to be enablers as shown in Figure G32.

In the cut set for w_{ABC}, events A and B are designated to be enablers and hence, do not have failure frequencies, only probabilities. Products containing w_A and w_B are eliminated, leaving only:

$$w_{ABC} = P_A * P_B * w_C$$

Alternatively, event C can be designated to be an initiator in a similar fashion as is shown for enablers in Figure G32. In this case, event C has no probability of failure P_C, only a failure frequency w_C. The calculation result would be the same:

$$w_{ABC} = P_A * P_B * w_C$$

In software packages that provide the option to calculate fault tree results in failure frequency, the elimination of the products, as shown above, is done automatically when enablers and initiators are designated.

It is important to note that the result of an AND-gate having only enablers or only initiators as inputs is meaningless, since in a combination of failure events not all can be enablers or initiators.

SAENORM.COM : Click to view the full PDF of arp4761a

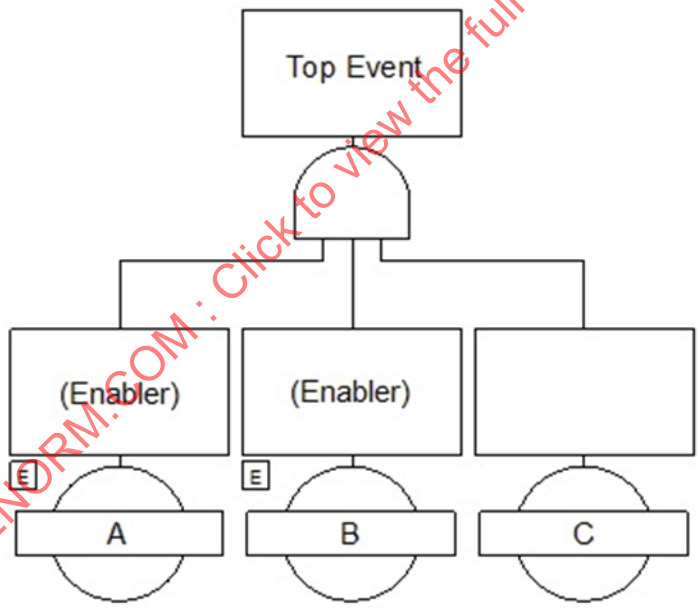


Figure G32 - Assigning enablers in a combination of failure events

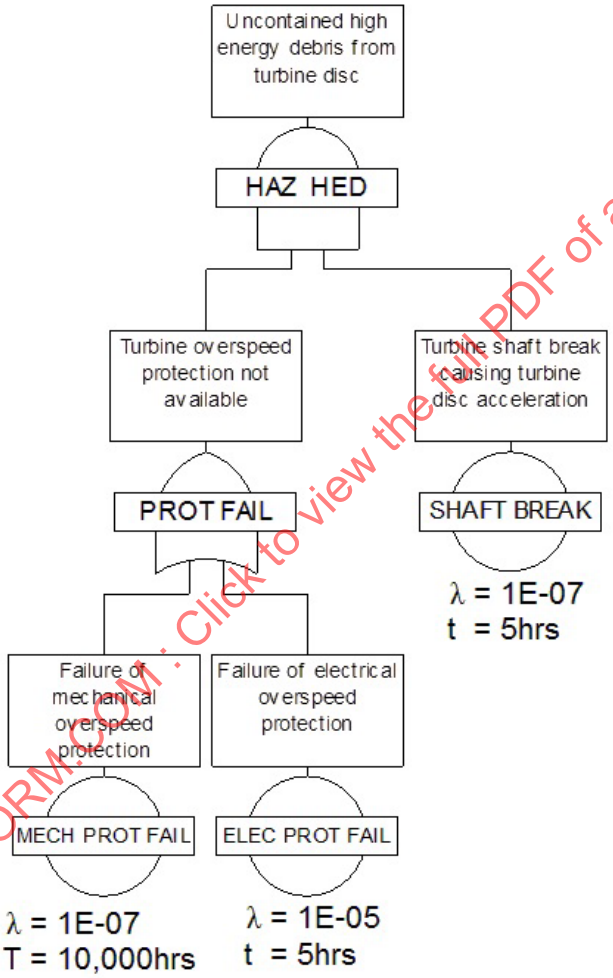
In both cases, P_f of the top event can still be calculated by the product $P_A * P_B * P_C$ but there is no longer any meaningful relationship between the rate represented by FF and unavailability for the top event. As a rule, any failure frequency fault tree that contains any enablers or initiators will produce a top event probability Pf that has no meaning. Only the failure frequency, w, is used. In an unavailability fault tree, the probability of the top event would have to be calculated by considering all combinations and then applying a required order factor as shown in G.11.1.4. This is one of the aspects that would preclude a direct integration of a failure frequency fault tree into an unavailability method fault tree.

G.12.5 Conversion from Failure Frequency FTA to Unavailability FTA

It is not advised to re-calculate a fault tree that has been constructed for failure frequency to determine unavailability P_f/t result. The result may be erroneous because of the differences between how the two methods are calculated. Every gate in a fault tree built for failure frequency would have either a probability P_f, or a failure frequency w, or both.

If a fault tree analyst wishes to use the result of a gate in a failure frequency fault tree as an undeveloped event in an unavailability fault tree, the question arises on which parameter (P_f or w) from the frequency model gate to use. The answer depends on what the frequency model gate represents.

For gates or sub-trees that include latent failures, P_f is used as illustrated by the gate PROT FAIL in Figure G33.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure G33 - FF FTA example where the result of P_f is used when converting to unavailability FTA

The results in a failure frequency calculation for gate PROT FAIL are:

$$w_{PROT\ FAIL} = 1.01E\text{-}05/hour$$

$$P_{PROT\ FAIL}/t_f = 2.10E\text{-}04/hour$$

The ratio between w and P_f for this gate is not simply represented by the system time t = 5 hours. To get the correct input into an unavailability fault tree, where the gate PROT FAIL is represented by an undeveloped event, $P_{PROT\ FAIL}/t_f$ = 2.10E-04/hour is used.

a. For gates or sub-trees representing only non-latent effects, w should be used as being equivalent to λ (for small values of w) or P_f/t where t represents the system time (e.g., flight time).

b. For gates representing enabling events in a failure frequency fault tree, it is recommended not to use either (w) or (P_f), but to re-build the fault tree in a way that all sequences are represented and to then apply a required order factor as explained in G.11.1.4.

Table G7 presents the (P_f/t) results obtained from using the same FF fault tree used to calculate Table G6 (Table G7, Column 7), and the same unavailability fault tree from Table G6 but computed with the P_f/t (Table G7, Column 6). For these particular examples, this table shows that the FF "simplified" fault tree computed with the P_{TE}/t_f is equivalent or conservative compared to the results given by the Unavailability "detailed" fault tree computed with its appropriate characteristic: P_{TE}/t_f.

Table G7 - Comparison of P_f/t results from unavailability and FF fault trees

Combination (No Order/ Sequence)	Latency of Basic Event (hours) A	B	C	D	Unavailability FTA (U-FTA) (Worst-Case Flight) "Unavailability Normalized": $P_{TE}(t_f)/t_f$ (failure/hr)	FF FTA (FF-FTA) "Unavailability Normalized": $P_{TE}(t_f)/t_f$ (failure/hr)	Ratio of Different FTAs with $P_{TE}(t_f)/t_f$ Computation: FF-FTA /U-FTA
AB	--	--	--	--	5.00E-11	5.00E-11	1.00
AB	50	--	--	--	5.00E-10	5.00E-10	1.00
AB	50	1000	--	--	1.04E-08	9.99E-08	9.57
ABC	--	--	--	--	1.25E-14	1.25E-14	1.00
ABC	50	--	--	--	1.25E-13	1.25E-13	1.00
ABC	50	1000	--	--	2.50E-11	2.50E-11	1.00
ABC	50	1000	10000	--	4.13E-09	3.93E-08	9.52
ABCD	--	--	--	--	3.12E-19	3.12E-19	1.00
ABCD	50	--	--	--	3.12E-18	3.12E-18	1.00
ABCD	50	1000	--	--	6.24E-16	6.24E-16	1.00
ABCD	50	1000	10000	--	9.83E-13	9.83E-13	1.00
ABCD	50	1000	10000	20000	3.92E-10	3.74E-09	9.55

SAENORM.COM : Click to view the full PDF of arp4761a

G.12.6 Conversion from Unavailability FTA to Failure Frequency FTA

An unavailability fault tree constructed in accordance with the methods for producing a P_f/t result can be directly used to obtain a result for failure frequency without any conversion. The failure frequency result would be conservative because failure combinations involving latent and active failures would automatically add additional products in the cut set calculations. To illustrate this, Table G8 presents the failure frequency results obtained from using the same FF fault tree used to calculate Table G6 (Table G8, Column 7), and the same unavailability fault tree from Table G6, but computed with the w_{TE} (Table G8, Column 6).

Table G8 - Comparison of failure frequency results from unavailability and FF fault trees

Combination (No Order/ Sequence)	Latency of Basic Event (hours) A	B	C	D	Unavailability FTA (U-FTA) (Worst-Case Flight) Unconditional Failure Intensity: $w_{TE}(t_f)$ (failure/hr)	Failure Frequency FTA (FF-FTA) Unconditional Failure Intensity: $w_{TE}(t_f)$ (failure/hr)	Ratio of Different FTAs with w_{TE} Computation: U-FTA/FF-FTA
AB	--	--	--	--	1.00E-10	1.00E-10	1.00
AB	50	--	--	--	6.00E-10	5.50E-10	1.09
AB	50	1000	--	--	1.06E-08	1.05E-08	1.01
ABC	--	--	--	--	3.75E-14	3.75E-14	1.00
ABC	50	--	--	--	2.75E-13	2.62E-13	1.05
ABC	50	1000	--	--	3.02E-11	2.76E-11	1.10
ABC	50	1000	10000	--	4.20E-09	4.14E-09	1.01
ABCD	--	--	--	--	1.25E-18	1.25E-18	1.00
ABCD	50	--	--	--	1.00E-17	9.68E-18	1.03
ABCD	50	1000	--	--	1.38E-15	1.31E-15	1.05
ABCD	50	1000	10000	--	1.19E-12	1.09E-12	1.10
ABCD	50	1000	10000	20000	3.96E-10	3.95E-10	1.00

Before initiator or enabler logics are applied, the analyst first checks that sequencing has not already been accounted for by the application of a required order factor.

G.13 ANALYZE AND SUMMARIZE THE FTA RESULTS

After the tree is constructed, the analyst will need to normalize and then summarize the fault tree data, and document the results of the FTA.

G.13.1 Fault Tree Data Analysis—Normalizing the FTA Numerical Calculation

Numerical safety objectives are typically identified in terms of “probability of failure per flight hour.” The guidelines presented in this appendix highlight techniques for creating fault trees which calculate a “probability of failure per flight” result. If the system under analysis has “per flight hour” objectives, the analyst normalizes the undesired top event probability of failure number. The analyst accomplishes the normalization of P_f(top) by dividing the top event probability result by the flight time, to report the probability of failure per flight hour.

When the FHA failure condition objective or a safety requirement is identified on a per flight phase basis the FTA may be calculated using the time associated with the flight phase as the “at risk” time (t_f). This results in an FTA result that is in the necessary “probability per flight phase” units.

G.13.2 Summarizing Fault Tree Analysis Results During SSA/ASA Process

One method for summarizing the FTA data is to construct an FTA data summary chart. This chart uses a columnar format which provides an engineering management or a Certification Authority reviewer with easy access to all the pertinent FTA criteria and results. Table G9 provides an example of this type of chart.

SAENORM.COM : Click to view the full PDF of arp4761a

Table G9 - Example of a system indenture level FTA data summary chart

Safety Design Criteria			Analysis Results		
List of Top-Level Events (from FHA)		Corresponding Maximum Allowable Probability	Systems Probability of Occurrence	Compliance (Yes or No)	Corrective Action
Function #	Description				
4A1	Loss of all altitude display in flight deck	1.0E-09	5.0E-09	No	Redesign air data system or add more detail to LRU FTA
4A2	Loss of primary altitude on both pilot PFDs	1.0E-07	1.0E-07	Yes	None
- additional rows as need to report FTA results					

The numbers entered into the “Corresponding Maximum Allowable Probability” column are based on the failure condition classification for the given top-level event.

The analyst can now tie the FTA boundaries and summarize FTA results. Table G9 illustrates that Function #4A1 does not meet its top-level event safety requirement at the system indenture level (e.g., FTA basic events are LRU level failure modes) and possible corrective actions include redesigning the system or increasing the FTA scope by further analyzing down below the LRU level failure modes. Assuming Function #4A1B55 is the primary event in the Function #4A1 system indenture level FTA, Table G10 provides an example of a summary table for an LRU indenture level FTA. Table G10 shows that Function #4A1B55 does not meet its top-level event safety requirement. Possible corrective actions include further increasing the detail in the FTA (e.g., expand basic events into more detailed branches) or implementing a design change (e.g., add redundancy or monitors).

Table G10 - Example of an LRU indenture level FTA data summary chart

Safety Design Criteria			Analysis Results		
List of Top-Level Events (from FHA)		Corresponding Maximum Allowable Probability	Systems Probability of Occurrence	Compliance (Yes or No)	Corrective Action
Function #	Description				
4A1B55		1.0E-09	1.0E-08	No	Perform more detailed FTA or HW/SW change
4A1B56		1.0E-05	1.0E-07	Yes	None
- additional rows as need to report FTA results					

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX H - DEPENDENCE DIAGRAM (DD)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

H.1 INTRODUCTION 168

H.2 SCOPE 168

H.3 BASIC LOGIC ARRANGEMENT 168

H.4 PICTORIAL REPRESENTATIONS OF EVENTS 169
H.4.1 Failure Modes 169
H.4.2 Failure Condition 169
H.4.3 External Events 170
H.4.4 DD Supporting Function Development Assurance Level and Item Development Assurance Level Assignment 170

Figure H1 Series/parallel combinations 168
Figure H2 Fully developed failure mode internal to the system 169
Figure H3 Undeveloped failure mode internal to the system or external failure mode 169
Figure H4 Indirect probability 170
Figure H5 Failure or event external to the aircraft 170
Figure H6 Error DD example 171

SAENORM.COM : Click to view the full PDF of arp4761a

H.1 INTRODUCTION

Dependence Diagrams (DD) may be used as an alternate method of representing the failure model data. This provides an alternate, pictorial representation to the Fault Tree Analyses (FTAs) of combinations of failures for the purpose of safety analysis. The processes and methods explained and described in Appendix G for FTAs also generally apply to DDs. The principal differences between FTAs and DDs are that DDs have no additional logic symbols, because they show the logic by serial or parallel arrangement of boxes. DDs do not show intermediate events which would appear in FTAs as descriptions of the output of a logic symbol. The DD is analytically identical to the FTA, and the role of the DD in the safety assessment process is the same as the role of FTAs. The guidelines in this appendix deal with DD unique issues not covered by the FTA process in Appendix G.

H.2 SCOPE

This appendix presents the logic arrangements, the analysis procedure, and the pictorial representation of several different types of events. Variations and additions on the event representations may be applied as necessary to support a specific analysis. This appendix provides guidance to enable an engineer experienced in FTA to apply the Dependence Diagram method.

H.3 BASIC LOGIC ARRANGEMENT

Each Dependence Diagram represents a failure condition (unwanted top event). It is constructed utilizing rectangular boxes, which represent fault events leading to the top event. These boxes are arranged in series or parallel formation. Series chains are OR situations, while parallel chains represent AND situations. Figure H1 presents the DD graphic method concept.

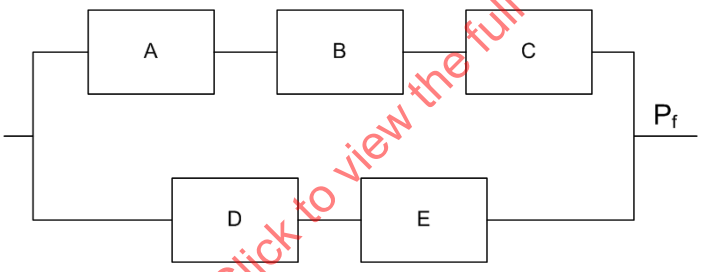


Figure H1 - Series/parallel combinations

The probability of the overall failure condition P_f in the DD shown in Figure H1 is approximately given by:

$$P_f = (P_fA + P_fB + P_fC) * (P_fD + P_fE) \text{ per flight} \quad \text{(Eq. H1)}$$

The arrangement shown is simplistic in order to introduce the reader to the basic philosophy. The Dependence Diagrams can become quite complex and may involve the multiple use of single failures throughout the diagram, in which case the application of Boolean algebra will be required in order to complete the probabilistic calculations and generate the minimal cut sets.

All the qualitative and quantitative evaluations using minimal cut sets are identical to those made with the FTA cut sets as described in the following paragraphs of Appendix G.

a. Qualitative importance determination (Section G.10.2).

b. Quantitative fault tree evaluation using unavailability method (Section G.11).

c. Quantitative fault tree evaluation based on failure frequency (Section G.12).

Errors can be incorporated into DD in the same way as in FTA, as described in G.10.3.

SAENORM.COM : Click to view the full PDF of arp4761a

H.4 PICTORIAL REPRESENTATIONS OF EVENTS

Dependence Diagrams are usually constructed utilizing rectangular boxes. Variations in the form of the boxes can be used to depict different conditions, similar in manner to the variety of shapes used in FTA. Examples are described in the following paragraphs.

H.4.1 Failure Modes

The “solid line” box depicts a failure mode which is internal to the system being analyzed and which needs no further development. This is comparable to a circle representation in fault trees. In the Preliminary System Safety Analysis (PSSA), the box contains a description of the failure mode and the budgeted failure rate with associated risk time and/or exposure time. In the System Safety Assessment (SSA), the budgeted failure rate may be replaced by the actual failure rate and may include the source. Figure H2 is an example from an SSA Dependence Diagram.

This example indicates that the failure “Loss of speed signal” is referenced back to an FMES, with a failure rate of 1.0E-06 and the risk time for that failure of 5 minutes.

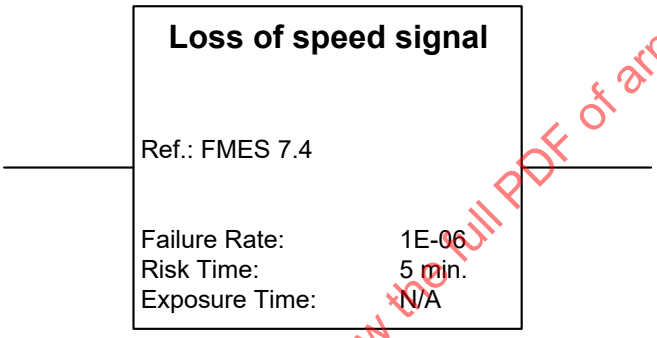


Figure H2 - Fully developed failure mode internal to the system

H.4.2 Failure Condition

A box drawn with “dashed” lines depicts another failure condition of the system under investigation or failure condition of another system. This box is comparable to a sub-tree in FTA.

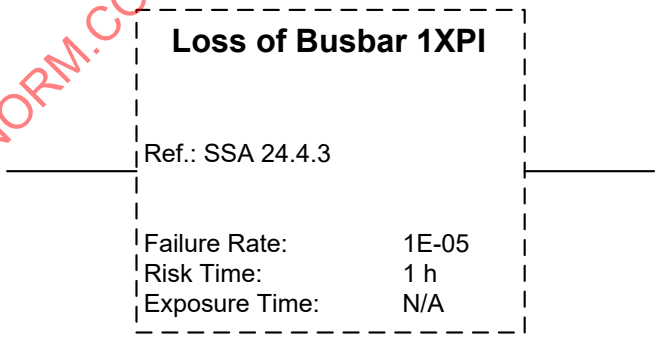


Figure H3 - Undeveloped failure mode internal to the system or external failure mode

The example in Figure H3 indicates that “Loss of Busbar 1XPI” can be found in the referenced SSA.

A box which has a diagonal cross depicts a failure mode for which the probability of failure cannot be directly derived from its stated λ and t. This box may be a further subset Dependence Diagram in its own right, and has to be referred to directly in order to determine its probability of failure. This box is shown in Figure H4.

SAENORM.COM : Click to view the full PDF of arp4761a

Take care when using these failure condition boxes in the probability calculation of the Dependence Diagram. They only show the top level of another Dependence Diagram, which could contain common elements with the Dependence Diagram under investigation. They may also contain exposure times different from the ones considered in the original Dependence Diagram.

Perform calculations with the complete Dependence Diagram structure for the failure condition of concern, and not by simply using the probability of that failure condition in the calculation.

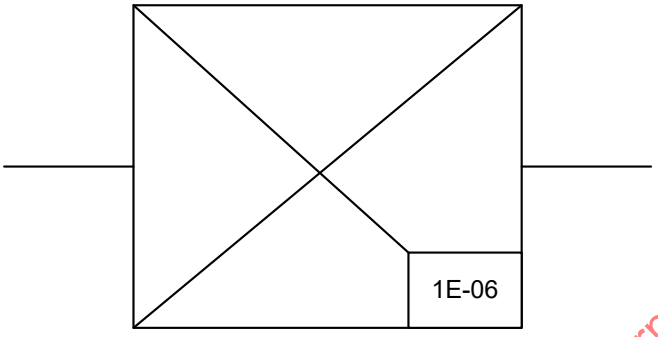


Figure H4 - Indirect probability

H.4.3 External Events

A “dotted” line box depicts an event which is external to the aircraft; for example, cross wind greater than 20 knots.

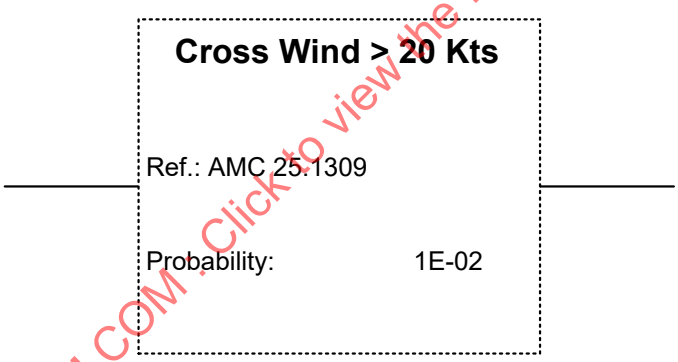


Figure H5 - Failure or event external to the aircraft

SAENORM.COM : Click to view the full PDF of arp4761a

The example in Figure H5 indicates that cross wind greater than 20 knots exist with a probability of 1.0E-02 per flight and the reference for the probability.

H.4.4 DD Supporting Function Development Assurance Level and Item Development Assurance Level Assignment

A Dependence Diagram may be used to support Function Development Assurance Level (FDAL) and Item Development Assurance Level (IDAL) assignment activities (see Appendix P). When supporting the FDAL/IDAL assignment process, the DD is constructed of potential error sources rather than failure mechanisms. An example of a Dependence Diagram which includes the consideration of errors is presented in Figure H6.

Figure H6 illustrates the potential error sources which when combined could cause the undesired failure condition event. For the Figure H6 example, two independent functions (F_1 and F_2) have to contain errors for the failure condition 2 (FC2) to occur. The sources of function error may be either in the development of the Functions (F_1, F_2) or in the development of the Items (I_1, I_2). This DD is a model of the planned development environment associated with the two functions. The minimum number of errors which will cause the DD result to be true is called a Functional Failure Set.

The FDAL/IDAL assignment activity may now use the DD qualitative presentation, in combination with all other failure conditions error DDs to derive an appropriate assignment.

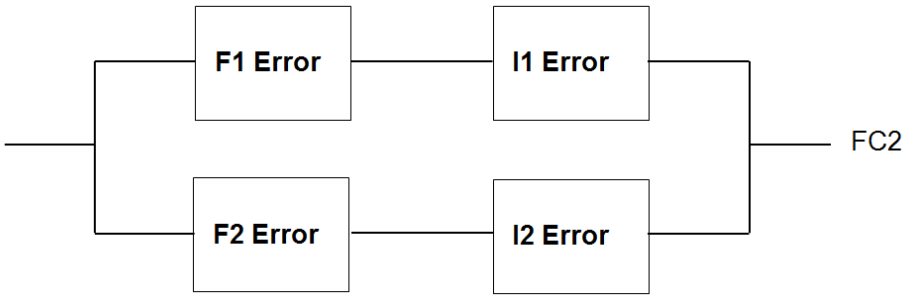


Figure H6 - Error DD example

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX I - MARKOV ANALYSIS (MA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

I.1 INTRODUCTION 174
I.1.1 Markov Models 174
I.1.2 What is a Markov Analysis? 175
I.1.3 Markov Model State Equations 176
I.1.4 Average System Failure Rate 177

I.2 BACKGROUND 178
I.2.1 Advantages of Markov Analysis 178
I.2.2 Limitations of Markov Analysis 178
I.2.3 Failure/Repair Scenarios and Modeling Strategies 179
I.2.4 Systems with Latent Faults 180
I.2.5 Systems Maintained on a Regular Schedule 180
I.2.6 Systems Sensitive to Sequence of Failures 180
I.2.7 Discrete Repair versus Continuous Repair Scenarios 181
I.2.8 Conditional Maintenance Scenarios 181
I.2.9 Phased Mission Systems 181
I.2.10 Time-Limited Dispatch (TLD) and MMEL Relief 182

I.3 MODELING STRATEGIES 182
I.3.1 Modeling Discrete Repairs 183
I.3.2 Repair Strategies Used In-Service 187
I.3.3 Simulating Repairs in Markov Models 187

I.4 MARKOV MODELING - DISCUSSION AND EXAMPLES 193
I.4.1 A Simple Open-Loop MM for a Two-Equipment System with Continuous Repair Transitions 193
I.4.2 Open-Loop and Closed-Loop Markov Models 193
I.4.3 Simplifying Markov Models - When Possible and Practical 198
I.4.4 Comparison of a Closed-Loop Continuous Repair MM to a Closed-Loop Discrete Repair MM - Two Solutions Equivalent 206
I.4.5 Example of an Average Failure Rate Analysis for an Active System (Which Has Internal Fault Monitoring) and a Backup System (Which Has an External Fault Monitor) 214
I.4.6 A Discussion of Model Completeness 219
I.4.7 Examples of System Analyses Where Sequential Calculations Are and Are Not Immediately Available 221
I.4.8 Non-Homogeneous versus Homogeneous MMs 225
I.4.9 Transient Analysis 225
I.4.10 Solution of Markov Chains 226
I.4.11 Reliability Metrics (Rates, Probabilities) 227

I.5 ANALYSIS TOOLS 239
I.5.1 Spreadsheet Calculations 240

I.6 SUMMARY 240

Figure I1 Triple redundant system Markov Model (chain) with no repair 174
Figure I2 Transitions into and out of state P_j 176
Figure I3 Simple two-equipment system block diagram 180
Figure I4 MM Showing the two different sequential failure states 181
Figure I5 MM for the two-equipment system with continuous repair for each failed equipment 182
Figure I6 Closed-loop MM simulating discrete repair with continuous repair from State 2 183
Figure I7 Open-loop MM showing discrete repair from State 2 184
Figure I8 Failure rate of two-equipment system over time 186

SAENORM.COM : Click to view the full PDF of arp4761a

Figure I9 Time between two periodic inspections 188
Figure I10 $T_{TSF}/T_{Inspect}$ as a function of $T_{Inspect}/T_{MTBF}$ 190
Figure I11 $T_{Inspect}/T_{TSF}$ as a function of T_{TSF}/T_{MTBF} 191
Figure I12 Closed-loop model for the simple two-equipment system 194
Figure I13 MM for Simple two-equipment system with μfb = ∞ 197
Figure I14 Equipment system with each equipment having the same failure and repair rates 198
Figure I15 Two-bus, three-equipment system 199
Figure I16 MM for two-bus, three-equipment system 201
Figure I17 Failure rates for the system bus portion, system equipment portion, and their sum, which is the total failure rate of the system 203
Figure I18 Markov Model for bus failures 204
Figure I19 Markov Model for three-equipment failures 204
Figure I20 MM used for the discrete repair simulation of the two-equipment system example 208
Figure I21 Failure rate time history for the two-equipment system using discrete repair with different repair times for the equipment 212
Figure I22 Diagram of active system with self-monitoring and back-up system with an independent monitor 214
Figure I23 Markov Model for an active system with internal self-monitoring and a backup system with independent monitor 215
Figure I24 Impact of equal repair rates for the back-up and monitor system on the system failure rate 219
Figure I25 MM for active/back-up, monitor system of Figure I23 without the active/monitor (P5) dual equipment failure state 220
Figure I26 Four-channel system with all repairs to full-up state 222
Figure I27 Four-channel system with repairs to intermediate states 223
Figure I28 Non-Homogeneous MM for dual-redundant system with aging equipment 225
Figure I29 MM for two-equipment system with no repair to a single equipment failed 230
Figure I30 Two-equipment MM with instantaneous return to fully failed state 230
Figure I31 Ratio of average renewal rate to the steady-state renewal rate at t = ∞ 231
Figure I32 Average hazard rate and renewal rates as a function of time 232
Figure I33 Three-equipment System with no repair until all equipment failed 232
Figure I34 MM for three-equipment system with instantaneous repair 232
Figure I35 Ratio of average renewal rate at time t to average renewal rate at t = ∞ 234
Figure I36 Two-equipment system for first phase where either equipment failed yields system failure 238
Figure I37 Two-equipment system for second phase 238

Table I1 Calculation of system failure rate for two-equipment system using a discrete repair simulation 185
Table I2 Values for the ratios P1/PFU through P5/PFU and the system failure rate (per hour) 202
Table I3 Markov Model spreadsheet for two separate systems: one for two-bus system (Figure I12) and the three-equipment system (Figure I14) 205
Table I4 Time-dependent calculations for the simple two-equipment system with different repair times for the equipment 210
Table I5 Spreadsheet for system failure rate calculations for active/back-up/monitor system of Figures I22 and I23 217
Table I6 Active/back-up/monitor system failure rates as a function of the back-up and monitor equipment repair rate when those repair rates are the same 218
Table I7 Comparison of system failure rate calculation results with and without P5 state 221
Table I8 Spreadsheet for solving system of equations where a sequential calculation of the probability ratios is not immediately possible 224
Table I9 Probabilities for being in states of operation of a two-equipment system where each equipment has Weibull failure distribution with shape beta of 2.0 and a characteristic life eta of 1000 hours 236

SAENORM.COM : Click to view the full PDF of arp4761a

I.1 INTRODUCTION

Much has been altered in the rewrite of this appendix. The changes are directed toward a presentation of “open-loop (acyclic)” and “closed-loop (cyclic)” Markov models (MM) and showing the benefits of each model type for the system analysis scenario where they apply.

This appendix presents an intuitive understanding of Markov Analysis (MA) without much of the complexity of the underlying mathematics.

I.1.1 Markov Models

A Markov model is a state-space representation of the system, which allows the behavior of a system to be analyzed using the theory of Markov processes. Markov processes are a special class of stochastic or random processes that exhibit a singular property (named the Markov property): the process is memory-less. This means that the predicted future operation of the system only depends on its current state, and is not predicated, altered, or affected by any of its history. When the past history of the process is completely summarized in the current state and is independent of the current time, then the MM is said to be (time) homogeneous one. Otherwise, the exact characterization of the present state needs the associated time history information, and the MM is said to be non-homogeneous. Throughout this document, the discussion assumes the MMs to be homogeneous, unless stated otherwise.

Markov models can be classified according to the nature of state space into processes (continuous state space) or chains (discrete state space). In particular, Markov chains (MC) have shown wide applicability to the performance, reliability, maintainability, and safety analyses of complex systems. Markov chains are visually represented by directed graphs (called “state-transition diagrams”) with nodes or “bubbles” representing system states and arcs capturing the dynamic system behavior through defined state transitions. Figure I1, for example, shows a Markov model for a triple equipment redundant system where all three equipment need to fail for the system to be considered failed.

Markov chains can be further classified based on the nature of the transitions. If a state transition is allowed at any given time, then the MC is called a “continuous-time Markov chain (CTMC)”. If the state transitions can only occur at specific times, the MC is called a “discrete-time Markov chain (DTMC)”. State transitions in CTMCs are labeled by exponential-distribution rates (see Figure I1), while in DTMCs the transitions are labeled by geometric-distribution probabilities.

SAENORM.COM : Click to view the full PDF of arp4761a

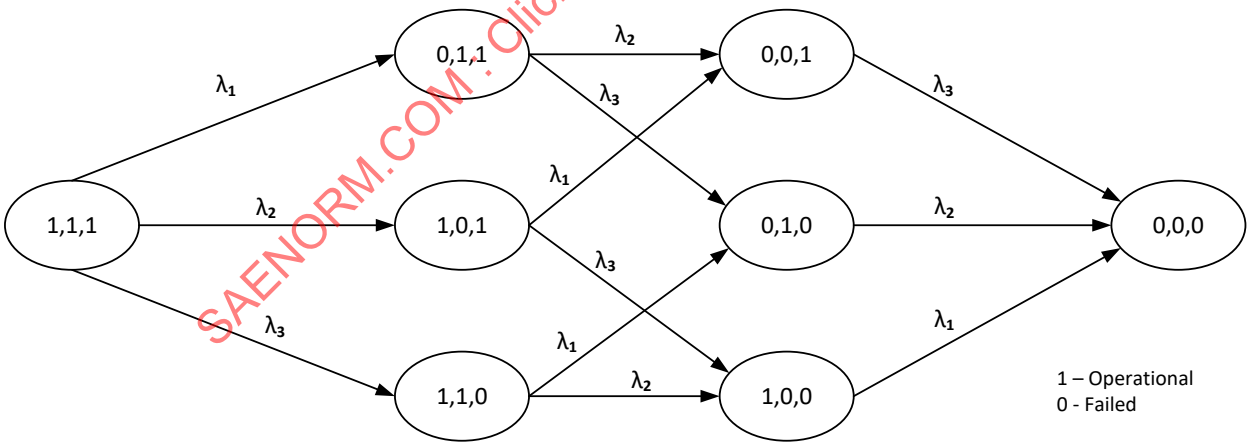


Figure I1 - Triple redundant system Markov Model (chain) with no repair

The Markov model states are shown by a simple triple digit vector, e.g., (0, 1, 1) with a separate counter for each equipment to represent the operational state of each of the three equipment. In this system, 0 represents a failure of the equipment and 1 represents its properly working condition. In this model, no repair transitions are modeled, so all transitions from one state to another are due to failures of one of the equipment. Figure I1 shows the various failure transitions. For simplicity, this particular system shows no repair transitions for the various failure states. Repairs are an important part of Markov models and the modeling of repairs is discussed in detail in this appendix.

Each state is mutually exclusive of the others, but the path(s) to that state will be a function of transitions (i.e., failures and repairs into that state) from the other states. The final failure state of the system is generally the state in which the system can no longer function because all redundant elements of the system are in a failed state. In the triple channel system, this would be represented by the (0, 0, 0) vector notation.

Failure and repair transitions between states are labeled by the rate at which such transitions occur, namely the failure rate (failures/hour) and repair rate (repairs/hour) associated with the various equipment being modeled. To complete the model one needs to specify the initial state of the system. Typically, this is the starting “All Operational (or Full Up)” state, which is shown by the triple (1,1,1) state in Figure I1. The output of a model is the probability that the system is in any particular state as a function of time. This is quantified by what are termed the “state probabilities” of the system. For example, the probability that the system is in the fully failed state, which is the (0, 0, 0) state in Figure I1, or any other state in that diagram, will be a function of the failure rates for the various equipment, and the model will yield this probability as a function of time. It is always a “conservation requirement” that the sum of all state probabilities be equal to unity.

Markov models are normally solved by representing the state space by a set of time dependent ordinary differential equations (ODEs), the solution of which yields the probabilities of being in the various system states as a function of time. As the time increases, the probability of the system failure increases. As the time approaches infinity, the state probabilities asymptotically approach steady-state values. This appendix presents two implementations of the solutions of MCs.

1. First, when discrete repair is being modeled, the MC solution is represented by ODEs which are solved to yield the probability time histories for the various states. The results can be plotted as graphs. These probability time histories are then used to estimate the average system failure rate. The details of examples are shown using spreadsheets.

2. Second, when continuous repair transitions are used to approximate discrete repair actions, it is shown that the system ODEs can be simplified to a set of algebraic equations, whose solution provides an excellent approximation to the average system failure rate. Detailed example calculations are also provided for these types of models. This technique is very useful when the MCs are small and less complex. Examples of this type of implementation abound in this appendix.

Note that Markov Chains for larger complex systems are analyzed by solving the ODEs (transient case) and the algebraic (steady-state case) by computerized solvers.

I.1.2 What is a Markov Analysis?

The previous section showed the MM of a simple triple redundant system with no repair. As stated above, this type of MM will yield the state probabilities for each state being modeled as a function of time and, since there is no repair, the state probabilities will always be changing with time. This is called a transient analysis model, and such a model is also referred to herein as an “open-loop” model. The “open-loop” terminology is used to indicate that a model is not simulating any repair from the fully failed state to the full-up or any other state. Once the state probabilities for all times are known, other measures such as Mean Time To Failure (MTTF) can be calculated from the probability time histories.

Another type of MA would be to ascertain the state probabilities after a long period of system operation with repair. Repairs can be simulated from the fully failed state as well as all other states, excepting, of course, the full-up state. This is called an “MA steady-state analysis.” When repair from the fully failed state is modeled, the model is herein called a “closed-loop” model. Once the state probabilities are obtained from an MM, then other measures such as reliability, average probability of failure per hour (failure rate) of the system can be calculated. As discussed herein, the use of the steady-state approach with continuous repair provides a simpler method for computing the average system failure rate, particularly when the equipment MTBFs and repair times are much shorter than the life of the fleet of aircraft in which the system resides.

Hence, an MA is defined as a process, technique, or method of deriving the state probabilities of an MC. The solution to the linear differential equations that describe/represent the system yields the probability of being in each of the defined states as a function of time. A simple derivation of the linear differential equations is provided in I.1.3.

SAENORM.COM : Click to view the full PDF of arp4761a

I.1.3 Markov Model State Equations

The state equation for each state is determined from the probability flow into and out of that state. The total probability flow into a given state is the sum of all transition rates into that state, each multiplied by the probability of the state at the origin of that transition, or the probability of the state "driving" the particular transition rate. The probability flow out of the given state is the sum of all transition rates out of the state multiplied by the probability of that given state. The state equation for a given state is defined as the time-rate-of-change of that state's probability, dP/dt, which is equal to the probability flow into that state minus the probability flow out of that state.

Consider the probability state diagram shown in Figure I2.

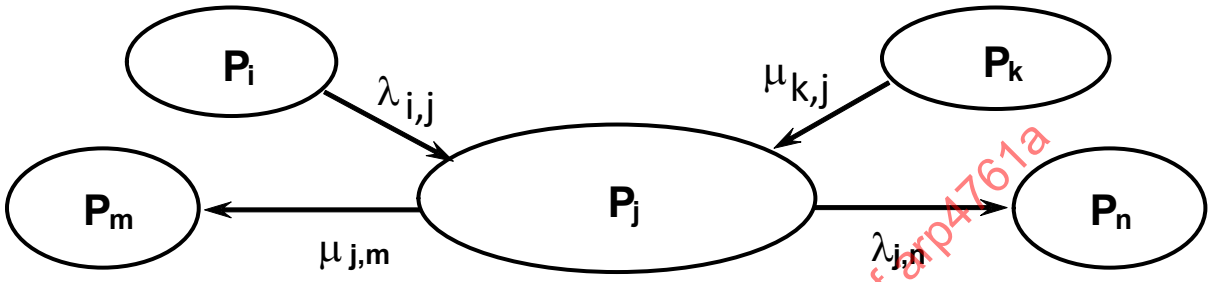


Figure I2 - Transitions into and out of state P_j

In this diagram, the different bubbles represent different system states, or configurations. Most all of the states in an MM will be operating states (or configurations) which simulate system operation with one or more failures. In Figure I2, P_i, P_j, and P_k represent the probabilities of the system being in those particular states or configurations, which are somewhere between full-up and complete system failure. This will become more obvious through the examples presented herein. If no repair of the various fault states being simulated is modeled, the probabilities of being in those various fault states will continue to change with time as the system progresses to failure. If repair is undertaken, the various state probabilities can become constant with time. This will be illustrated in the examples presented. Lambdas (λ) are generally used to represent failure rates. In Figure I1, $\lambda_{I,j}$ represents the failure rate of operative equipment or elements in the P_i state that would cause the system to transition to the P_j state. $\lambda_{j,n}$ presents the failure rate of operative equipment in the P_j state that would cause the system to transition to another (P_n) state. Mu (μ) is generally used to represent repair rates. In the diagram, $\mu_{k,j}$ represents the repair rate from the P_k state to the P_j state, and $\mu_{j,m}$ represents the repair rate from the P_j state to another (P_m) state. The time-rate-of-change of the probability of being in a particular state is determined from the probability flow into that state minus the probability flow out of that state. The probability flow into a state is the sum of all of the failure rate and repair rate transitions into that state multiplied by the probabilities of the states "pushing" those transitions. For the state P_j, this is illustrated in Equation I1.

Probability flow into state:

$$P_j = \Sigma\ (\lambda_{i,j}*P_i) + \Sigma\ (\mu_{k,j}*P_k) \qquad \text{(Eq. I1)}$$

The probability flow out of a state is the sum of the failure rates and repair rates leaving that state multiplied by the probability of the state, itself. For the P_j state, this is Equation I2.

Probability flow out of state:

$$P_j = \Sigma\ (\mu_{j,m} + \lambda_{j,n})*P_j \qquad \text{(Eq. I2)}$$

The time-rate-of-change of the probability of being in the P_j state is equal to the difference in the two probability flows (see Equation I3).

$$dP_j/dt = \Sigma\ (\lambda_{i,j}*P_i) + \Sigma\ (\mu_{k,j}*P_k) - \Sigma\ (\mu_{j,m} + \lambda_{j,n})*P_j \qquad \text{(Eq. I3)}$$

Although in-service failures and repairs are discrete events, they can be represented in MMs as continuous transitions from one state to another. In MMs, the failure rates represented by λ, and the repair rates represented by μ, are continuous transitions. When the λ and μ are constants with time, the Mean Time Between Failures (MTBF) will be 1/λ and the mean time to repair will be 1/μ hours after the failure. Repair scenarios are discussed in more detail in Section I.3.

SAENORM.COM : Click to view the full PDF of arp4761a

Markov Analysis involves obtaining the various state probabilities through the use of probability flow equations. The results can be used to calculate the system's instantaneous failure rate as a function of time and the average system failure rate over many hours of service. In general, the approach and examples contained in this appendix are oriented toward determining the overall average system failure rate, as this is generally the way the requirements for aircraft systems are specified prior to (and during) system design.

A system reliability MA generally consists of two parts:

1. Constructing an MM, or flow diagram, that represents the system as it transitions from its full-up state (all elements operating which have an effect on the system's capability to implement its design function), to its fully failed state (the system's inability to implement its design function). The model may include repair rates (if desired), as well as failure rates.

2. Adjusting the various repair rates and, if necessary, system architecture (and its associated MM diagram) to achieve a desired system reliability or limit/control the system's average failure rate.

It is recognized that these two tasks are commonly interrelated and there is a constant iteration between the two. When the analyst starts adjusting repair intervals, or changing the architecture of the system to achieve a desired level of reliability or a desired level of average system failure rate, he is changing the design and parameters of the system. Hence, the design of the system is not independent of the analysis. The two go together. This is an important benefit of the analysis, i.e., that it leads to better (more optimized) designs. Sometimes the analysis leads to elimination of a common cause from the design, and other times the analysis leads to a shortened or lengthened a repair interval. There is feedback from the analysis to the design.

In summary, MMs are quite simple, and they provide a reasonably powerful analysis tool for estimating system failure rates. In all models, the user defines the transition paths and their values, i.e., the failure or repair rates, between the various states. The state equations for any model are simple first order differential equations, which can be constructed by inspection of the model diagram. In complex models involving many states it may be helpful to use an automated equation generation/solution program. Many are commercially available.

I.1.4 Average System Failure Rate

For closed-loop MM (i.e., failure states are repaired to the full-up state) of a system, the average failure rate over an interval T is defined as the expected number of failures in the interval divided by T (see I.4.11.7). Every failure is renewed or repaired to full-up state in a closed-loop MM. So, N(T) in Equation I4 also represents the number of renewals in the interval T.

$$\lambda_{Average} = E(N(T))/T \qquad \text{(Eq. I4)}$$

If repairs are instantaneous, as in a discrete repair system, the expected number of failures E(N(t)) is the sum of integrals of the product of the transition rate $\lambda_{I,Pfail}$ from a non-failure state into the failure state Pfail and the probability of the non-failure state $P_I(t)$. It is assumed that the failure states are aggregated in the single state Pfail and the sum runs over the number of transitions into the failure state.

$$\lambda_{AVERAGE} = \frac{1}{T}\sum_{I}\int_{0}^{T}\lambda_{I,Pfail}P_I(t)dt \qquad \text{(Eq. I5)}$$

In the steady-state closed-loop formulation, in which every state probability has settled to a constant value, the average probability expression simplifies to Equation I6.

$$\lambda_{AVERAGE} = \sum_{I}\lambda_{I,Pfail}P_I \qquad \text{(Eq. I6)}$$

For an open-loop MM which has no repairs by definition from failure states, the appropriate measure is the average system hazard rate (see I.4.11.5).

SAENORM.COM : Click to view the full PDF of arp4761a

I.2 BACKGROUND

I.2.1 Advantages of Markov Analysis

The complexity and size of systems are rapidly increasing with new advances in technology. Aircraft systems are relying more and more on fault-tolerant designs featuring continuous monitoring of their condition, the instantaneous reconfiguration capability of the systems, and the on-condition repair of failed system equipment. Such systems hardly ever fail completely unless external events override system operation. Given this scenario of fault tolerance, the safety assessment process and evaluation of such systems may be more appropriately achieved by the application of the Markov modeling technique. The MM approach is particularly useful when repairs are to be simulated/modeled. This is a significant advantage of MMs as compared with Fault Tree Analyses (FTAs).

For civil airborne systems and equipment, end users may take advantage of the available redundancy to schedule maintenance activities for failed or inoperative equipment at some future date. This scheduling is possible if system redundancy provides adequate safety levels when equipment or portions of the system are inoperative. Examples of this are discussed in the various MM analyses contained in this appendix.

Fault Tree Analyses and Dependence Diagrams (DD) have traditionally been widely used for safety assessment because they are conceptually simple, reasonably easy to understand, and can handle very complex systems. FTAs and DDs, however, have some limitations:

a. It is difficult to allow for various types of failure modes and dependencies such as failure sequence dependency, time-dependent failure rates, and systems with “hot” or “cold” spares.

b. Simulating system element repairs is not easily handled.

MAs do not possess the above limitations. The sequence-dependent events are included naturally; therefore, a wide range of system behaviors can be readily modeled.

In an MM, one can more easily include the scenarios pertaining to the user operational environments; e.g., airline maintenance policies, dispatch requirements and safety considerations. MMs are also capable of handling several phases of a flight, state dependent failure rates, common cause failures, “performability” and performance-reliability dependence, physical interconnection dependence, time dependent transitions, imperfect coverage, and above all, various system repair scenarios. The repair scenarios can be quite different for many of the equipment and at different frequencies, and the MM will automatically account for the differences and yield the average system failure rate. This later point is significant, because it alleviates the concern of working with probabilities for the failures of equipment with different repair intervals and then trying to use that data to calculate an overall probability of failure and divide by a suitable time period to obtain an average probability per hour of flight failure rate. MMs can also simulate latent failures as well as less than 100% failure detectability.

More specifically, the MA method is most suitable to solve problems which require determining system availability, scheduled maintenance, and deferred maintenance.

SAENORM.COM : Click to view the full PDF of arp4761a

I.2.2 Limitations of Markov Analysis

MMs rely on a key assumption which is called the “memoryless” property. This means that the system behavior in the future (i.e., following a given point in time) is captured entirely by the current state of the system and it does not depend on the “probability history” of the states being modeled. This assumption implies that the probability distribution of all transitions (failures and repairs) is exponential, which means that the failure and repair rates for the equipment being modeled is constant with time. This permits the transient solution to be represented by a system of linear constant coefficient ODEs, and the steady-state solution for a closed-loop model to be obtained from a system of linear algebraic equations. Wear out of equipment, whose failure probability is characterized by a Weibull probability distribution with a shape parameter (slope) greater than one, cannot be modeled because the equipment failure rates are not constant with time. Hence, a wear out type of failure is not “memoryless” with regard to time. The previous history affects the failure rate of the equipment. For equipment where the failure rate is constant-with-time, when the equipment is inspected and found to be operating, it is functionally indistinguishable from new equipment, regardless of operating age. MMs can be used for aging systems without repair but the computations can become onerous. Refer to I.4.11.10 on non-homogeneous MCs for more information.

The representation of an MC can be more complex than that of a fault tree. For a system with N equipment, the number of gates and events in a fault tree is on-the-order of N, where N is the number of events in the tree. The corresponding MC has potentially 2^N states which show that there is an exponential growth in the state space. In practice the number of states is between $O(2^{k1})$ and $O(2^{k2})$ where, disregarding repair transitions, k1 is the minimum number of transitions to system failure and k2 represents the maximum number of transitions. Construction of an MC involves manual generation of all minimal cut sets of the corresponding fault tree, as well as all intermediate states.

Although fault trees and MCs both have computational complexity $O(2^N)$, the best fault tree algorithms are generally much faster than differential equation solution methods and in practice the size of the MC that can be solved is usually an order of magnitude smaller than the equivalent fault tree. In practice the largeness problem in the MM is mitigated by the fact that the systems to be analyzed are not fully general, partly because they have been specifically designed to isolate redundant functional paths and avoid common causes. This not only is sensible design practice; it also tends to make systems easier to analyze, because groups of related equipment can be lumped together into a much smaller number of high-level partitions. In addition, the failure probabilities of practical equipment tend to be many orders of magnitude smaller than 1, so combinations of more than two or three failures are often found to be negligible. It is often possible to greatly simplify an analysis by exploiting these special aspects of practical systems. However, care should be taken not to assume, in advance, that a particular system can be simplified in these ways. Meaningful substantiation of the extremely high levels of reliability (e.g., one per billion hours) mandated for safety-related systems requires a reasonably high level of reliability in the analysis method, so it is not permissible to employ a method that gives the right answer for almost all systems. But depending on the repair times, simplifying the models by discarding highly unlikely multiple failure states can often be done with little loss in analysis accuracy. This highlights the importance of applying good design practices, including strict isolation of redundant functional paths, so that systems are amenable to rigorous analysis.

MCs tend to become very large when the number of equipment increases. Therefore, it may be difficult to solve a complex scenario. The usual practice to simplify the problem is to take a sub-tree from a large fault tree which requires solution by MA, solve it separately and insert the sub- tree probability in the large fault tree before solving the fault tree.

Meticulous bookkeeping is required when constructing a large chain, and a program that allows the user to specify the problem as a fault tree, and then automatically generates the MC from the fault tree representation is helpful in reducing clerical errors in the description of the chain. Of course, the program should allow the user to insert repair transitions after the fault tree is generated.

The steady-state solution to an MC can usually be obtained much more quickly than the transient differential equation solution, and in many MMs for aircraft systems, the “closed-loop” steady-state solution approach provides an accurate estimation of the average failure probability over a specified interval. Take care in employing a steady-state solution that the operating interval, which is generally the aircraft life is long enough that the transient solution has time to settle out to the steady-state solution. Steady-state is achieved faster when the equipment MTBFs and repair times are shorter than the interval. This is normally the case and even otherwise the average system failure rate obtained from a steady-state solution is typically larger than the true rate and hence conservative.

I.2.3 Failure/Repair Scenarios and Modeling Strategies

As indicated previously, a significant advantage in using a Markov modeling approach for analyzing the failure rate of a system is the capability of MMs to include repair scenarios in the models. The approaches and techniques for modeling repairs in an MM do not often receive much discussion. A good understanding of repair path modeling is needed to ensure that the model will yield useful and accurate results, and be representative of in-service maintenance.

Before delving into the modeling aspects of various failure/repair scenarios, a discussion of the different in-service repair scenarios is useful. Section I.3 discusses the different repair scenarios which occur in service, and a discussion of how to address/model those different repair scenarios is included herein.

SAENORM.COM : Click to view the full PDF of arp4761a

I.2.4 Systems with Latent Faults

Most critical aircraft and aerospace systems are designed to be fault-tolerant with many types of redundancy such as functional and spatial. Also, highly reliable equipment are used with low failure rates. In many such systems, the primary equipment is called the active equipment and the backup equipment is considered “passive”—even if powered during flight. Active equipment provide the function during flight, and when the active equipment has a fault, the backup equipment becomes active either via automatic reconfiguration, by crew action, or a combination of the two. Active equipment faults are indicated in flight so that the crew is immediately aware—either by an obvious aircraft response to the loss of function, or by a suitable flight deck indication. For this reason, the fault is known within a flight and maintenance can be triggered, as needed, before the next flight. Such faults are called “active faults” and have the exposure time of single flight duration in the reliability or failure rate analysis. However, when a failure is not obvious and there is no flight deck indication for the failure, a periodic inspection can be used to find/repair the failure. These types of faults or failures are undetected until the inspection. Such faults are called latent faults. This is one scenario for latent faults. Sometimes faults happen on mechanical equipment such as coolant leak etc. which are not easily visible and are not indicated directly except when the pressure drops to some threshold level. Such a fault can also be considered a latent fault. Some equipment are never inspected for the life of the aircraft. In this case, the exposure period for the fault/failure would be the life of the aircraft. MMs can easily simulate latent exposure periods.

I.2.5 Systems Maintained on a Regular Schedule

To reduce the risk associated with latent faults and increase system availability, periodically scheduled maintenance tasks are used to look for, and if found, repair equipment failures that may not be apparent to the flight crew. Typically, these periodic tasks are documented in the aircraft’s maintenance planning document. The scheduled maintenance tasks could be simple inspection tasks, functional tests, or hard-timing parts. MMs can represent these scheduled inspection/repair activities using repair transitions from failed states to operational states.

I.2.6 Systems Sensitive to Sequence of Failures

Depending on the functional logic in a system, the equipment failures in the system may lead to system failure only if they happen in a specific sequence or order. For example, if a cargo fire detection/suppression system fails before a cargo fire event happens, then the occurrence of a cargo fire would probably lead to a Catastrophic condition, but if the detection/suppression system is operative when the cargo fire occurs, the detection/suppression system is expected to extinguish the fire. Another example is a system with an equipment and a monitor. If the equipment fails before the monitor fails, then it is a detected fault and can be repaired. This is a safe condition and will not lead to system failure, while the other order of failure leads to system failure. Typically, such sequential logic is modeled in Fault Tree Analyses approximately by putting 1/2 factors in the “AND” gates. MMs can easily simulate this by the ordering of the failure state “bubbles.” However, it is very easy to model sequential failures in an MM. Figure I3 shows a simple two-equipment system, and Figure I4 shows the MM for the system with its two possible sequences of failure.

SAENORM.COM : Click to view the full PDF of arp4761a

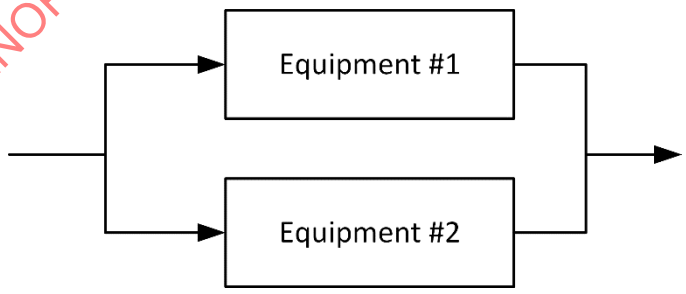


Figure I3 - Simple two-equipment system block diagram

Solving the MM will yield the probabilities of being in each of the five states modeled and the failure rates associated with the two different, two-equipment failure sequences. The system-level consequences can depend on the failure order.

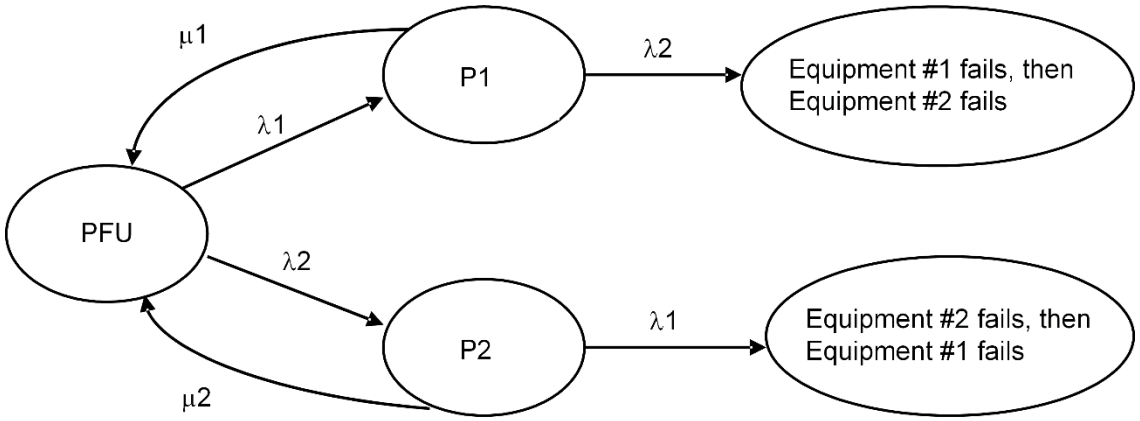


Figure I4 - MM Showing the two different sequential failure states

I.2.7 Discrete Repair versus Continuous Repair Scenarios

Needless to say, virtually all maintenance is performed when the aircraft is on the ground, whether the maintenance is triggered by on-board diagnostics or a scheduled maintenance inspection/repair activity. The above fact implies that repair is not immediately completed following the failure. In addition, the repair is a discrete transition from a failed equipment to a working equipment at a discrete or specific point in time. This can make the discrete repair process somewhat more difficult to model. In contrast, in continuous time MMs, failures and repairs occur continuously with time. The following discussions will show how to accommodate and model discrete repair scenarios, and how to model discrete repairs using continuous repair transitions. There are tools which faithfully model the discrete repair scenario (see Section I.5 on tools), but for practical situations, there is not much lost in modeling discrete repairs with continuous repairs so long as they are modeled carefully, as detailed in this appendix.

I.2.8 Conditional Maintenance Scenarios

In some systems, the maintenance of an equipment is conditioned on the failure or repair of another equipment. This may be due to many reasons such as fault tolerance, repair logistics, and maintainability. This is different from on-condition maintenance where the maintenance depends on the degraded condition and age of the equipment. In MM, it is easy to model the dependence of repair on the system state. For example, consider an engine with dual-redundant controller mounted on the engine. A single controller may fail without immediate maintenance action but when the engine shuts down for some other reason, the entire engine/controller equipment is repaired and returned to full functionality. In such a case, the controllers are repaired when the engine is maintained. An example of a conditional maintenance scenario is contained in the system discussed in I.4.5, where one of the monitor repair paths is based on an inspection for the availability of the backup system.

I.2.9 Phased Mission Systems

In aircraft systems and, more commonly, in aerospace systems such as launch vehicles, there are clearly many identifiable phases of flight. Different fault-tolerant systems come into play at each phase and there could be a reconfiguration of systems from one phase to another to satisfy mission requirements. Also, the failure rates can vary from one phase to another due to the environmental stresses being different between phases. For example, during lower stages of a rocket launch the failure rates can be lot higher than other stages. An MM can be useful for modeling phased mission scenarios. Specifically, the MM can be solved for each subsequent phase using transient analysis with different failure rates and by starting each phase with an initial condition which is the final state probabilities of the previous phase. This is mathematically equivalent to a piece-wise integration of the linear differential equations.

SAENORM.COM : Click to view the full PDF of arp4761a

I.2.10 Time-Limited Dispatch (TLD) and MMEL Relief

Fault-tolerant systems, such as the Full-Authority Digital Engine Control (FADEC) systems on modern turbine and reciprocating engines, have high levels of reliability. This is primarily due to the redundancy provided in electrical/electronic equipment. To improve aircraft availability, the aircraft is allowed to be dispatched when one or more electrical/electronic equipment are unavailable or degraded. The “time” that is allowed for these dispatches depends on the criticality of the equipment and the increase in the instantaneous Loss of Thrust Control (LOTC) rate - when operating with the failed equipment. Generally, two repair intervals are used. One is a short time repair interval of approximately 125 hours, and the other is a long time repair interval of 500 hours or more. A fault that requires repair within the short time interval is generally indicated via a generic flight deck display, and there is an MMEL listing which indicates that the aircraft is dispatchable (for the short time interval) with that fault condition present. The flight deck display is used to “start the clock” for the short time interval, and the fault must be repaired by the end of the interval. Faults that have a lesser impact on the system are generally placed in the long time interval. These faults are usually addressed by the use of a periodic inspection/repair task, which is contained in the engine maintenance manual.

A discussion of how both of these different repair scenarios can be modeled is contained in I.3.1.

I.3 MODELING STRATEGIES

It is useful to have a simple system and its MM in mind when discussing the various repair scenarios. This facilitates an understanding of how repair scenarios can be simulated. The simple two-equipment system shown in Figure I3 will be used for many examples contained in this appendix. The system is shown in Figure I2. Assume that this system will perform its intended function if either equipment #1 or equipment #2, or both are operational.

When the sequence of failure is not important and both equipment failures lead to loss of the system, the MM for this simple two-equipment system—with continuous repair shown for each equipment—is shown in Figure I5.

In the Figure I5 model:

- PFU represents the probability of being in the full-up state (i.e., there are no faults).
- P1 represents the probability of being in the equipment #1 (only) failed state.
- P2 represents the probability of being in the equipment #2 (only) failed state.
- Pfail represents the probability of being in the system failure state where both equipment are failed.

λ1 and λ2 represent the failure rates of equipment #1 and #2, respectively, and μ1 and μ2 represent the continuous repair rates (or transitions) from those single equipment failed states to the full-up state.

SAENORM.COM : Click to view the full PDF of arp4761a

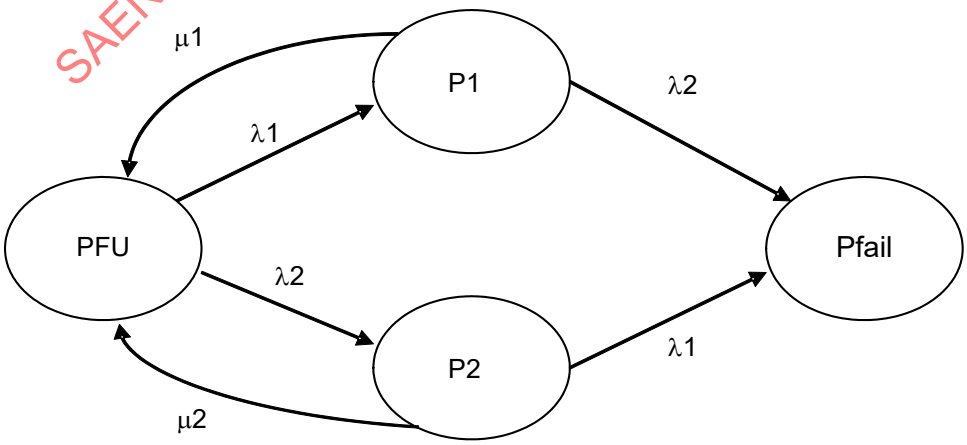


Figure I5 - MM for the two-equipment system with continuous repair for each failed equipment

The set of first order system equations are presented in Equations I7 through I9:

$$dP1/dt = \lambda1*PFU - (\lambda2 + \mu1)*P1 \quad \text{(Eq. I7)}$$

$$dP2/dt = \lambda2*PFU - (\lambda1 + \mu2)*P2 \quad \text{(Eq. I8)}$$

$$dPfail/dt = \lambda2*P1 + \lambda1*P2 \quad \text{(Eq. I9)}$$

The first order differential equation for the full-up state, PFU, could also be written down, but in all MMs, one of the state equations can be eliminated (it doesn't matter which one) and replaced with the constraint equation. The constraint equation often referred to as the conservation equation states that the sum of all probability states should equal unity. This assures that the conservation constraint is applied continuously throughout the "time history" calculation process.

In this appendix, the first order differential equation for the full-up state is always replaced by the conservation equation. This choice is arbitrary. Thus, the fourth system equation for the two-equipment system is shown in Equation I10:

$$1 = PFU + P1 + P2 + Pfail \quad \text{(Eq. I10)}$$

The instantaneous failure rate of the system is Equation I11:

$$\lambda(\text{instantaneous sys fail}) = -R'(t)/R(t)=f(t)/R(t)=(d(F(t)/dt)/(1-F(t))=(dPfail/dt)/(1-Pfail) \quad \text{(Eq. I11)}$$

This is also called the "hazard rate" in reliability literature. For more details on reliability metrics, nomenclature and definitions, see I.4.11. For this simple two-equipment system, the hazard rate is shown in Equation I12:

$$\lambda(\text{instantaneous sys fail}) = (\lambda2*P1 + \lambda1*P2)/(1 - Pfail) \quad \text{(Eq. I12)}$$

Assume that the failure rates for the equipment, λ1 and λ2, are given. If the continuous repair transitions shown as μ1 and μ2 in Figure I5 can be appropriately defined, then Equations I7 through I10 can be calculated as a function of time, and Equation I12 used to calculate the system's instantaneous failure rate at each point in time.

In the MM shown in Figure I5, the repair paths shown as μ1 and μ2 represent continuous repair transitions for the single equipment #1 and #2 failure states, respectively. A continuous repair path or transition is one where the repair is constantly occurring. Hence, the repair of the failed equipment represented by a particular state is not simulated as a discrete event, it is constantly occurring. This is similar to how failures are simulated in MMs. In actual service, failures are discrete events. In MMs, they are simulated as continuous events: having a constant failure rate of lambda (λ). (Failure rates in MMs can be variables as a function of time, but in this appendix, they will be assumed to be fixed constants.)

The following discussion will illustrate how discrete repair scenarios may be modeled as discrete events; then, how discrete repair may be represented by continuous repair transitions. The use of continuous repair transitions, and how they greatly simplify the modeling/analysis task, with usually no significant loss of accuracy, is illustrated in several examples.

SAENORM.COM : Click to view the full PDF of arp4761a

I.3.1 Modeling Discrete Repairs

Suppose State 2 is repaired to State 1 every T hours in the fragment of an MC shown in Figure I6.

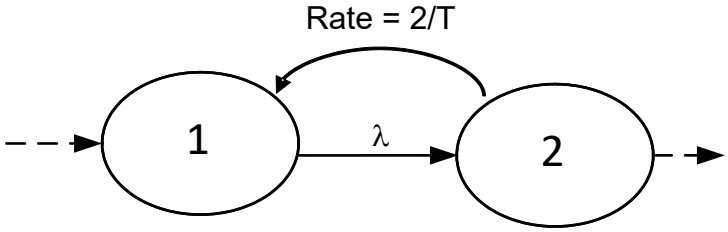


Figure I6 - Closed-loop MM simulating discrete repair with continuous repair from State 2

In the continuous repair model, the mean time to repair (MTTR) is approximately T/2 hours, corresponding to an exponential rate of 2/T per hour, and the repair is modeled by a repair arc from State 2 to State 1 with rate 2/T.

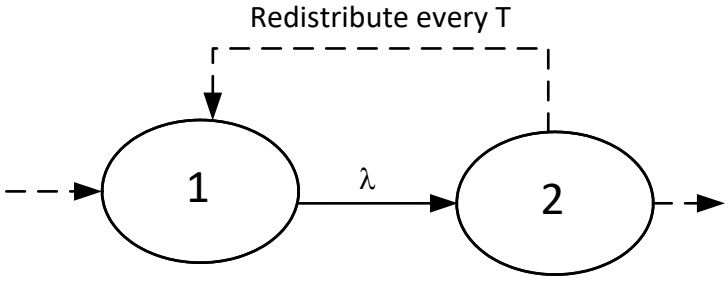


Figure I7 - Open-loop MM showing discrete repair from State 2

In a discrete repair model (Figure I7), the open-loop MM transient solution is interrupted every T hours and the repair is modeled by redistributing the probabilities from states being repaired to other states. The solution is continued with the redistributed probabilities providing initial conditions. In this case, the redistribution would be accomplished as follows, where P_1 and P_2 represent respectively the probabilities of states 1 and 2 the instant before redistribution (i.e., just before discrete repair) and P_1' and P_2' represent the probabilities after redistribution:

- $P_1' = P_1 + P_2$
- $P_2' = 0$

From a philosophical viewpoint, the continuous repair model simulates repairs with variable repair times which have a repair rate equal to twice the inverse of the prescribed maintenance interval. The discrete repair is done at precisely times T, 2T, and 3T.

A continuous repair approximation to discrete repair is made by setting the repair rate to the inverse of the mean time to repair, where the MTTR is calculated as the maintenance interval T minus the conditional MTTF of the subsystem being repaired. Here, conditional MTTF means the Mean Time To Failure for subsystems that actually fail in the interval. If the subsystem being repaired is a single equipment and the product of the equipment failure rate and the maintenance interval is small—say, less than 0.1—the MTTR is approximately half the maintenance interval. For more complex systems, the MTTR can be difficult to calculate and the discrete repair method is more accurate.

A Markov model can contain both discrete and continuous repairs. For example, in Figure I5, the transition from P1 to PFU could be scheduled and transition P2 to PFU could be modeled as continuous repair. I.3.3.2 and I.3.3.3 describe the relationship between repair rate and discrete repair interval for various scenarios.

Discrete repair is illustrated in the system shown in Figure I3 and represented by the MM of Figure I5. Assume that the failure rate of both equipment is 50 failures per million hours and that a periodic inspection every 100 hours is used to determine if either equipment is failed. If found failed, that equipment is replaced with an operative equipment. If both are failed, both would be replaced. In this particular example, it is assumed that the failure of both equipment would not be recognizable to the flight crew; therefore, the repair of both failed equipment—if both fail in an interval—would only be done at the 100-hour inspection interval. (If the failure of both equipment was obvious to the flight crew, the repair of both equipment could be scheduled to occur before the next flight, if that were required.)

In the following example, Equations I7 through I9 are solved with the continuous repair rates set to zero. This results in Equations I13 through I15:

$$dP1/dt = 50E\text{-}06*PFU - 50E\text{-}06*P1 \quad \text{(Eq. I13)}$$

$$dP2/dt = 50E\text{-}06*PFU - 50E\text{-}06*P2 \quad \text{(Eq. I14)}$$

$$dPfail/dt = 50E\text{-}06*(P1 + P2) \quad \text{(Eq. I15)}$$

SAENORM.COM : Click to view the full PDF of arp4761a

And the conservation equation shown in Equation I16:

$$1 = PFU + P1 + P2 + Pfail \quad \text{(Eq. I16)}$$

Using a 10-hour integration step size and the simple numerical integrator:

$$P^{n+1} = P^n + (dP/dt)^n * \Delta t \quad \text{(Eq. I17)}$$

where dP/dt is given by Equations I7 through I9. The numerical spreadsheet for the calculated system state probabilities and the system failure rate (as a function of time) is given in Table I1. The computations are stopped at 100 hours because at this point both equipment would be inspected and repaired if failed. Since the system is completely repaired at 100 hours, the time history beyond 100 hours would repeat the 0-hour to 100-hour values every 100-hour interval.

NOTE: In this particular example, failure of the two-equipment in this system are probably only involved in a Minor effect, as the aircraft would likely not be dispatchable with both equipment failed if the result was either Major, Hazardous or Catastrophic.

Table I1 - Calculation of system failure rate for two-equipment system using a discrete repair simulation

Failure rate for both equipment is: 0.00005 failures/hr.

time (hours)	P1	P2	Pfail	PFU	dP1/dt	dP2/dt	dPfail/dt	λ(t) = Instant Sys Fail Rate
0	0	0	0	1	0.00005	0.00005	0	0
10	5.000E-04	5.000E-04	0.000E+00	9.990E-01	4.993E-05	4.993E-05	5.000E-08	5.000E-08
20	9.993E-04	9.993E-04	5.000E-07	9.980E-01	4.985E-05	4.985E-05	9.993E-08	9.993E-08
30	1.498E-03	1.498E-03	1.499E-06	9.970E-01	4.978E-05	4.978E-05	1.498E-07	1.498E-07
40	1.996E-03	1.996E-03	2.997E-06	9.960E-01	4.970E-05	4.970E-05	1.996E-07	1.996E-07
50	2.493E-03	2.493E-03	4.993E-06	9.950E-01	4.963E-05	4.963E-05	2.493E-07	2.493E-07
60	2.989E-03	2.989E-03	7.485E-06	9.940E-01	4.955E-05	4.955E-05	2.989E-07	2.989E-07
70	3.484E-03	3.484E-03	1.047E-05	9.930E-01	4.948E-05	4.948E-05	3.484E-07	3.484E-07
80	3.979E-03	3.979E-03	1.396E-05	9.920E-01	4.940E-05	4.940E-05	3.979E-07	3.979E-07
90	4.473E-03	4.473E-03	1.794E-05	9.910E-01	4.933E-05	4.933E-05	4.473E-07	4.473E-07
100	4.966E-03	4.966E-03	2.241E-05	9.900E-01	4.925E-05	4.925E-05	4.966E-07	4.966E-07
		Expected # of failures/hour	2.241E-07				Average Failure Rate	2.4894E-07
		Exact Value	2.500E-07					

The instantaneous failure rate (Equation I12) of the system is shown as a function of time in Figure I8.

SAENORM.COM : Click to view the full PDF of arp4761a

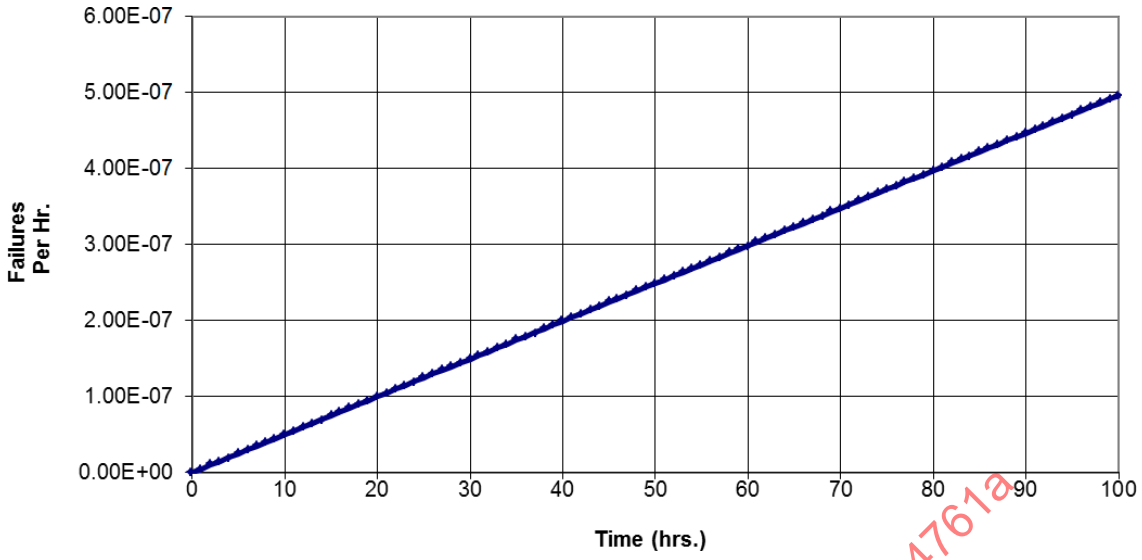


Figure I8 - Failure rate of two-equipment system over time

The system's instantaneous failure rate, λ(t), at each point in time is simply (dPfail/dt)/(1-Pfail) at that point in time. This is shown in the right-hand column of Table I1 and plotted in Figure I8. The average system failure rate of 2.4894E-07 failures/hour is determined by integrating the time history shown in Figure I8 and dividing by 100 hours. Referring to Table I1, this is represented by the summation (Equation I18).

$$\lambda(\text{average sys fail}) = \{0.5*[\lambda(0) + \lambda(100)] + \text{Sum}[\lambda(10):\lambda(90)]\}/10 \qquad \text{(Eq. I18)}$$

The instantaneous system failure rate as a function of time is given in the last column of Table I1 and shown in Figure I8. At the 100-hour point, the probabilities of being in the various failure states (i.e., P1, P2, and Pfail) would be reset to zero to simulate the repair of those states. When resetting either the P1 or P2 probability states to zero, the Pfail state is also reset to zero, because when either equipment is not failed, the system cannot be in the totally failed state. Hence, at the 100-hour point where both the equipment #1 and equipment #2 are repaired, the instant probability of being in the totally failed state (Pfail) is also reset to zero. In effect, by resetting Pfail to zero, a transition from the fully failed state back to the full-up state is being added, even though that repair transition is not shown in Figure I5.

Also shown in Table I1 is the expected number of failures per flight hour. This value is the probability of being in the failed state at 100 hours divided by 100 hours, i.e., Pfail(100)/100. The value calculated is 2.241E-07 failures/hour.

The exact probability of failure for a two-equipment system where both equipment have the same failure rate, is (Equation I19).

$$\text{Pfail} = (1 - e^{-\lambda t})^2 \qquad \text{(Eq. I19)}$$

For a λ of 50E-06 and a time of 100 hours, Equation I19 yields a Pfail of 2.5E-05 failures, and the probability per hour for the 100-hour interval would be 2.5E-07 failures per hour. The difference between this and the calculated value is due to the large integration step size of 10 hours used for Δt in Equation I17.

Observe that the calculated average failure rate value of 2.4894E-07, as given by Equation I18, is within 0.07% of the exact value for average failure rate of 2.4876E-07 (see I.4.11.8). In time history models, calculating the average system failure rate from the time history of the instantaneous failure rate will be reasonably accurate when λt is small, i.e., less than 0.1. In this particular case, λt is 100*50E-06 = 0.005.

SAENORM.COM : Click to view the full PDF of arp4761a

I.3.2 Repair Strategies Used In-Service

The example above illustrates a discrete repair simulation for a periodic inspection/repair scenario. In comparison with the MMEL or time-since-fault (TSF) repair scenario, this is the more historic of the two approaches, as early electrical/electronic systems and many mechanical/hydromechanical systems have little self-test and/or system health monitoring capability. In these cases, the time of fault occurrence is normally unknown because there is usually no flight deck indication of the existence of the fault; hence, the flight crew and maintenance personnel are generally not be aware of the fault. In such cases, a periodic inspection is used to find the fault(s). When found, the faults may require immediate repair or repair within a specified number of flight hours. Until found at inspection, these faults are latent faults. This approach is called the “periodic inspection/repair maintenance approach.”

The second repair approach (called the “MMEL approach” above) is generally called “on-condition” or “time since fault” repair. In this repair scenario, the time of the fault is known and recorded, and the fault is fixed within a specified or given numbers of hours of the fault occurrence. This on-condition fault/repair category is much more the “norm” in modern systems, as modern systems have considerably more internal self-test and health monitoring capability.

It should be noted that even though a system may have internal self-test sufficient to detect many system faults, a flight deck indication of those fault conditions is not necessarily required. The system’s fault information may be stored in some appropriate memory device, and a periodic check used to review that memory and repair the indicated faults. In this case, the faults are considered latent until the fault information is reviewed and repaired.

I.3.3 Simulating Repairs in Markov Models

Repairs in an MM can be simulated using a discrete repair procedure, as done in the example above, or by use of continuous transitions, as shown by the repair transitions shown as μ1 and μ2 in the MM diagram of Figure I3.

The relationship(s) between the modeling of TSF repairs versus using a periodic inspection/repair strategy and performing discrete repairs versus using continuous repair paths in an MM, is developed in I.3.3.1 through I.3.3.3.

I.3.3.1 Discrete Repair Simulations in Markov Models

I.3.3.1.1 Discrete Repair(s) Using the Periodic Inspection/Repair Approach

The first example given above simulates a discrete repair action using a periodic inspection/repair strategy. This means that whether the equipment are failed or not at the periodic inspection time of 100 hours is not known. The model is simply interrupted at that time, and any equipment found failed are replaced with fully operative equipment. This is modeled in the above example by resetting the probabilities of the P1, P2, and Pfail states to zero and the PFU state to unity at the 100-hour inspection interval.

I.3.3.1.2 Discrete Repair Based on a TSF Repair Approach

In this case, a discrete repair action is to be modeled, but the discrete repair action to be simulated is that associated with an on-condition or TSF repair. In this scenario, the time of the repair is known and the repair is scheduled to occur within a given number of hours of the failure.

When using the TSF repair approach in-service, the repair is virtually always completed before the end of the allowed interval, because if not completed by then, the aircraft might be grounded until the fault is repaired. Based on this, it could be argued that average repair interval is always less than the TSF specified time, and this would be true. However, for the purposes of this discussion, it will be assumed that the fault is on-average, always repaired at the maximum allowed TSF time. This will yield a conservative (i.e., higher) estimate of the system’s unreliability and average failure rate.

SAENORM.COM : Click to view the full PDF of arp4761a

A discrete repair in an MM always simulates a periodic inspection/repair scenario. However, in this case the discrete repair needs to simulate a TSF repair. When the TSF repair time is short with respect to the MTBF of the elements being repaired, the TSF discrete repair time can be simulated by means of a periodic inspection/repair model (as described in the previous section), where the periodic repair interval is approximately twice the TSF specified repair interval. The factor of two is used because the periodic repair simulation does not know when the failure occurred; when performing a periodic inspection/repair action, if a fault is found at the time of inspection, the fault will be approximately half of the inspection period old. Hence, on average, the fault will have occurred approximately half-way through the interval, and this half-interval time will be quite close to the TSF specified repair time. If the TSF repair time is given, the approximation for the periodic inspection/repair interval should be twice the TSF repair time.

The above approximation is applicable when the inspection period is much more frequent than the MTBF of the part(s) being inspected for failure (or when the TSF repair time is small with respect to the MTBF of the part(s) being repaired).

When the inspection is not so frequent (or the TSF repair time not small), the relationship between the periodic repair interval and the TSF interval is not a simple 2:1 ratio. The relationship(s) between the TSF time and periodic inspection/repair time in such cases is discussed in I.3.3.2.

I.3.3.2 The Relationship Between TSF and Periodic Inspection/Repair Times

When the periodic inspection/repair interval becomes larger than approximately 10% of the equipment (or group of equipment) MTBF, the “twice the TSF repair time” for the periodic inspection /repair time begins to lose accuracy. The relationship between a TSF repair time and a periodic inspection/repair time is developed and shown in Figure I9.

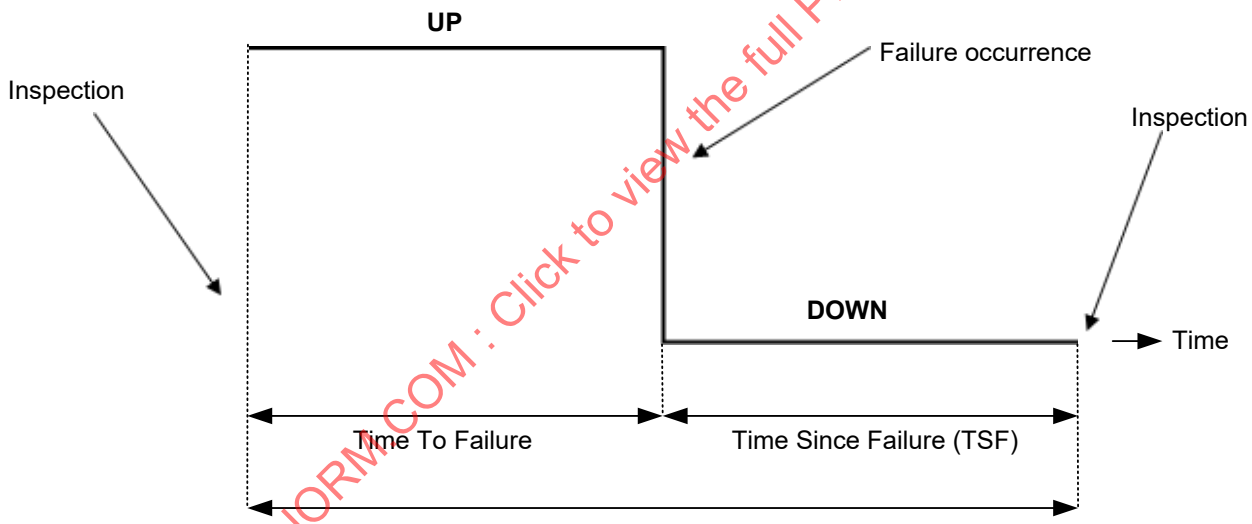


Figure I9 - Time between two periodic inspections

SAENORM.COM : Click to view the full PDF of arp4761a

The TSF can be defined as the mean down time of the equipment (or group of equipment) considering only inspections where the equipment is found failed. Other inspections have not to be counted because “nothing” happens between those inspections. Note that the TSF would be assimilated as the accumulated failure time divided by the accumulated number of failures. Thus, the TSF is the mean failure time, given that the failure occurs (at time = T) before the periodic inspection time, which is mathematically given by the following equation:

$$T_{TSF} = \mathbb{E}\left(T_{Inspect} - T \middle| T \le T_{Inspect}\right) = T_{Inspect} - \mathbb{E}\left(T \middle| T \le T_{Inspect}\right)$$

where T is the lifetime of the equipment (or group of equipment), T_{TSF} is the TSF (or average time that the fault has been present before repair is made) and $T_{Inspect}$ is the periodic inspection time. The expression of $\mathbb{E}\left(T \middle| T \le T_{Inspect}\right)$ which is the time to failure (considering that the failure occurs before the inspection) is defined by:

$$\mathbb{E}\left(T \middle| T \le T_{Inspect}\right) \stackrel{def}{=} \int_{-\infty}^{+\infty} t * f_{T|T \le T_{Inspect}}(t)\, dt$$

T has an exponential distribution which failure rate is λ. Thus, the survivor function (also called “reliability function”) and the density function of T are respectively given by $R_T(t) = e^{-\lambda * t}$ and $f_T(t) = -R'_T(t) = \lambda * e^{-\lambda * t}$. Furthermore, we need the conditional density of T, considering T is less or equal to $T_{Inspect}$.

By definition, $R_{T|T \le T_{Inspect}}(t)$ is given by the following equation.

$$R_{T|T \le T_{Inspect}}(t) \stackrel{def}{=} \mathbb{P}(T > t | T \le T_{Inspect})$$

Then, this conditional probability can be defined as:

$$\mathbb{P}(T > t | T \le T_{Inspect}) = \frac{\mathbb{P}(T > t \cap T \le T_{Inspect})}{\mathbb{P}(T \le T_{Inspect})}$$

Which gives:

$$\mathbb{P}(T > t | T \le T_{Inspect}) = \frac{\mathbb{P}(t < T \le T_{Inspect})}{\mathbb{P}(T \le T_{Inspect})}$$

$\mathbb{P}(t < T \le T_{Inspect})$ is the probability that the equipment (or group of equipment) fails after t and before $T_{Inspect}$. This probability can be defined as:

$$\mathbb{P}(t < T \le T_{Inspect}) = \int_t^{T_{Inspect}} f_T(s) ds$$

$$\mathbb{P}(t < T \le T_{Inspect}) = [F_T(s)]_t^{T_{Inspect}}$$

$$\mathbb{P}(t < T \le T_{Inspect}) = 1 - e^{-\lambda * T_{Inspect}} - (1 - e^{-\lambda * t}) = e^{-\lambda * t} - e^{-\lambda * T_{Inspect}}$$

By definition $\mathbb{P}(T \le T_{Inspect})$ is the probability distribution function which is the probability that the equipment (or group of equipment) fails prior to time $T_{Inspect}$.

$$\mathbb{P}(T \le T_{Inspect}) = F_T(T_{Inspect}) = 1 - e^{-\lambda * T_{Inspect}}$$

Then,

$$R_{T|T \le T_{Inspect}}(t) = \mathbb{P}(T > t | T \le T_{Inspect}) = \frac{e^{-\lambda * t} - e^{-\lambda * T_{Inspect}}}{1 - e^{-\lambda * T_{Inspect}}}$$

Therefore, the density function is $-R'_{T|T \le T_{Inspect}}(t)$, i. e.:

$$f_{T|T \le T_{Inspect}}(t) = \frac{\lambda * e^{-\lambda * t}}{1 - e^{-\lambda * T_{Inspect}}}$$

Note that:

- The time t cannot be lower than zero.
- The time t cannot be higher than $T_{Inspect}$ because the condition is that lifetime T should be lower or equal to $T_{Inspect}$.

Thus, $t \in [0 ; T_{Inspect}]$, and $\mathbb{E}(T | T \le T_{Inspect}) = \int_{-\infty}^{+\infty} t * f_{T|T \le T_{Inspect}}(t)\, dt$ becomes:

$$\mathbb{E}(T | T \le T_{Inspect}) = \int_0^{T_{Inspect}} t * f_{T|T \le T_{Inspect}}(t)\, dt$$

SAENORM.COM : Click to view the full PDF of arp4761a

Then, by integrating by parts we obtain the result below:

$$\mathbb{E}\left(T\middle|T \le T_{Inspect}\right) = \int_0^{T_{Inspect}} t * \frac{\lambda * e^{-\lambda * t}}{1-e^{-\lambda * T_{Inspect}}} dt = \frac{1-e^{-\lambda * T_{Inspect}}\left(1+\lambda * T_{Inspect}\right)}{\lambda * \left(1-e^{-\lambda * T_{Inspect}}\right)}$$

Finally, the expression of the TSF is:

$$TSF = T_{Inspect} - \frac{1-e^{-\lambda * T_{Inspect}}\left(1+\lambda * T_{Inspect}\right)}{\lambda * \left(1-e^{-\lambda * T_{Inspect}}\right)} = T_{Inspect} * \frac{1-\frac{1-e^{-\lambda * T_{Inspect}}}{\lambda * T_{Inspect}}}{1-e^{-\lambda * T_{Inspect}}}$$

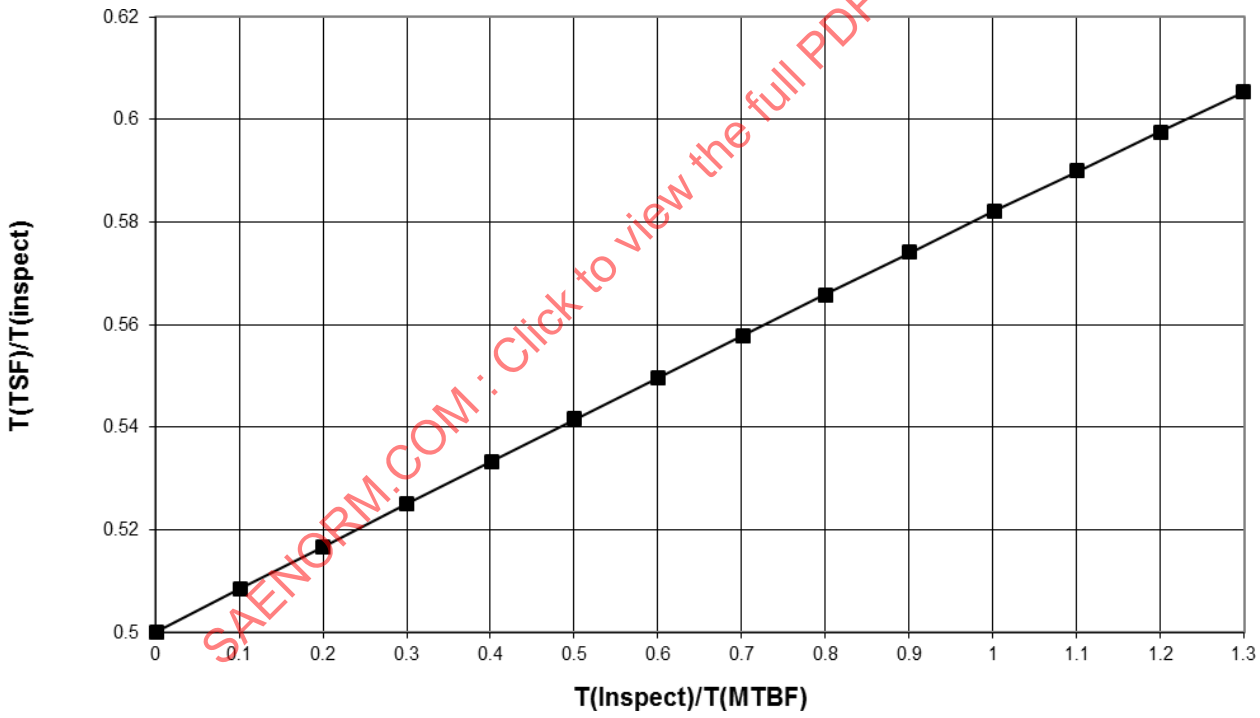
The relationship (after simplifying the forward expression) is presented in Equation I20.

$$T_{TSF}/T_{Inspect} = \{ 1 - (1 - e^{-R})/R \}/\{1 - e^{-R}\} \quad \text{(Eq. I20)}$$

where: $R = T_{Inspect}/T_{MTBF} = \lambda * T_{Inspect}$

T_{MTBF} is the mean time between failures of the fault, or group of faults, which are being inspected and repaired.

A plot of Equation I20 is shown in Figure I10.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure I10 - $T_{TSF}/T_{Inspect}$ as a function of $T_{Inspect}/T_{MTBF}$

Equation I20 allows the TSF repair time, T_{TSF}, to be calculated as a function of the inspection/repair interval, $T_{Inspect}$, and the MTBF of the elements being inspected, T_{MTBF}, but it doesn't allow $T_{Inspect}$ to be easily calculated as a function of T_{TSF} and T_{MTBF}.

Equation I20 can be used to obtain a relationship between $T_{Inspect}/T_{TSF}$ as a function of T_{TSF}/T_{MTBF}. The relationship is approximated by Equation I21.

$$T_{Inspect}/T_{TSF} \approx (3*\{-1 + [1 + (4/3)*(T_{TSF}/T_{MTBF})]^{0.5}\})/(T_{TSF}/T_{MTBF}) \quad \text{(Eq. I21)}$$

Valid for $T_{TSF}/T_{MTBF} \le 2.0$

When the TSF repair time, T_{TSF}, and the MTBF of the equipment or group of equipment under consideration are known, Equation I21 can be used to calculate the equivalent periodic inspection/repair time. This periodic time would be the periodic interrupt/reset time used in an MM simulation to represent a discrete TSF repair action.

Figure I11 shows a plot of $T_{Inspect}/T_{TSF}$ as a function of T_{TSF}/T_{MTBF} as calculated from Equation I21.

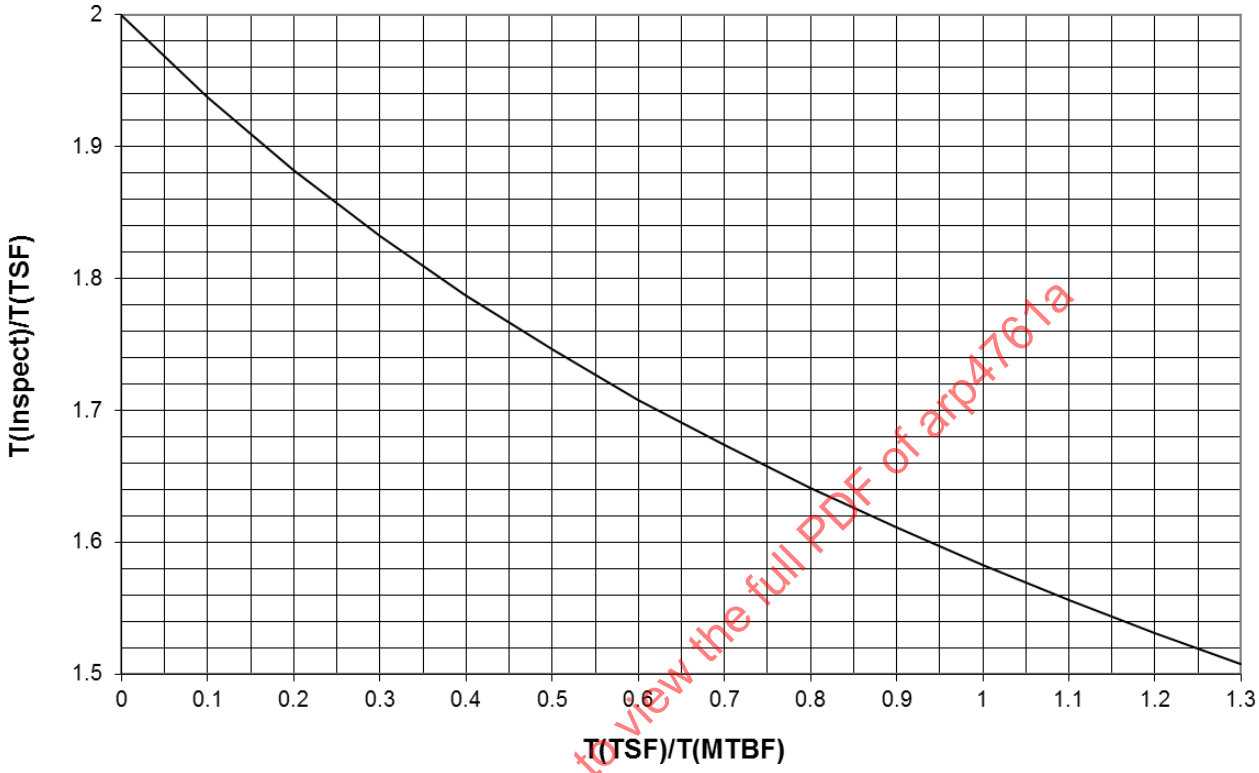


Figure I11 - $T_{Inspect}/T_{TSF}$ as a function of T_{TSF}/T_{MTBF}

As Figure I11 shows, the periodic inspection repair time is quite close to twice the TSF repair time when the TSF repair time is less than (about) 10% of the MTBF of the element(s) being repaired.

When the periodic inspection/repair interval is specified for a fault or group of faults, determine the MTBF for the fault or the group of faults from the failure rate data given for the fault(s), and use Equation I20 to determine the equivalent TSF repair time.

SAENORM.COM : Click to view the full PDF of arp4761a

I.3.3.3 Using Continuous Repair Transitions to Represent Discrete Repairs

In contrast to discrete repairs which happen only at distinct time intervals, continuous repairs happen at random times after failure according to some repair distribution, normally taken to be exponential. However, a discrete repair action can usually be approximated accurately by a continuous repair path or transition. In addition, a system in which all repairs are continuous and the MM contains a continuous repair path from the fully failed state to the full-up state (or another state), the time dependent differential equations approach a steady-state solution. Because of this, the time dependent differentials (i.e., the dP/dt) can be set to zero, and the steady-state solution obtained from the resulting set of algebraic equations. The steady-state solution to the set of algebraic equations provides the average failure rate of the system. (See Section I.4 for detailed discussion on transient and steady-state models.) This steady-state (limit) solution is accurate enough for engineering applications, and is much simpler to calculate than the complex differential equation solution required by the discrete repair method (I.3.1). This is illustrated in the example given in I.4.4. A continuous repair solution is shown in I.4.4.1 along with the more complex discrete repair solution shown in I.4.4.2.

Continuous repair paths are shown in MMs as transition paths similar to those shown for failure rates. In Figure I2 $\mu_{k,j}$ and $\mu_{j,m}$ and in Figure I4 μ1 and μ2 denote continuous repair transitions. In Figure I2, $\mu_{k,j}$ is the continuous repair rate from the state P_k to the state P_j and $\mu_{j,m}$ is the continuous repair rate from P_j to the state P_m.

When using continuous repair transitions, the time from failure to repair has an exponential distribution, which means the repair can be accomplished at any time (just like failure transitions). This is in contrast with discrete repairs, which occur only at discrete times. As a result, repair transitions with constant rates do not behave exactly the same as either periodic or TSF discrete repair transitions. However, for the purposes of computing the overall failure rate of a system over an interval of time that is long enough to include many individual failures and repairs, the result is determined almost entirely by the MTTF and mean time to repair for all of the non-fully failed states, regardless of how that mean time is achieved or simulated. In other words, the precise shape of the repair distribution is relatively unimportant. The overall average failure rate of the system is a function of the failure rates between the various states and the repair rates for all states, except the fully failed state. The mean time for repair from the fully failed state does not affect the failure rate of the system. This is discussed in more detail in I.4.2.2 and I.4.2.3. For this reason, it is generally possible to substitute constant-rate repair transitions for either periodic or TSF discrete repair transitions—without significantly altering the overall system failure rate—provided the constant repair rates are chosen to yield the same mean repair times as the actual discrete repair transitions.

Unlike discrete repair simulations, which model a periodic inspection/repair scenario, a continuous repair path, or transition, models a TSF repair action. It is usually quite straightforward to determine the constant rates corresponding to given periodic or TSF time intervals. For a TSF repair, if the repair is scheduled to take place T hours after the failure, then obviously the mean time to repair is T hours. As noted above, this is most likely conservative, since in practice the repair would often occur in less than T hours. The corresponding constant repair rate is simply $\mu = 1/T$. When using a continuous repair to represent periodic inspection/repair interval, there is usually justification for taking half of the inspection/repair interval as the mean time of the continuous repair, but this is only valid if the repair interval is much smaller than the MTBF of the equipment (which is usually the case). For longer intervals, the method described by Equations I20 and I21 can be used to estimate the mean time to repair.

In summary, when using a continuous, constant rate repair path in an MM, the average TSF repair time will be the reciprocal of the repair rate used in the model, and the continuous repair rate solution will yield essentially the same result as the discrete periodic inspection/repair solution - provided the continuous TSF repair time (i.e., the reciprocal of the continuous repair rate,$1/\mu$) is equal to the MTTR of the specified periodic (discrete) inspection/repair time or the specified TSF discrete repair time, whichever is to be simulated.

The following examples are considered:

Assume that a single fault or group of faults being repaired has a total failure rate (λ) of 50 per million hours, which equates to a T_{MTBF} of 20000 hours.

- Consider that the in-service TSF repair of 100 hours is specified. In this case, the time of occurrence of the fault(s) is known.
    - A discrete repair simulation using a periodic inspection time of 199.67 hours, which was calculated from Equation I21, could be used to estimate the system's failure rate, or
    - A continuous repair rate (μ) of 1/100 hours could be used in a continuous repair simulation to estimate the system's failure rate.
- Conversely, consider that an in-service discrete repair approach of periodically inspecting the single or group of faults every 200 hours is used, and when a fault is found, it is repaired.
    - This can be modeled as a discrete repair simulation, similar to the first example given above. In this case, the periodic inspection/repair would occur every 200 hours.
    - This could also be modeled using a continuous repair simulation with a continuous repair rate equal to the reciprocal of the T_{TSF} repair time as calculated from Equation I20. Using Equation I20, the T_{TSF} repair time is calculated as 100.167 hours, and the continuous repair rate would be 0.009983 repairs per hour.

NOTE: In the examples above, the relationship between the T_{TSF} and periodic inspection/repair time is quite close to a factor of two. This is because the times are quite short when compared to the group of faults T_{MTBF} time of 20000 hours.

SAENORM.COM : Click to view the full PDF of arp4761a

I.4 MARKOV MODELING - DISCUSSION AND EXAMPLES

I.4.1 A Simple Open-Loop MM for a Two-Equipment System with Continuous Repair Transitions

Figure I5, discussed in Section I.3 and repeated below, shows an open-loop MM with continuous repair paths for the states P1 and P2, but no repair from the fully failed state, Pfail.

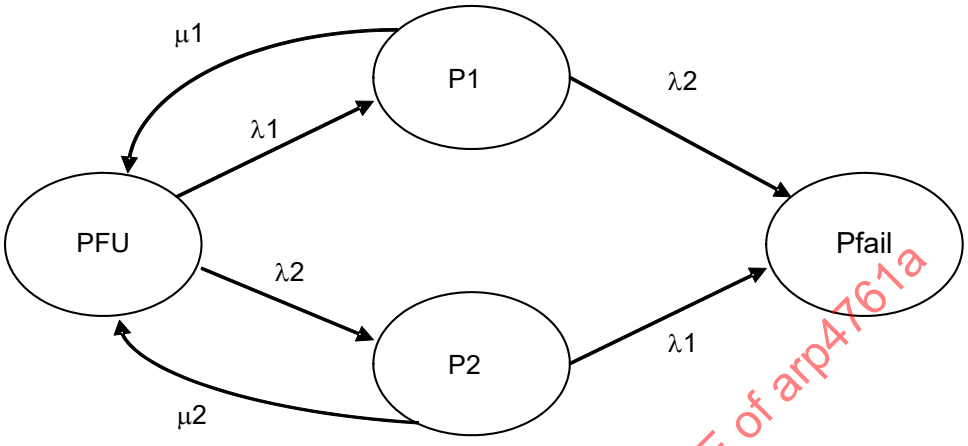


Figure I5 (repeated) - Closed-loop model for the simple two-equipment system with repair from the P1 and P2 states, but no repair from the fully failed state

The model is called “open-loop” because even though there is repair from the failure states P1 and P2, there is no repair from the Pfail state, and hence, the probabilities of all states will always continue to change with time. Since there is no repair from the Pfail state, the probability of being in that state will approach unity as time approaches infinity, and the probability of being in each of the other three states will approach zero as time approaches infinity.

Because there is no repair from the fully failed state to the full-up or any other state, this is also called an “open-loop” model.

I.4.2 Open-Loop and Closed-Loop Markov Models

For the purposes of this appendix, the MMs discussed herein will be classified as either “open-loop” or “closed-loop” models. To our knowledge, this nomenclature is not used in text books or other articles on MMs. It is used herein in anticipation that it will enhance the readers’ understanding of MMs in general, how open-loop and closed-loop models differ, and how much easier it is to apply closed-loop models to some system reliability analyses.

I.4.2.1 Open-Loop Markov Models

For the purposes of this appendix, an open-loop MM is one which has no repair (or feedback) from the fully failed state to the full-up (or any other) state. The simple two-equipment MM depicted in Section I.3 is an example of an open-loop (acyclic) model, because there is no repair from the total system failure state, Pfail, to any other state. As a result, the values of the probabilities of being in the various states do not re-occur or repeat at any point in time. As time advances, the probability of the fully failed state asymptotically approaches unity and the probabilities for all other states approach zero.

Starting with the initial conditions PFU = 1.0 and P1 = P2 = Pfail = 0.0, the system Equations I7 through I10 are easily integrated and Equation I12 is used to calculate the instantaneous system failure rate at each point in time. Contrary to what was done in the discrete repair simulation in Section I.3, the model is not stopped at any given point in time to perform repairs. The continuous repair paths represented in Figure I3 by μ1 and μ2, would have fixed values of $1/T_{TSF}$, where TSF is the discrete TSF repair time specified for the equipment. The time history would be calculated from Equations I7 through I10 to a very high elapsed time, such as 100000 hours, by which time almost all the system “probability” would be in the fully failed state.

SAENORM.COM : Click to view the full PDF of arp4761a

For systems that have a relatively high failure rate relative to system life, the possibility of multiple system failures needs to be considered—that is, the system can fail, be repaired, and subsequently fail again. Simply calculating the average failure rate as the probability of system failure in a lifetime divided by the system life can be inaccurate when this effect is not considered in the analysis. As indicated in I.1.4, the average system failure rate is expected to be the number of failures in a given time interval, divided by that time interval.

It is recommended that, whenever possible, repair from the fully failed state be modeled when estimating the average system failure rate.

I.4.2.2 Closed-Loop Markov Models - Steady-State Solutions

In this appendix, closed-loop models are models that have a repair (or feedback) transition from the fully failed state to the full-up state, or other intermediate state. Figure I12 shows a closed-loop model for the two-equipment system discussed above, where repair from the fully failed state, Pfail, to the full-up state, PFU, is simulated.

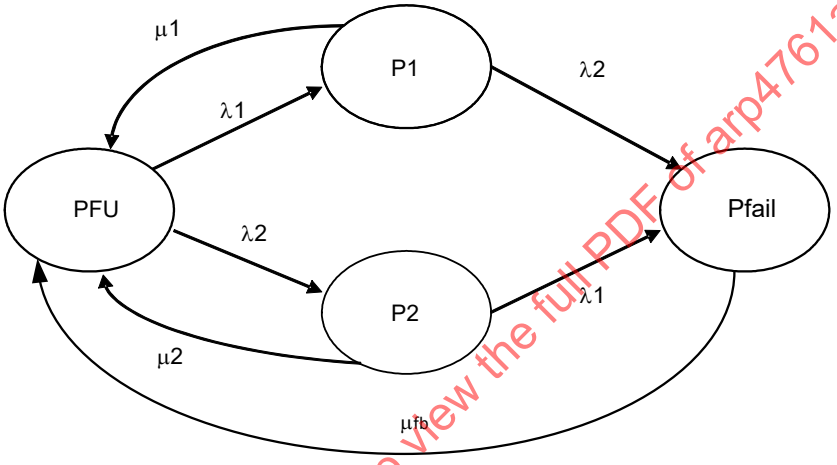


Figure I12 - Closed-loop model for the simple two-equipment system

The state equations for this closed-loop model are the same as those for the open-loop model for the P1 and P2 states. The conservation equation is being used in place of the PFU state equation. The state equation for the Pfail state in the closed-loop model is shown in Equation I22:

$$dPfail/dt = \lambda 2*P1 + \lambda 1*P2 - \mu fb*Pfail \quad \text{(Eq. I22)}$$

where μfb is the repair rate from the fully failed state.

In closed-loop models, the steady-state solution to the state equations is the solution of interest, because this solution represents the average, fleet-wide failure rate of the system.

I.4.2.2.1 Closed-Loop Models Using Periodic Discrete Repair Transitions

Discrete repair simulations are inherently closed-loop models because when an equipment is repaired at a specified periodic point in time, the system failure state, Pfail, should also be emptied (i.e., reset to zero), since the system is no longer fully failed. The time history calculations are then re-started at that point in time.

As shown by the first example in I.3.1, the steady-state solution of a discrete repair simulation is a time periodic one because the set of differential equations representing the system have to be integrated (in time) until the periodic repair intervals are reached. At those times the model is stopped, the probabilities for the states being repaired and the fully failed Pfail state are set to zero; the probabilities of the states absorbing the repairs are reset so that the sum of all probability states is unity; and the model time history calculation is restarted until the next repair interval is encountered. This process continues until the same initial conditions are obtained as those that existed at time zero. When the initial conditions are obtained, the model time history will repeat the first cycle. Hence, when discrete repairs are being simulated, the model will yield a repeating cycle, periodic steady-state solution. The failure rate of the system is obtained by calculating the average system failure rate during one of the periodic cycles. This is illustrated in the example given in I.3.1.

SAENORM.COM : Click to view the full PDF of arp4761a

I.4.2.2.2 Closed-Loop Models Using Continuous Repair Transitions

In a closed-loop model where all repairs, including repair from the fully failed state, are represented using continuous repair transitions, the steady-state solution will not be periodic. A closed-loop model does not require that continuous repair transitions be modeled for all intermediate states. Although it is unusual, some intermediate state may have no planned repair action. Their repair may be included when a more multi-equipment failed state is repaired. However, by definition, a closed-loop model should have a continuous repair path from the fully failed state to the full-up or other intermediate state. This repair path will cause the system to approach a steady-state solution with time. This solution will approach fixed numeric values for all variables because the set of differential equations representing the system will yield constant (and hence the term “steady”) values as time approaches infinity. Because of this, the steady-state solution can be obtained by setting the time differential, dP/dt, terms to zero and solving the remaining algebraic equations.

Using the conservation equation in place of the PFU state equation, the steady-state equations for closed-loop models using continuous repair transitions are shown in Equations I23 through I26:

$$1 = PFU + P1 + P2 + Pfail \quad \text{(Eq. I23)}$$

$$0 = \lambda1*PFU - (\lambda2 + \mu1)*P1 \quad \text{(Eq. I24)}$$

$$0 = \lambda2*PFU - (\lambda1 + \mu2)*P2 \quad \text{(Eq. I25)}$$

$$0 = \lambda2*P1 + \lambda1*P2 - \mu fb*Pfail \quad \text{(Eq. I26)}$$

Given values for the failure rates (λ) and repair rates (μ)—and selecting a repair rate for the feedback, μfb—these algebraic equations are easily solved to obtain values for the various probability states. However, note that from Equations I23 through I26, the various values calculated for the state probabilities will change if the value of μfb is changed. If μfb is very small as compared with the other transition rates in the model (i.e., the other failure and repair rates), the value of Pfail will be close to unity and the other state probabilities will be close to zero. If the value of μfb is very large as compared with the other transition rates, the value of Pfail will be close to zero, and the sum of the probabilities of being in the other probability states will be close to one.

The question then becomes: What value should be used for μfb? The answer is that it does not matter. The steady-state failure rate of a system does not depend on the repair rate from the fully failed state. That is, the steady-state failure rate of a system is independent of whether it is ever repaired or is repaired instantaneous from the fully failed state. Note that this is not to be confused with the rates used to repair equipment before the system is fully failed. Those repair rates very much affect the system’s failure rate.

To explain why the value of the feedback rate μfb does not affect the steady-state system failure rate, recall that the “failure rate” for entering any state is defined as the positive probability flow contribution from failures (i.e., not repairs) into that state, divided by (1-P) of that state. Thus, Equation 27:

$$\lambda(\text{average fail rate into state P}) = \text{Probability flow (from failures) into state P}/(1-P) \quad \text{(Eq. I27)}$$

For the Pfail state of the simple two-equipment model, this is represented by Equation I28:

$$\lambda(\text{inst. sys fail at steady-state}) = \lambda(\text{average sys fail at steady-state}) = (\lambda2*P1 + \lambda1*P2)/(1 - Pfail) \quad \text{(Eq. I28)}$$

Using the conservation equation, Equation I23, allows the substitution of (PFU + P1 + P2) for (1-Pfail). Equation I27 is then written as Equation I29;

$$\lambda(\text{inst. sys fail at steady-state}) = \lambda(\text{average sys fail at steady-state})$$

$$= \frac{(\lambda2*P1 + \lambda1*P2)}{(PFU + P1 + P2)} \quad \text{(Eq. I29)}$$

SAENORM.COM : Click to view the full PDF of arp4761a

Note that, at steady-state, the average rate is same as instantaneous rate which becomes constant in time just as the probabilities. From Equation I29, it still appears as though the system failure rate will depend on the various state probabilities, but divide through by PFU to obtain Equation I30:

$$\lambda(\text{inst. sys fail at steady-state}) = \lambda(\text{average sys fail at steady-state})$$

$$= \frac{(\lambda 2 * (P1/PFU) + \lambda 1 * (P2/PFU))}{(1 + (P1/PFU) + (P2/PFU))} \quad \text{(Eq. I30)}$$

This may not seem much different, but in looking at most MM used for reliability analyses, the downstream states (i.e., those "bubbles" to the right of PFU in Figure I4) can always be written as a function of the upstream states. This is accomplished in the simple two-equipment MM by re-arranging Equations I24 and I25 to yield Equations I31 and I32:

$$P1/PFU = \lambda 1/(\lambda 2 + \mu 1) \quad \text{(Eq. I31)}$$

$$P2/PFU = \lambda 2/(\lambda 1 + \mu 2) \quad \text{(Eq. I32)}$$

Substituting Equations I31 and I32 into Equation I29 yields the system failure rate shown in Equation I33:

$$\lambda(\text{inst. sys fail at steady-state}) = \lambda(\text{average sys fail at steady-state})$$

$$= \frac{(\lambda 1 * \lambda 2/(\lambda 2 + \mu 1) + \lambda 1 * \lambda 2/(\lambda 1 + \mu 2))}{(1 + \lambda 1/(\lambda 2 + \mu 1) + \lambda 2/(\lambda 1 + \mu 2))} \quad \text{(Eq. I33)}$$

It should be noted that Equation I33 is independent of all state probabilities and the value of μfb. The average system failure rate in a closed-loop model is only a function of the equipment failure and repair rates, and does not depend on the repair rate from the fully failed state or any state probabilities. Also, the expression in Equation I33 is the inverse of the MTBF of the system at steady-state. After a large period of time is elapsed one may predict that the expected number of failures in an incremental time period T will be λ(average sys fail at steady-state)*T.

This is why a closed-loop MM using continuous repair transitions is considered a failure rate model, not a probability model. In a closed-loop model with only one final failure state, the probabilities of being in the various probability states are not important and do not affect the value for the system's average failure rate.

In general, this is what is desired when performing failure rate analyses. The fact that the system failure rates into the various states can always be determined from the system's transition rates will be illustrated in further examples in this appendix.

I.4.2.3 Closed-Loop Models with Instantaneous Repair from the Fully Failed State

Following a system failure, the time to complete repairs and restore the system to the full-up state does not play a role in the numerical analysis of the failure rate of the system, because the analyst is looking for the expected number of failures during in-flight operations. To model this aspect correctly, the repair rate from their fully failed state needs to be set to infinity. This essentially means that the probability of being in the fully failed state Pfail will be zero, or that as soon as the system fails, it is immediately returned to the full-up state (for numerical analysis purposes) and the system "failure history" starts over again. Knowing Pfail as trivially equal to 0.0 effectively reduces the number of unknown state probabilities by 1 and also the number of equations by 1 (e.g., Equation I25 is trivially satisfied).

In the case where μfb = ∞, the MM model diagram will remain the same, but it will be shown slightly differently by using a dashed line for the transition from the fully failed state to the full-up state as a reminder that μfb has been set to infinity. The Pfail state is also shown as a dashed oval to indicate that the system does not spend any time in that state and is there for reference only to determine the system.

The MM model shown in Figure I12 for the two-equipment system is modified only slightly for μfb = ∞ and is shown in Figure I13.

SAENORM.COM : Click to view the full PDF of arp4761a

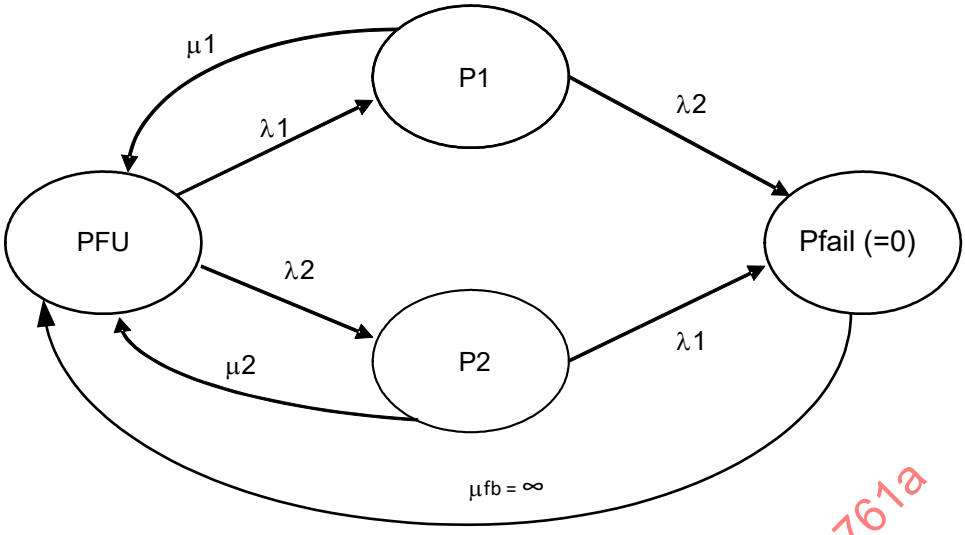


Figure I13 - MM for Simple two-equipment system with μfb = ∞

The state equations are reduced to:

Conservation equation: $1/PFU = 1 + P1/PFU + P2/PFU$ (Eq. I34)

P1 State Equation: $0 = \lambda1*PFU - (\lambda2 + \mu1)*P1$ (Eq. I35)

P2 State Equation: $0 = \lambda2*PFU - (\lambda1 + \mu2)*P2$ (Eq. I36)

Since the system is instantaneously repaired after failure, a metric which captures the rate of repair is called the “renewal rate.” The renewal rate is the time rate of change of the expected number of repairs at any point in time. When assuming instantaneous repair, every repair is matched to a failure, and therefore, the expected number of system repairs is equal to the expected number of system failures. Hence, it has the same units as failure rates (failures per hour).

Because of this equivalence, the material contained herein uses the nomenclature λ(sys fail) in place of what is normally termed the renewal rate. This is done because the engineers are more familiar with the terminology of “failure rates”, and what they are trying to estimate is the “average failure rate of a system”. When analyzing closed-loop MMs, whether they be repeating time history models or steady-state continuous repair models, the desired result is the average failure rate of the system.

When the system uses continuous repair and the steady-state analysis approach, as in this example, the λ(average sys fail) is the average system failure rate.

In this example, the average system failure rate for the two-equipment system equation is shown in Equation I37 as per the definition in I.1.4.

$$\lambda(\text{average sys fail}) = \lambda2*P1 + \lambda1*P2 \quad \text{(Eq. I37)}$$

This equation reflects the rate at which failures (renewals) occur for the MM shown in Figure I12.

Dividing through by PFU, the system failure rate can be written as shown in Equation I38:

$$\lambda(\text{average sys fail}) = (\lambda2*(P1/PFU) + \lambda1*(P2/FU))/ (1/PFU) \quad \text{(Eq. I38)}$$

Substituting Equation I33 for 1/PFU yields Equation I39:

$$\lambda(\text{average sys fail}) = (\lambda2*(P1/PFU) + \lambda1*(P2/PFU))/(1 + P1/PFU + P2/PFU) \quad \text{(Eq. I39)}$$

SAENORM.COM : Click to view the full PDF of arp4761a

It should be noted that Equation I39 is exactly the same as Equation I29, as it should be. Hence, when convenient, use a feedback rate (μfb) from the fully failed state to the full-up state of infinity (∞) to simplify the model and eliminate a variable. This will make Pfail a "collector state" only. The probability of being in that state will be zero, but there will still be a failure rate into the state.

I.4.3 Simplifying Markov Models - When Possible and Practical

I.4.3.1 The Two-Equipment System where Both Equipment Have the Same Failure and Repair Rates

It is usually useful to simplify the MM of the system by reducing the number of states, when possible and practical. The MM of the simple two-equipment system of Figure I3 can be simplified if the failure rates and repair rates for equipment #1 and #2 are the same. In this case, the MM diagram for the two-equipment system can be reduced from Figure I13 to the diagram in Figure I14.

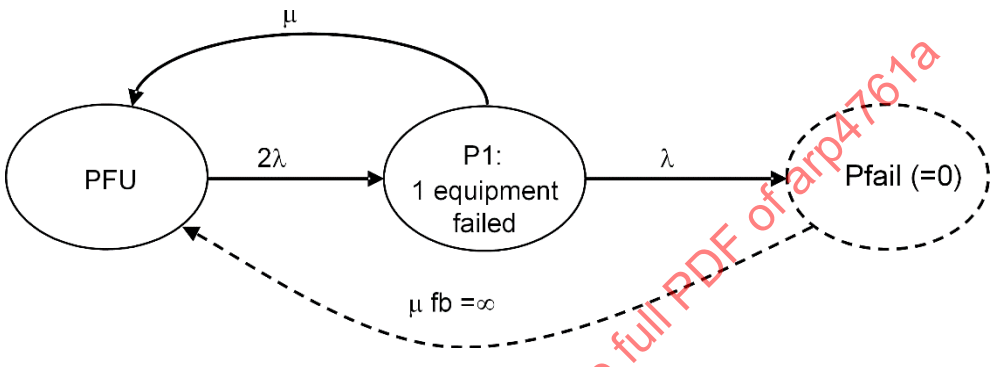


Figure I14 - Equipment system with each equipment having the same failure and repair rates

This significantly simplifies the MM system diagram, and whenever possible, this type of diagram consolidation should be employed. The system state equations are basically the same. Using the conservation equation in place of the PFU state equation results in Equations I40 and I41:

Conservation equation: $1 = PFU + P1$ (Eq. I40)

P1 State Equation: $0 = 2\lambda*PFU - (\mu + \lambda)*P1$ (Eq. I41)

The system failure rate equation is shown in Equation I42:

$$\lambda(\text{average sys fail}) = \lambda*P1/(1 - Pfail) = \lambda*P1 \text{ (because Pfail = 0)} \quad \text{(Eq. I42)}$$

Dividing the numerator and denominator of Equation I42 by PFU allows this to be written as Equation I43:

$$\lambda(\text{average sys fail}) = \lambda*(P1/PFU)/(1/PFU) \quad \text{(Eq. I43)}$$

The conservation equation can be written as: 1/PFU = 1 + P1/PFU. Substituting this into the failure rate equation (Equation I43) yields Equation I44:

$$\lambda(\text{average sys fail}) = \lambda*(P1/PFU)/(1 + P1/PFU) \quad \text{(Eq. I44)}$$

From Equation I41, P1/PFU = (2λ)/(μ + λ). Substituting this into Equation I44 yields Equation I45:

$$\lambda(\text{average sys fail}) = 2\lambda^2/(3\lambda + \mu) \quad \text{(Eq. I45)}$$

Equation I45 is the same as Equation I33, where λ1 = λ2 = λ, and μ1 = μ2 = μ.

SAENORM.COM : Click to view the full PDF of arp4761a

Use the data from the first example in I.3.1, to calculate the system failure rate from Equation I45. In the earlier example, the failure rate for each equipment was 50E-06 failures per hour. This is the λ to use in Equation I45. The repair modeled in the example in I.3.1 was a periodic inspection/repair for each of the equipment at 100 hours. Since both equipment are being inspected at the same time, the repair rate from the single equipment failed state shown in Figure I13 would be an inspection/repair time of 100 hours. The T_{MTBF} for both of the equipment (together) is 10000 hours. This yields a $T_{inspect}/T_{MTBF}$ of 0.01. Using Equation I20 with a value of $T_{inspect}/T_{MTBF}$ = 0.01 yields $T_{TSF}/T_{Inspect}$ = 0.500833. For a $T_{inspect}$ of 100 hours, this yields T_{TSF} = 50.0833 hours, which results in a continuous repair rate of $1/T_{TSF}$ = 1/50.0833 = 0.019967 repairs/hour.

Again, the TSF repair time is needed because continuous repair transitions (i.e., rates) are based on TSF repair times.

Because the periodic inspection interval of 100 hours was much less than the overall MTBF of the two equipment of 10000 hours, the T_{TSF} repair time could have been estimated as 1/2 of the periodic inspection interval, or 50 hours. This would have yielded a continuous repair rate of 0.02 repairs/hour, which would have provided accurate results for the failure rate calculation.

Using these values for λ and μ in Equation I45 yields a system failure rate of 2.4855E-07 failures per hour. This compares very well with the system failure rate estimate using discrete repair of 2.4878E-07 failure per hour. The difference in these estimates is 0.3%.

This is a negligible difference, and the example illustrates the accuracy of using continuous repair rate to approximate discrete repairs.

When the repair rate = μ is set to zero, the system failure rate is 2/3 λ, which is recognized as the known failure rate of a two-equipment system with no repair when the two-equipment have the same failure rate.

I.4.3.2 Example of a Two-Bus and Three-Equipment System

The following is an example of a system that can be modeled with a single, more complex MM, or by two separate MMs. The significance of this example is to show that two separate MMs provides a much simpler approach to determining the average failure rate of the system.

The example problem system is shown in Figure I15.

In this simplified system there are two buses feeding information to three equipment. Each of the buses has the same failure rate, λb, and each of the three-equipment has the same failure rate, λc. Assume the following: If both buses are lost, the system fails. If all three equipment fail, the system fails. Assume that both buses are needed for dispatch, but only two equipment are needed for dispatch. The mean flight time is 5 hours. Determine the system failure rate as a function of the repair time for a failed equipment.

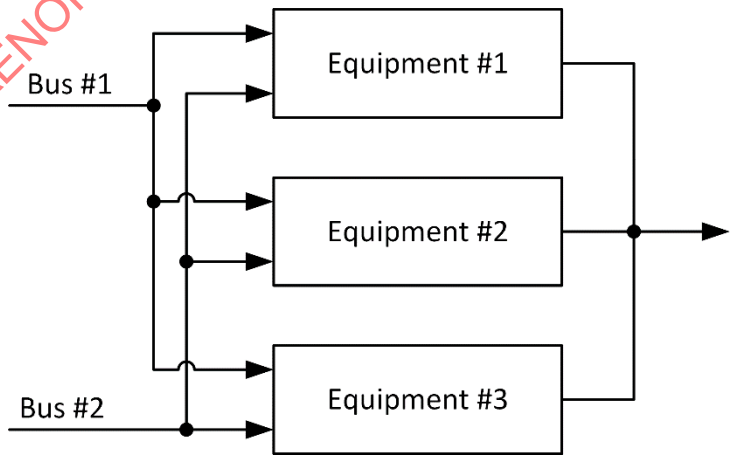


Figure I15 - Two-bus, three-equipment system

SAENORM.COM : Click to view the full PDF of arp4761a

I.4.3.2.1 Single MM Diagram Approach for Three-Equipment System Example

The single MM diagram constructed for this system is shown in Figure I16.

A description of the probability states will not be given here, as they should be self-evident from the Figure I15 diagram. Since μfb has been set to infinity, the probability of being in the Pfail state is 0.0, but the state is included in the system diagram, as it is the “collector” state used to determine the system’s failure rate.

- λb is the failure rate of a single bus.
- λc is the failure rate of a single equipment.
- μflt is the repair rate for a single bus failed. μflt is set equal to 2/Tflt, where Tflt is the mean time of one flight.
- μc is the repair rate for a single equipment failed. (μc is varied between 5 and 5000 hours to establish the effect of this repair rate on the system’s failure rate.)

With the state equation for the full-up state deleted and replaced by the conservation equation, the state equations are shown in Equations I46 through I51:

P1 State: $2\lambda b*PFU = (\mu flt + 3\lambda c + \lambda b)*P1$ (Eq. I46)

P2 State: $3\lambda c*PFU + \mu flt*P4 = (\mu flt + 2\lambda c + 2\lambda b)*P2$ (Eq. I47)

P3 State: $2\lambda c*P2 = (\mu flt + 2\lambda b + \lambda c)*P3$ (Eq. I48)

P4 State: $3\lambda c*P1 + 2\lambda b*P2 = (\mu flt + 2\lambda c + \lambda b)*P4$ (Eq. I49)

P5 State: $2\lambda b*P3 + 2\lambda c*P4 = (\mu flt + \lambda c + \lambda b)*P5$ (Eq. I50)

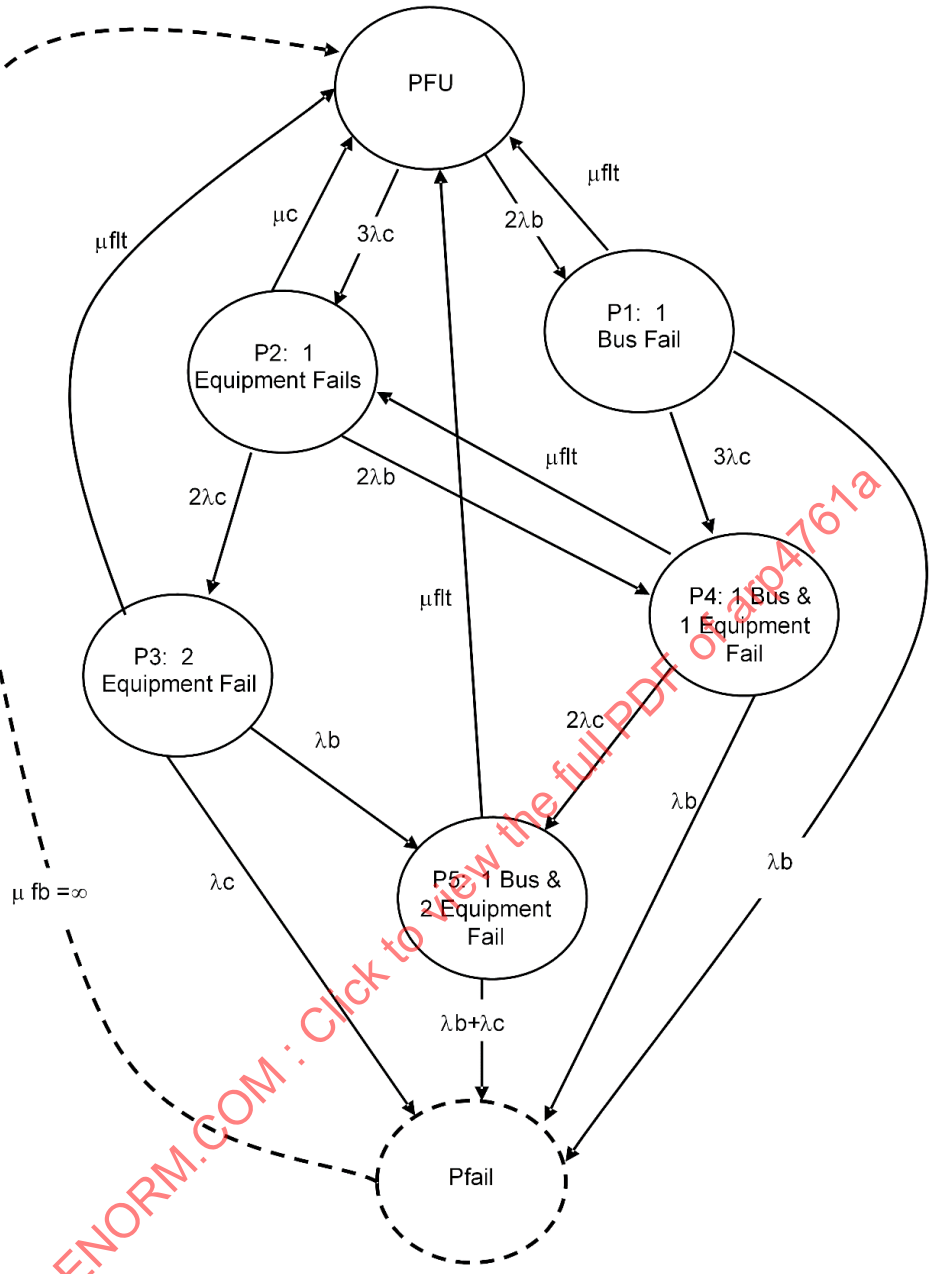
Conservation Equation: $1/PFU = 1 + (P1 + P2 + P3 + P4 + P5)/PFU$ (Eq. I51)

The failure rate equation is shown in Equation I52:

$$\lambda(\text{avg sys fail}) = \lambda c*(P3 + P5) + \lambda b(P1 + P4 + P5) \quad \text{(Eq. I52)}$$

One could easily solve the above equations using an algebraic equation solver program, but since the equations are relatively simple, they will be re-arranged in a manner that allows a solution to be obtained using a spreadsheet type of approach. Note that some spreadsheet programs contain linear equation solvers that allow numerical solutions of the equations to be obtained directly. To do this, each state P1 through P5 needs to be written as a function of the states preceding it. To accomplish this requires that the state equation for P2, which is a function of P4, be a function of PFU and P1 only. This is readily accomplished as follows. Let $A = 2\lambda b/(\mu flt + 2\lambda c + \lambda)$ and $B = 3\lambda c/(\mu flt + 2\lambda c + \lambda b)$:

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure I16 - MM for two-bus, three-equipment system

The equation for state P4 (Equation I49) can then be rewritten as Equation I53:

$$P4 = B*P1 + A*P2 \quad \text{(Eq. I53)}$$

This is substituted into the state equation for P2, and the resulting equation re-arranged to obtain state P2 as a function of PFU and P1 only. This is another example of how the state probabilities in an MM can be written as a function of the upstream state probabilities.

The state probability equations can then be written as ratios to PFU, in ascending order, as:

P1 State: $P1/PFU = 2\lambda b/(\mu flt + 3\lambda c + \lambda b)$ (Eq. I54)

P2 State: $P2/PFU = (3\lambda c + \mu flt*B*(P1/PFU))/(\mu c + 2\lambda c + 2\lambda b - \mu flt*A)$ (Eq. I55)

Where $A = 2\lambda b/(\mu flt + 2\lambda c + \lambda b)$ and $B = 3\lambda c/(\mu flt + 2\lambda c + \lambda b)$

P3 State: $P3/PFU = 2\lambda c^*(P2/PFU)/(\mu flt + 2\lambda b + \lambda c)$ (Eq. I56)

P4 State: $P4/PFU = B^*(P1/PFU) + A^*(P2/PFU)$ (Eq. I57)

P5 State: $P5/PFU = 2\lambda b^*(P3/PFU) + 2\lambda c^*(P4/PFU)/(\mu flt + \lambda c + \lambda b)$ (Eq. I58)

The conservation equation is written as shown in Equation I59:

$$1/PFU = 1 + (P1 + P2 + P3 + P4 + P5)/PFU \quad \text{(Eq. I59)}$$

And the failure rate equation is written as shown in Equation I60:

$$\lambda(\text{avg sys fail}) = (\lambda c^*(P3 + P5)/PFU + \lambda b^*(P1 + P4 + P5)/PFU)/(1/PFU) \quad \text{(Eq. I60)}$$

Or as Equation I61:

$$\lambda(\text{avg sys fail}) = \frac{\lambda c*(P3 + P5)/PFU + \lambda b*(P1 + P4 + P5)/PFU}{(1 + (P1 + P2 + P3 + P4 + P5)/PFU)} \quad \text{(Eq. I61)}$$

Calculating these probability ratios in ascending order, which means that each can be calculated from those preceding it, the failure rate of the system can be easily computed using a simple spreadsheet approach. This has been completed as shown in Table I2.

SAENORM.COM : Click to view the full PDF of arp4761a

Table I2 - Values for the ratios P1/PFU through P5/PFU and the system failure rate (per hour)

		lambda(b)	lambda(c)	Tflt	Mu(flt)			Constants (A & B)		
		2.00E-05	5.00E-05	5	0.4			A =	1.00E-04	
								B =	3.75E-04	
		Solution for MM shown in Fig. I-14.								
Column	***B***	***C***	***D***	***E***	***F***	***G***	***H***	***I***	***J***	***K***
Row #	Trepair	Mu(c)	P1/PFU	P2/PFU	P3/PFU	P4/PFU	P5/PFU	lambda(bus fail rate)	lambda(unit fail rate)	lambda (sys fail)
1	5	2.00E-01	1.00E-04	7.50E-04	1.87E-07	1.12E-07	4.68E-11	2.00E-09	9.36E-12	2.009E-09
2	500	2.00E-03	1.00E-04	7.14E-02	1.79E-05	7.18E-06	3.58E-09	2.00E-09	8.33E-10	2.833E-09
3	1000	1.00E-03	1.00E-04	1.36E-01	3.41E-05	1.37E-05	6.83E-09	2.00E-09	1.50E-09	3.500E-09
4	1500	6.67E-04	1.00E-04	1.96E-01	4.89E-05	1.96E-05	9.79E-09	2.00E-09	2.05E-09	4.045E-09
5	2000	5.00E-04	1.00E-04	2.50E-01	6.25E-05	2.50E-05	1.25E-08	2.00E-09	2.50E-09	4.499E-09
6	2500	4.00E-04	1.00E-04	3.00E-01	7.50E-05	3.00E-05	1.50E-08	2.00E-09	2.88E-09	4.884E-09
7	3000	3.33E-04	1.00E-04	3.46E-01	8.65E-05	3.46E-05	1.73E-08	2.00E-09	3.21E-09	5.214E-09
8	3500	2.86E-04	1.00E-04	3.89E-01	9.72E-05	3.89E-05	1.94E-08	2.00E-09	3.50E-09	5.499E-09
9	4000	2.50E-04	1.00E-04	4.29E-01	1.07E-04	4.29E-05	2.14E-08	2.00E-09	3.75E-09	5.749E-09
10	4500	2.22E-04	1.00E-04	4.66E-01	1.16E-04	4.66E-05	2.33E-08	2.00E-09	3.97E-09	5.970E-09
11	5000	2.00E-04	1.00E-04	5.00E-01	1.25E-04	5.00E-05	2.50E-08	2.00E-09	4.17E-09	6.166E-09

In Table I2, Column B shows the “allowed” dispatch time with a single equipment failed—before repair of that equipment is required. It is assumed that the system is not dispatchable with either two of the equipment failed or one bus failed. The immediate repair of these states (following the completion of a flight) is shown in Figure I15 by μflt repair paths from the P1 and P3 states to the full-up state. In the case where two equipment are failed, it is assumed that both are repaired before the next dispatch. Column I (i.e., lambda(b)) represents the contribution to system failures from bus failures. This rate is constant and independent of the repair rate for a failed equipment. Column J (i.e., lambda(c)) represents the contribution to system failures from equipment failures. The bus and equipment failures (given in Equations I62 and I63) are added together to get the total system failure of Column K.

$$\lambda(\text{avg bus fail}) = (\lambda b^*(P1 + P4 + P5)/PFU)/(1/PFU) \quad \text{(Eq. I62)}$$

$$\lambda(\text{avg equipment fail}) = (\lambda c^*(P3 + P5)/PFU))/(1/PFU) \quad \text{(Eq. I63)}$$

Figure I17 shows the failure rate contributions from bus failures, equipment failures, and the total system failure rate as a function of the repair time for a single failed equipment.

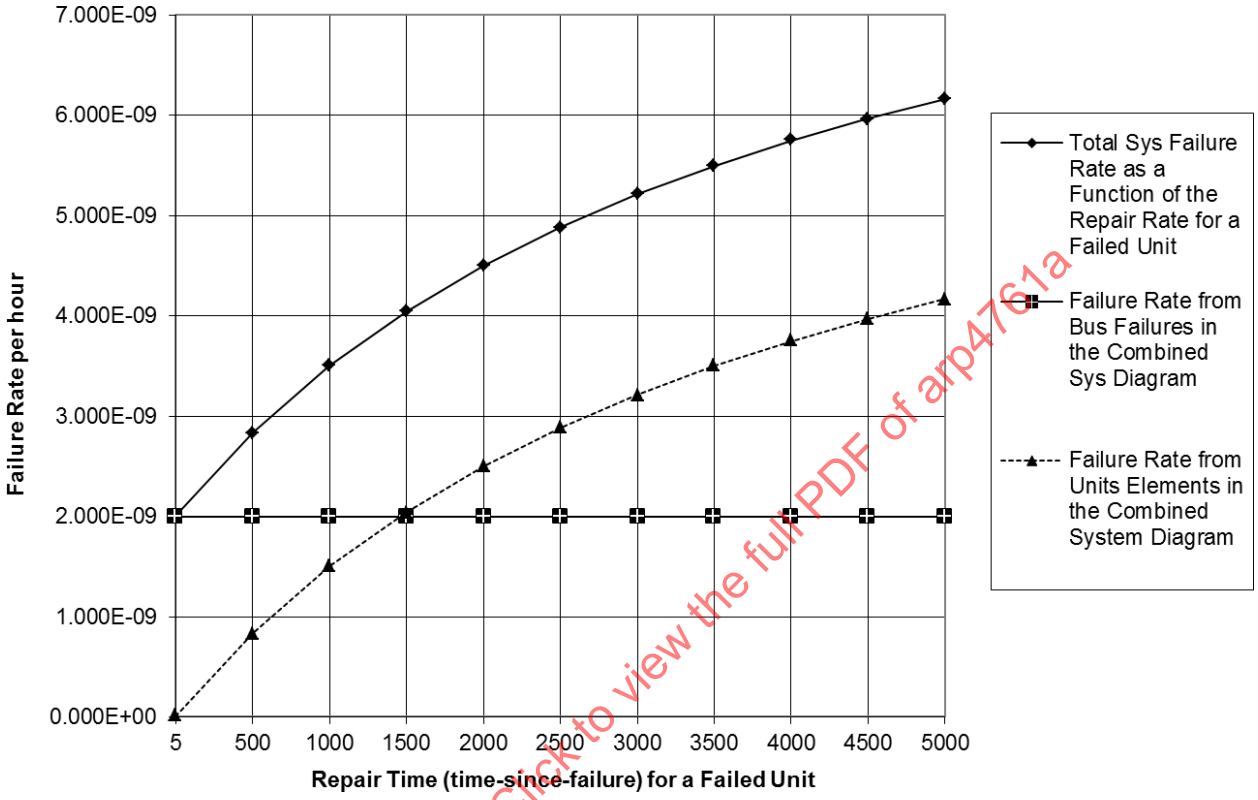


Figure I17 - Failure rates for the system bus portion, system equipment portion, and their sum, which is the total failure rate of the system

SAENORM.COM : Click to view the full PDF of arp4761a

Again, it is noted that the contribution to the total failure rate from bus failures is a constant $2.0*10^{-9}$ failure events per hour. This is because the system is not dispatchable with a failed bus; because both buses should be working for dispatch, the contribution of bus failures to the total system failure is the same on every flight.

I.4.3.2.2 Separate MM Diagrams for the Bus System and the Equipment System

Also, because bus and equipment failures are completely independent from one another, this system can be represented by two separate, independent system diagrams: One for bus failures and one for equipment failures. Separate MMs for these portions of the system are shown in Figures I18 and I19. It is highlighted that Figure I15 for the two-bus system is that same as the MM for the two-equipment system shown in Figure I11.

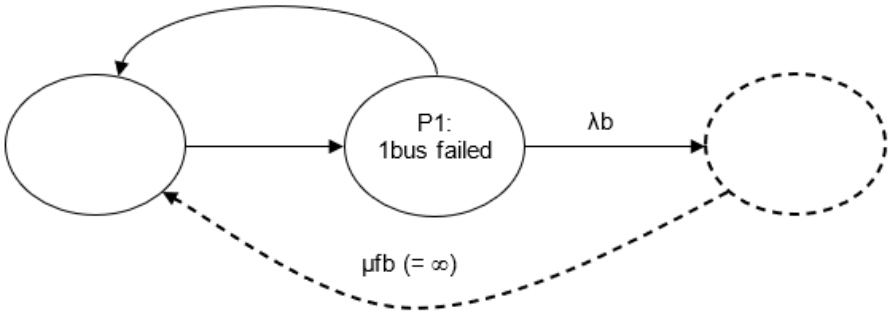


Figure I18 - Markov Model for bus failures

The state equation for P1 is:

$$P1/PFU = 2\lambda b/(\mu flt + \lambda b) \quad \text{(Eq. I64)}$$

The conservation equation is:

$$1/PFU = 1 + P1/PFU \quad \text{(Eq. I65)}$$

The failure rate relationship is:

$$\lambda(\text{avg bus sys fail}) = \lambda b*P1 = \lambda b*(P1/PFU)/(1/PFU) \quad \text{(Eq. I66)}$$

Substituting the relationships for P1/PFU and 1/PFU into the failure rate equation yields the system failure as:

$$\lambda(\text{avg bus sys fail}) = 2*(\lambda b)^2/(\mu flt + 3\lambda b) \quad \text{(Eq. I67)}$$

For λb = 2.0E-05 and μflt = 0.4, λ(bus sys fail) = 2.0E-09 events per hour, which is in agreement with the more complex model.

The MM model for equipment failures is shown in Figure I19.

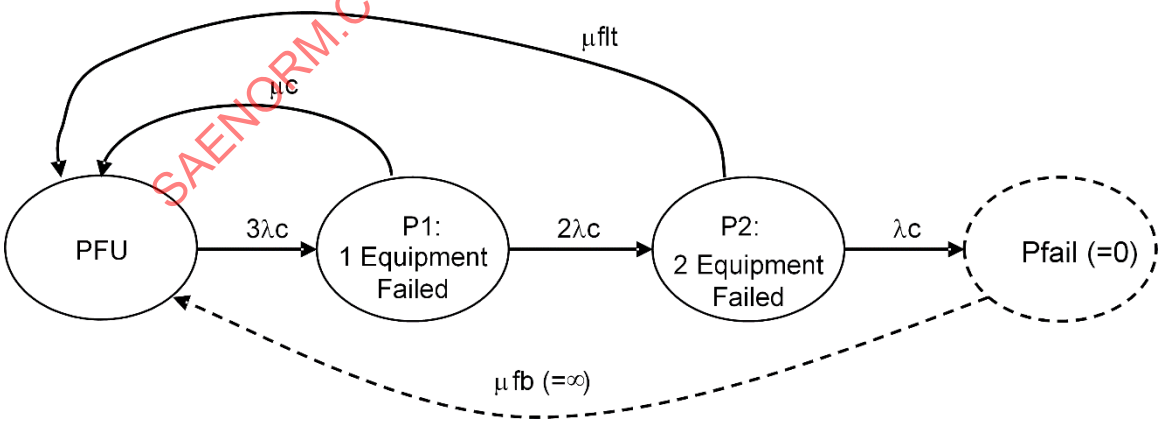


Figure I19 - Markov Model for three-equipment failures

SAENORM.COM : Click to view the full PDF of arp4761a

The state equations for the Figure I19 model are:

P1 State: $$P1/PFU = 3\lambda c/(\mu c + 2\lambda c) \quad \text{(Eq. I68)}$$

P2 State: $$P2/PFU = 2\lambda c*(P1/PFU)/(\mu flt + \lambda c) \quad \text{(Eq. I69)}$$

The conservation equation is:

$$1/PFU = 1 + P1/PFU + P2/PFU \quad \text{(Eq. I70)}$$

The failure rate equation is:

$$\lambda(\text{avg equipment sys failure}) = \lambda c*(P2/PFU)/(1/PFU) \quad \text{(Eq. I71)}$$

The spreadsheet solution for this two separate system model is given in Table I3.

The failure rate for the bus system is a function of the mean flight time and the bus failure rate. Because the mean flight time of 5 hours is much smaller than the MTBF of a bus, a bus failure (if one occurs) will occur on average half way through the flight. Hence, it's repair rate μflt. will be 2/Tflt, or 0.4 repairs per hour. Since the aircraft is not dispatchable with a bus failure, the loss of both buses is the same for all flights and represented by Equation I66.

Table I3 - Markov Model spreadsheet for two separate systems: one for two-bus system (Figure I12) and the three-equipment system (Figure I14)

		lambda(b)	lambda(c)	Tflt	Mu(flt)		**Lambda(b)**
		2.00E-05	5.00E-05	5	0.4		**2.00E-09**
		2-separate systems as shown in Fig. I12 and I14					
Column	***A***	***B***	***C***	***D***	***E***	***F***	***G***
Row #	Trepair	Mu(c)		P1/PFU	P2/PFU	**lambda (sys c)**	**Sum sys b + sys c**
1	5	2.00E-01		7.50E-04	1.87E-07	9.36E-12	2.009E-09
2	500	2.00E-03		7.14E-02	1.79E-05	8.33E-10	2.833E-09
3	1000	1.00E-03		1.36E-01	3.41E-05	1.50E-09	3.500E-09
4	1500	6.67E-04		1.96E-01	4.89E-05	2.05E-09	4.045E-09
5	2000	5.00E-04		2.50E-01	6.25E-05	2.50E-09	4.499E-09
6	2500	4.00E-04		3.00E-01	7.50E-05	2.88E-09	4.884E-09
7	3000	3.33E-04		3.46E-01	8.65E-05	3.21E-09	5.214E-09
8	3500	2.86E-04		3.89E-01	9.72E-05	3.50E-09	5.499E-09
9	4000	2.50E-04		4.29E-01	1.07E-04	3.75E-09	5.749E-09
10	4500	2.22E-04		4.66E-01	1.16E-04	3.97E-09	5.970E-09
11	5000	2.00E-04		5.00E-01	1.25E-04	4.17E-09	6.166E-09

SAENORM.COM : Click to view the full PDF of arp4761a

Columns D and E of Table I3 are the values for Equations I68 and I69 for the "equipment" system as a function of the repair time given in Column A. Column F is the failure rate for the equipment system (Equation I71) as a function of the repair time, and Column G if the sum of equipment system's failure rate and the (constant) bus system's failure rate. Column G of Table I3 agrees with Column K of Table I2. This shows that the simplification of using two separate models to represent the system, and simply adding the failure rates of each to get the total system failure rate of the system, is accurate for this particular case.

I.4.3.2.3 Comparison of Single and Dual Markov Model Approaches

The example in I.4.3.2.2 is used to show that in general, whenever it is possible to separate independent systems into individual models and add the failures rates of those models together to get the total system failure rate, it is advantageous to do so. It simplifies the system analysis. As shown in this example, the separation of the bus and equipment systems into two separate models provides a significant simplification to the system model(s).

I.4.4 Comparison of a Closed-Loop Continuous Repair MM to a Closed-Loop Discrete Repair MM - Two Solutions Equivalent

Referring back to Figure I3, which is the simple two-equipment system. This example will be used to compare the continuous repair and discrete repair solutions in an MM. This is the same system as that shown in Figure I3 and discussed in I.4.2.2.

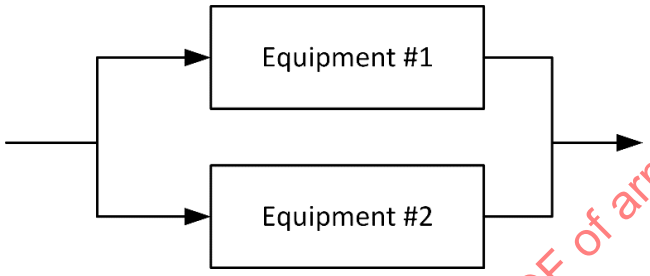


Figure I3 (repeated) - The simple two-equipment system used for comparison of continuous TSF and discrete repair actions

The MM for this system is the same as that shown in Figure I12, and is repeated here.

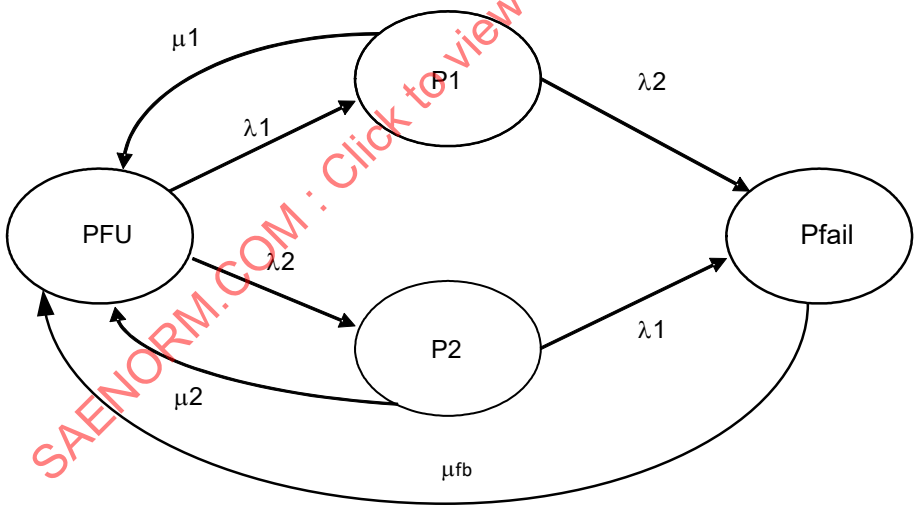


Figure I12 (repeated) - Example system used for a comparison of continuous TSF and periodic (discrete) repair simulations

Assume that the system's data is as follows:

- λ1 = 0.00010 failures/hour.
- λ2 = 0.00005 failures/hour.
- Mean flight time (Tflt) = 5 hours.

SAENORM.COM : Click to view the full PDF of arp4761a

For repairs, assume that the repair scenarios are as follows:

- Equipment #1 is examined before each 5-hour flight and if failed, is repaired before the next flight.
- Equipment #2 is examined after every tenth flight, which is every 50 hours; and if failed, is repaired before the next flight.

These are both periodic inspect/repair scenarios.

The question to be answered is, “Given this data, what is the system’s average failure rate?”

I.4.4.1 Continuous Repair Model Solution

The first solution presented here is the steady-state solution based on a continuous TSF repair rate, using the repair rates μ1 and μ2 as shown in Figure I12.

Using the periodic inspection repair times of 5 and 50 hours, and the T_{MTBF} for equipment #1 and #2 as the reciprocals of their respective failure rates, the continuous repair rates for equipment #1 and #2 are calculated from Equation I20 as:

μ1 = 0.39997 and μ2 = 0.039983 repairs per hour.

The steady-state solution is simple to obtain. The steady-state equations are the same as those given in I.4.2.3, and the system failure rate equation is the same as Equation I33, repeated here as Equation I72:

$$\lambda(\text{avg sys fail}) = \frac{\lambda 1 \lambda 2\,[1/(\mu 1 + \lambda 2) + (1/(\mu 2 + \lambda 1))]}{((1 + \lambda 1)/(\mu 1 + \lambda 2) + \lambda 2/(\mu 2 + \lambda 1))} \qquad \text{(Eq. I72)}$$

Substituting the values for λ1, λ2, μ1, and μ2 into Equation I72 yields an average system failure rate of:

λ(avg sys fail) = 1.37032E-07 failures/hour.

Note that, since the periodic inspection/repair times for both equipment #1 and equipment #2 are relatively short as compared with the MTBFs for those equipment, the simple approximations for the TSF repair times for those equipment would be 2.5 hours and 25 hours, respectively. The reciprocal of these times would yield approximate repair rates of 0.4 repairs/hour and 0.04 repairs/hour, respectively. These values could have been used in Equation I72 with little error.

I.4.4.2 Discrete Repair Simulation Solution

In general, discrete repairs transitions are more difficult to handle in an MM than continuous repair transitions, due primarily to the following calculation activities:

1. A time history for the probabilities of being in the various states should be calculated by solving a system of linear ODEs. This contrasts with the system of linear algebraic equations to be solved for the steady-state solution when using continuous repair transitions.

2. The differential equations are integrated from one repair time to the next. When a repair time is reached, pairs of state probabilities are reset to model repair arcs that are being completed at that time. A repair arc represents a repair action form one state to another at a fixed point in time. For example, a repair from state P1 to Pfu (see Figure I19), that is scheduled at a particular repair time, is modeled by adding the probability of state P1 to the probability of state Pfu and then setting the probability of state P1 to zero. Repair arcs from fully failed state(s) are “scheduled” at every repair time, as well. (It would not make sense to perform repairs that do not take the system out of the fully failed state.) It is generally assumed that all elements in the fully failed state are repaired, i.e., all repair arc from fully failed state(s) goes to the full-up state.

   If the most frequent repair time is greater than one flight, and the failure of the system would result in a Major or more severe level event, the Pfu state should be repaired after each flight, as the aircraft would not be dispatched with an important system known to be failed. (This assumes that the failure of the system would be apparent to the flight crew, and they would inform maintenance of the needed repair.)

SAENORM.COM : Click to view the full PDF of arp4761a

The time history solution is then restarted using the reset state probabilities as the initial conditions, and the calculations continue to the next repair time. At this point in time, the appropriated repairs are again simulated as discussed above, and the simulation is again restarted to get to the next repair time.

The model is integrated in time until the entire system is repaired and the time histories of all states start over with the probability of being in the full-up state being unity and all other states having probability values of zero or the system reaches its lifetime. In this latter case, the time history would not repeat itself. For Catastrophic, Hazardous and Major top-level events, the probability of being in the fully failed state should be reset at least every flight because the aircraft would most likely not be considered dispatchable with failed equipment that leads to these events.

At this point, the time history of the probability of being in the fully failed state can be used to calculate the expected number of failures in that periodic interval or the lifetime of the system, and the calculated number of failures can be divided by the periodic interval or system lifetime to determine the average failure rate of the system. If the probability of being in the final failed state is reset to zero one or more times before the time full periodic solution was achieved, the probability values for being in the failure state are summed just before each reset to determine the total number of expected failures in the overall periodic interval. Divide that value by the total time interval to obtain the estimated value for the system's average failures per hour rate. See the example below and the results in Table I4, Row 70, Column D.

When the failure rates of each of the elements, λ_I, in a system times the maximum repair interval for each of those elements, $T_{MAX\text{-}i}$ is small, e.g., less than 0.1, the average failure rate of the system may also be approximated from the instantaneous failure rate time history by simply integrating the instantaneous failure rate over an entire periodic time interval and dividing the result by that value of time. This sometimes provides a simpler calculation technique to be used, because the integration of a complete time history is easier to calculate than the summation of the fully failed probability values at each specific reset (i.e., repair) time. The expected number of failures in that periodic time interval would simply be the average failure rate times the length of the time interval.

When $(\lambda_i * T_{MAX\text{-}I})$s become much greater than 0.1, the above method for determining the average system failure rate will start to lose accuracy. In these cases, use the time history of the probability of being in the fully failed state (e.g., Column D in Table I4) to determine the expected number of failures and the average probability/hour of system failure.

To simulate discrete repair, the MM diagram for the simple two-equipment system is re-drawn as shown in Figure I20.

The MM has been re-drawn to show that none of the states has a continuous repair path. The discrete repair paths from the P1 and P2 states to full-up at 5 hours and 50 hours, respectively, are easy to understand and model. The discrete repair path from the fully failed Pfail state to the full-up Pfu state is also apparent in the diagram. The repair path from this state could go to the P1 or P2 states, and if this were the case, the value of the Pfail state would be added to one of those states during this reset. In general, it is assumed that if the system is failed all elements contributing to that failure would be repaired. In such a case the value of the Pfail state would be added to the full-up Pfu state at this reset/repair time, and the Pfail state would be reset to zero.

SAENORM.COM : Click to view the full PDF of arp4761a

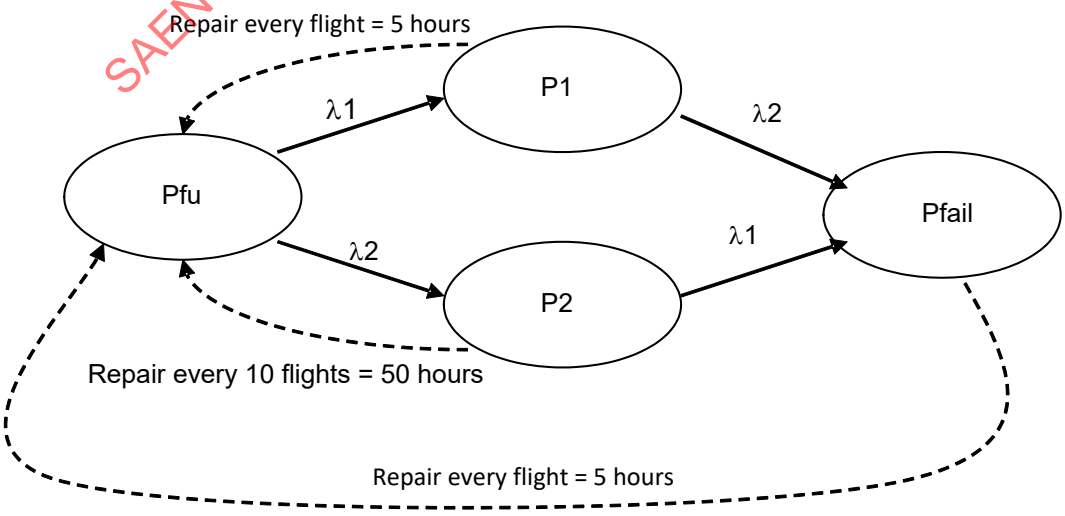


Figure I20 - MM used for the discrete repair simulation of the two-equipment system example

The model is a “closed-loop” model but the solution is a time dependent one - as repair from the P1, P2, and Pfail states are only going to occur at specified times. Since continuous repair of the P1 and P2 states is not being simulated, μ1 and μ2 in Figure I20 are set to zero, and the repair times are as illustrated in Figure I20. The simple time dependent first order state equations are shown in Equations I73 through I75:

For state P1: $dP1/dt = \lambda1*Pfu - \lambda2*P1$ (Eq. I73)

For state P2: $dP2/dt = \lambda2*Pfu - \lambda1*P2$ (Eq. I74)

For state Pfail: $dPfail/dt = \lambda2*P1 + \lambda1*P2$ (Eq. I75)

And the conservation equation is:

$$1 = Pfu + P1 + P2 + Pfail \quad \text{(Eq. I76)}$$

Using an integration step size, Δt, of one hour and a very simple first order integrator, the values of P1, P2, and Pfail at time, t + Δt, are calculated from Equations I77 through I79.

$$P1(t+\Delta t) = P1(t) + (dP1/dt)(t) * \Delta t \quad \text{(Eq. I77)}$$

$$P2(t+\Delta t) = P2(t) + (dP2/dt)(t) * \Delta t \quad \text{(Eq. I78)}$$

$$Pfail^{(t+\Delta t)} = Pfail^{(t)} + (dPfail/dt)^{(t)} * \Delta t \quad \text{(Eq. I79)}$$

And then:

$$Pfu^{(t+\Delta t)} = 1 - P1^{(t+\Delta t)} - P2^{(t+\Delta t)} - Pfail^{(t+\Delta t)} \quad \text{(Eq. I80)}$$

After five integration steps, the 5-hour point is reached and the inspection/repair of the P1 failed state is simulated by resetting P1 to zero. Pfail is also reset to zero because the system cannot be in the Pfail state if equipment #1 is known to be functioning. Pfu is also recalculated at this point using the zero values of P1 and Pfail, so that the conservation equation is satisfied when starting the next 5-hour interval. The value for P2 is not altered at this point, as the inspection/repair time for P2 is 50 hours.

The instantaneous system failure rate equation at each point in time is shown in Equation I81:

$$\lambda(\text{inst. sys fail}) = (\lambda2*P1 + \lambda1*P2)/(1 - Pfail) \quad \text{(Eq. I81)}$$

This failure rate is calculated at each point in time.

The time dependent calculation results are shown in Table I4.

Table I4 uses a shaded row after each 5-hour period to show the resetting of the P1 and Pfail probability values to zero and recalculating PFU so that the sum of the probability states is unity. These values are then the starting point for the time integration of the next 5-hour flight.

The calculations are discontinued after time of 50 flight hours, because after the reset at 50 hours, which includes repairs to both equipment (a) and (b), the initial conditions are the same as those at time zero. Hence, if the time integrations were to continue, the results would be the same (for the next 50 hours) as those for the first 50 hours.

Figure I21 shows the failure rate of the two-equipment system (Column H in Table I4) with time.

SAENORM.COM : Click to view the full PDF of arp4761a

Table I4 - Time-dependent calculations for the simple two-equipment system with different repair times for the equipment

Column →	B	C	D		E	F	G		H	I
	lam(1)	lam(2)	Flt. Time		MU(1)	MU(2)				
	1.000E-04	5.00E-05	5		0	0				
Row#									Instantaneous	Integrate
	Time (hrs)	P1	P2	Pfail	PFU	dP1/dt	dP2/dt	dPfail/dt	λ(sys fail)	λ(sys fail)
0	0.0	0.000E+00	0.000E+00	0.000E+00	1.000E+00	1.000E-04	5.000E-05	0.000E+00	0	
1	1.0	1.000E-04	5.000E-05	0.000E+00	9.999E-01	9.998E-05	4.999E-05	1.000E-08	1.000E-08	5.00E-09
2	2.0	2.000E-04	9.999E-05	1.000E-08	9.997E-01	9.996E-05	4.998E-05	2.000E-08	2.000E-08	1.50E-08
3	3.0	2.999E-04	1.500E-04	3.000E-08	9.996E-01	9.994E-05	4.996E-05	2.999E-08	2.999E-08	2.50E-08
4	4.0	3.999E-04	1.999E-04	5.999E-08	9.994E-01	9.992E-05	4.995E-05	3.999E-08	3.999E-08	3.50E-08
5	5.0	4.998E-04	2.499E-04	9.998E-08	9.993E-01	9.990E-05	4.994E-05	4.998E-08	4.998E-08	4.50E-08
6	5.0	0.000E+00	2.499E-04	0.000E+00	9.998E-01	9.998E-05	4.996E-05	2.499E-08	2.499E-08	
7	6.0	9.998E-05	2.998E-04	2.499E-08	9.996E-01	9.996E-05	4.995E-05	3.498E-08	3.498E-08	3.00E-08
8	7.0	1.999E-04	3.498E-04	5.997E-08	9.995E-01	9.994E-05	4.994E-05	4.498E-08	4.498E-08	4.00E-08
9	8.0	2.999E-04	3.997E-04	1.049E-07	9.993E-01	9.992E-05	4.993E-05	5.497E-08	5.497E-08	5.00E-08
10	9.0	3.998E-04	4.497E-04	1.599E-07	9.992E-01	9.990E-05	4.991E-05	6.495E-08	6.495E-08	6.00E-08
11	10.0	4.997E-04	4.996E-04	2.249E-07	9.990E-01	9.988E-05	4.990E-05	7.494E-08	7.494E-08	6.99E-08
12	10.0	0.000E+00	4.996E-04	0.000E+00	9.995E-01	9.995E-05	4.993E-05	4.996E-08	4.996E-08	
13	11.0	9.995E-05	5.495E-04	4.996E-08	9.994E-01	9.993E-05	4.991E-05	5.995E-08	5.995E-08	5.50E-08
14	12.0	1.999E-04	5.994E-04	1.099E-07	9.992E-01	9.991E-05	4.990E-05	6.993E-08	6.993E-08	6.49E-08
15	13.0	2.998E-04	6.493E-04	1.798E-07	9.991E-01	9.989E-05	4.989E-05	7.992E-08	7.992E-08	7.49E-08
16	14.0	3.997E-04	6.992E-04	2.598E-07	9.989E-01	9.987E-05	4.988E-05	8.990E-08	8.990E-08	8.49E-08
17	15.0	4.996E-04	7.491E-04	3.497E-07	9.988E-01	9.985E-05	4.986E-05	9.988E-08	9.988E-08	9.49E-08
18	15.0	0.000E+00	7.491E-04	0.000E+00	9.993E-01	9.993E-05	4.989E-05	7.491E-08	7.491E-08	
19	16.0	9.993E-05	7.990E-04	7.491E-08	9.991E-01	9.991E-05	4.988E-05	8.489E-08	8.489E-08	7.99E-08
20	17.0	1.998E-04	8.488E-04	1.598E-07	9.990E-01	9.989E-05	4.986E-05	9.487E-08	9.487E-08	8.99E-08
21	18.0	2.997E-04	8.987E-04	2.547E-07	9.988E-01	9.987E-05	4.985E-05	1.049E-07	1.049E-07	9.99E-08
22	19.0	3.996E-04	9.485E-04	3.595E-07	9.987E-01	9.985E-05	4.984E-05	1.148E-07	1.148E-07	1.10E-07
23	20.0	4.994E-04	9.984E-04	4.744E-07	9.985E-01	9.983E-05	4.983E-05	1.248E-07	1.248E-07	1.20E-07
24	20.0	0.000E+00	9.984E-04	0.000E+00	9.990E-01	9.990E-05	4.985E-05	9.984E-08	9.984E-08	
25	21.0	9.990E-05	1.048E-03	9.984E-08	9.989E-01	9.988E-05	4.984E-05	1.098E-07	1.098E-07	1.05E-07
26	22.0	1.998E-04	1.098E-03	2.097E-07	9.987E-01	9.986E-05	4.983E-05	1.198E-07	1.198E-07	1.15E-07
27	23.0	2.996E-04	1.148E-03	3.295E-07	9.986E-01	9.984E-05	4.981E-05	1.298E-07	1.298E-07	1.25E-07
28	24.0	3.995E-04	1.198E-03	4.592E-07	9.984E-01	9.982E-05	4.980E-05	1.397E-07	1.397E-07	1.35E-07
29	25.0	4.993E-04	1.248E-03	5.990E-07	9.983E-01	9.980E-05	4.979E-05	1.497E-07	1.497E-07	1.45E-07
30	25.0	0.000E+00	1.248E-03	0.000E+00	9.988E-01	9.988E-05	4.981E-05	1.248E-07	1.248E-07	
31	26.0	9.988E-05	1.297E-03	1.248E-07	9.986E-01	9.986E-05	4.980E-05	1.347E-07	1.347E-07	1.30E-07
32	27.0	1.997E-04	1.347E-03	2.595E-07	9.985E-01	9.984E-05	4.979E-05	1.447E-07	1.447E-07	1.40E-07
33	28.0	2.996E-04	1.397E-03	4.042E-07	9.983E-01	9.982E-05	4.978E-05	1.547E-07	1.547E-07	1.50E-07
34	29.0	3.994E-04	1.447E-03	5.588E-07	9.982E-01	9.980E-05	4.976E-05	1.646E-07	1.646E-07	1.60E-07
35	30.0	4.992E-04	1.496E-03	7.235E-07	9.980E-01	9.978E-05	4.975E-05	1.746E-07	1.746E-07	1.70E-07
36	30.0	0.000E+00	1.496E-03	0.000E+00	9.985E-01	9.985E-05	4.978E-05	1.496E-07	1.496E-07	

SAENORM.COM : Click to view the full PDF of arp4761a

Table I4 (continued)

37	31.0	9.985E-05	1.546E-03	1.496E-07	9.984E-01	9.983E-05	4.976E-05	1.596E-07	1.596E-07	1.55E-07
38	32.0	1.997E-04	1.596E-03	3.093E-07	9.982E-01	9.981E-05	4.975E-05	1.696E-07	1.696E-07	1.65E-07
39	33.0	2.995E-04	1.646E-03	4.788E-07	9.981E-01	9.979E-05	4.974E-05	1.795E-07	1.795E-07	1.75E-07
40	34.0	3.993E-04	1.695E-03	6.584E-07	9.979E-01	9.977E-05	4.973E-05	1.895E-07	1.895E-07	1.85E-07
41	35.0	4.991E-04	1.745E-03	8.479E-07	9.978E-01	9.975E-05	4.971E-05	1.995E-07	1.995E-07	1.94E-07
42	35.0	0.000E+00	1.745E-03	0.000E+00	9.983E-01	9.983E-05	4.974E-05	1.745E-07	1.745E-07	
43	36.0	9.983E-05	1.795E-03	1.745E-07	9.981E-01	9.981E-05	4.973E-05	1.845E-07	1.845E-07	1.80E-07
44	37.0	1.996E-04	1.845E-03	3.590E-07	9.980E-01	9.979E-05	4.971E-05	1.944E-07	1.944E-07	1.89E-07
45	38.0	2.994E-04	1.894E-03	5.535E-07	9.978E-01	9.977E-05	4.970E-05	2.044E-07	2.044E-07	1.99E-07
46	39.0	3.992E-04	1.944E-03	7.579E-07	9.977E-01	9.975E-05	4.969E-05	2.144E-07	2.144E-07	2.09E-07
47	40.0	4.989E-04	1.994E-03	9.722E-07	9.975E-01	9.973E-05	4.968E-05	2.243E-07	2.243E-07	2.19E-07
48	40.0	0.000E+00	1.994E-03	0.000E+00	9.980E-01	9.980E-05	4.970E-05	1.994E-07	1.994E-07	
49	41.0	9.980E-05	2.043E-03	1.994E-07	9.979E-01	9.978E-05	4.969E-05	2.093E-07	2.093E-07	2.04E-07
50	42.0	1.996E-04	2.093E-03	4.087E-07	9.977E-01	9.976E-05	4.968E-05	2.193E-07	2.193E-07	2.14E-07
51	43.0	2.993E-04	2.143E-03	6.280E-07	9.976E-01	9.974E-05	4.966E-05	2.292E-07	2.293E-07	2.24E-07
52	44.0	3.991E-04	2.192E-03	8.573E-07	9.974E-01	9.972E-05	4.965E-05	2.392E-07	2.392E-07	2.34E-07
53	45.0	4.988E-04	2.242E-03	1.096E-06	9.973E-01	9.970E-05	4.964E-05	2.492E-07	2.492E-07	2.44E-07
54	45.0	0.000E+00	2.242E-03	0.000E+00	9.978E-01	9.978E-05	4.966E-05	2.242E-07	2.242E-07	
55	46.0	9.978E-05	2.292E-03	2.242E-07	9.976E-01	9.976E-05	4.965E-05	2.342E-07	2.342E-07	2.29E-07
56	47.0	1.995E-04	2.341E-03	4.584E-07	9.975E-01	9.974E-05	4.964E-05	2.441E-07	2.441E-07	2.39E-07
57	48.0	2.993E-04	2.391E-03	7.025E-07	9.973E-01	9.972E-05	4.963E-05	2.541E-07	2.541E-07	2.49E-07
58	49.0	3.990E-04	2.441E-03	9.566E-07	9.972E-01	9.970E-05	4.961E-05	2.640E-07	2.640E-07	2.59E-07
59	50.0	4.987E-04	2.490E-03	1.221E-06	9.970E-01	9.968E-05	4.960E-05	2.740E-07	2.740E-07	2.69E-07
60	50.0	0.000E+00	0.000E+00	0.000E+00	1.000E+00	1.000E-04	5.000E-05	0.000E+00	0.000E+00	
			Calculated Prob/hr. = SUM(P5.P11. P17,P23,P29, P35,P41,P47, P53,P59)/50 =	1.3217E-07					Average System Failure Rate (per hour) = SUM(I0:I60)/50 =	1.3716E-07
			Calculated prob/hr using a better (i.e., smaller step size) integrator =	1.3714E-07						

SAENORM.COM : Click to view the full PDF of arp4761a

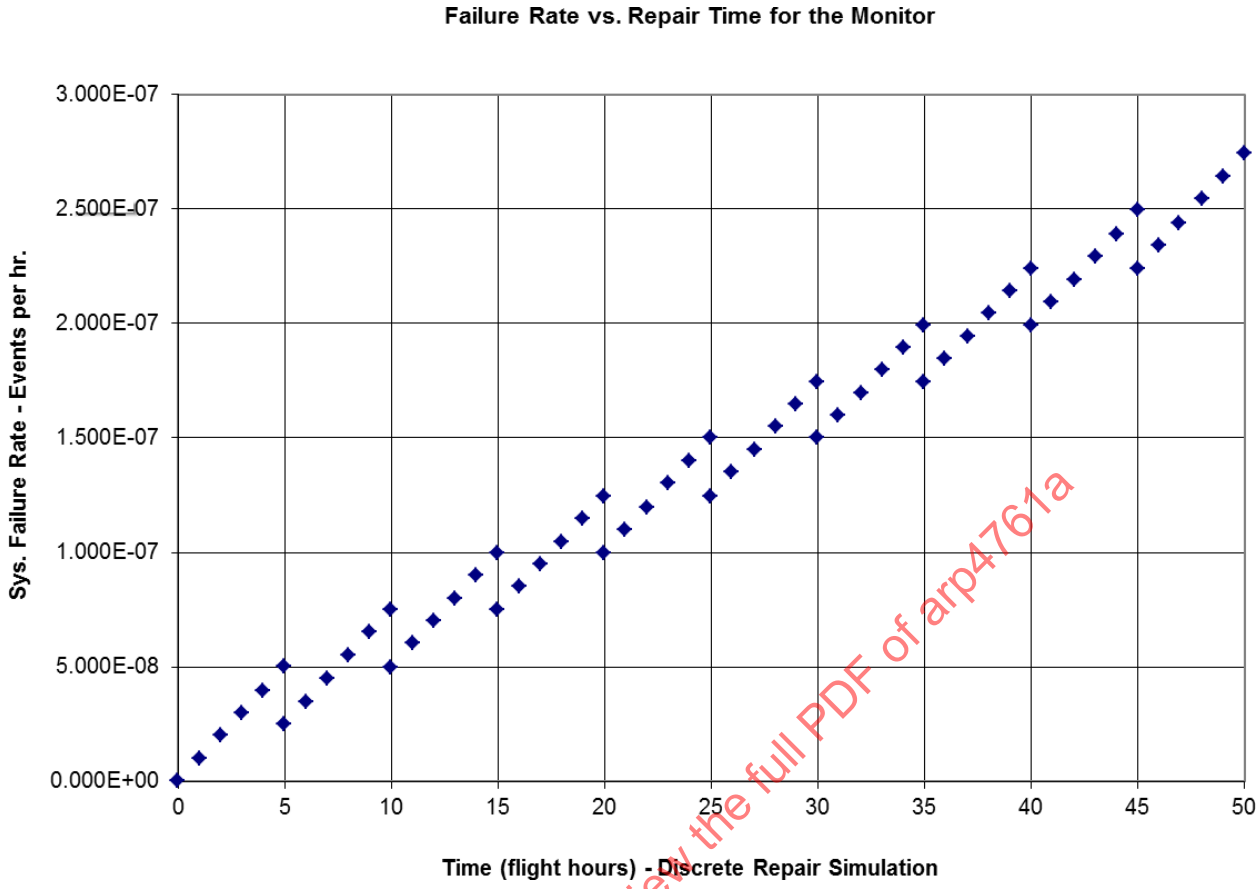


Figure I21 - Failure rate time history for the two-equipment system using discrete repair with different repair times for the equipment

Column H of Table I4 shows the calculated value of the system failure rate at each point in time. Column I is the simple time integral of Column H for the previous hour. Thus, Column I, Row #1 is:

Column I, Row #1 value = (Column H, Row #0 + Column H, Row #1)/2

The integral value is zero for those rows where P1 is being reset, as no time elapses during the reset.

The average system failure rate is the integral of the system failure rate from time zero to 50 hours, divided by 50 hours. This is the sum of all the time integral values given in Column H of Table I4 divided by the 50-hour flight time. This value is 1.37156E-07 events per hour. This compares very well with the simple closed-loop solution using continuous TSF repair of 1.37032E-07 failure events per hour. The difference is approximately 0.09%.

The Table also shows the computed probability/hour. of being in the Pfail state in Column D. The computed value given in Column D, Row 70, is 1.3217E-07 events/flight hour. The difference between this value and the average failure rate of 1.37156 events/flight hour. is 3.7%. This is more than acceptable agreement for most engineering problems, but note that this larger-than-normal discrepancy in these numbers is due to the large integration step size of 1 hour that was used in the spreadsheet. When a more refined “integrator” (i.e., a program which has step size control to limit computation error) is used, a more accurately calculated value for the probability per hour of failure is shown in Column D, Row 71 as 1.3714E-07 events per hour. This is in excellent agreement with the average failure rate as calculated from the time history of the instantaneous failure rate.

The (lambda*T)s for this problem are $\lambda_1 * T_1$ = 1E-04 = E-04, and $\lambda_2 * T_2$ = 50*5E-05 = 2.5E-03. Since both of these values are much less than 0.1, the calculated average from the time history of the instantaneous failure rate agrees quite well with the average value as calculated from the time history of the probability state. If the (lambda*T)s were not small (i.e., each less than 0.1), the two different calculated average would not be in agreement and the analyst should use the failure rate as calculated from the time history data of the probability of being in the failed state at the end of each flight, or in this case, at the end of each 5-hour interval.

SAENORM.COM : Click to view the full PDF of arp4761a

In summary, this example illustrates—in more detail than the example in I.3.0—how discrete repairs are simulated in an MM. Although computing the time histories for the various probability states in discrete repair models/simulations is more complex than determining the average failure rate from steady-state, continuous repair models, the discrete repair simulations are more accurate for models where periodic inspections and repairs are the in-service maintenance scenario/approach. This is particularly true when the model has multiple higher order multiple failure states, such as states with two or more failed elements. The reason for this is that when there are higher order multiple failure states, the determination of a continuous repair rate value to replace a discrete repair interval for a multiple element failure state becomes increasingly difficult to estimate. Hence, if an accurate representation of a discrete repair scenario is wanted/needed, use the discrete repair simulation approach.

Simple closed-loop MMs with continuous repair rates—based on TSF repair times, which can be equated to periodic, discrete repair actions—provide a much easier approach to obtaining system failure rates. The above example illustrates this for a simple system. As the system becomes more complex, the savings in computational effort and the bookkeeping of the various repair actions is far more dramatic. Hence, always attempt to use continuous time-since fault repair times (the reciprocal of which is a continuous repair rate) and a closed-loop MM approach when using an MM to estimate the average failure rate of a system.

I.4.4.3 Choice of Solution Method

The choice of whether to use a continuous repair, steady-state modeling approach or to use the discrete repair approach is always one which generates much discussion. If the system being modeled uses an in-service inspection/repair approach, the discrete repair time history model will provide a more accurate solution.

Having said that, the continuous repair steady-state models can provide a suitably accurate approach and solution method, which is much easier to calculate. For example, assume a model has several single failure states and each failure state has a reasonably frequent TSF or periodic inspection repair interval. In such a situation, the probability of having the system be in a multiple element failure state is quite small, and the higher states can be neglected with little error in estimating (computing) the average system failure rate. When this is the case, using continuous repair transitions, which model TSF repair rates set to the reciprocal of 1/2 of the periodic inspection/repair time intervals, will yield an accurate solution for the average system failure rate. When multiple failure states need to be included in the model, the analyst can still use the reciprocal of 1/2 of the inspection/repair time for the continuous repair rate for those multiple failure states. The result will lose a bit of accuracy, but the resulting value for the average system failure rate will be a conservative one. In other words, the calculated system failure rate will be higher than it actually is.

If a Markov modeling computer program is available, the analyst can simply use it. Care should be exercised to understand how the program computes the model. For example, if fully failed state has to be reset after every flight because the aircraft is not considered to be dispatchable in that condition, then it needs to be assured that the modeling program will do this. Actual experience with the two different approaches is most useful. Experience is the best teacher.

I.4.4.3.1 Steady-State versus Transient

The initial state of a system is commonly taken to be “full-up.” In this event, system steady-state reliability is less than the initial reliability. The transient solution tracks system degradation from full-up to steady-state and the average reliability based on the transient solution may be greater than the steady-state reliability. This implies that the transient average failure rates (at earlier time intervals) will be less than the steady-state average failure rate. Thus, the closed-loop MM based steady-state average failure rates may be conservative if the interval of system operation is not long enough to reach steady-state. The effect fades as the number of inspection/repair maintenance intervals increases. As a rule of thumb, transient effects can be ignored in computation of average reliability if there are four or more of the longest inspection/repair maintenance intervals in the life of the system being modeled.

I.4.4.3.2 Discrete Repair versus Continuous Repair

If the product λT is small (e.g., less than 0.1), where λ is the equipment failure rate and T is the inspection interval, there is little error in approximating a discrete repair at T by a continuous repair with repair rate 2/T. Errors are introduced as the product λT increases.

SAENORM.COM : Click to view the full PDF of arp4761a

If λT equals 0.1 the relative error in the approximation is about 10 percent. For most analyses calculation, an error of 10% is considered acceptable in a system's estimated failure rate. It is possible to compensate for large values λT of by adjusting the repair rate, but this process becomes complicated if there are several distinct inspection intervals T_k, each of which has the property that the product $\lambda_k T_k$ is large.

If the error in using a continuous repair rate is considered unacceptable, the analyst can choose to use the time history, discrete repair modeling approach.

I.4.5 Example of an Average Failure Rate Analysis for an Active System (Which Has Internal Fault Monitoring) and a Backup System (Which Has an External Fault Monitor)

Figure I22 shows the block diagram of the active-backup system to be analyzed.

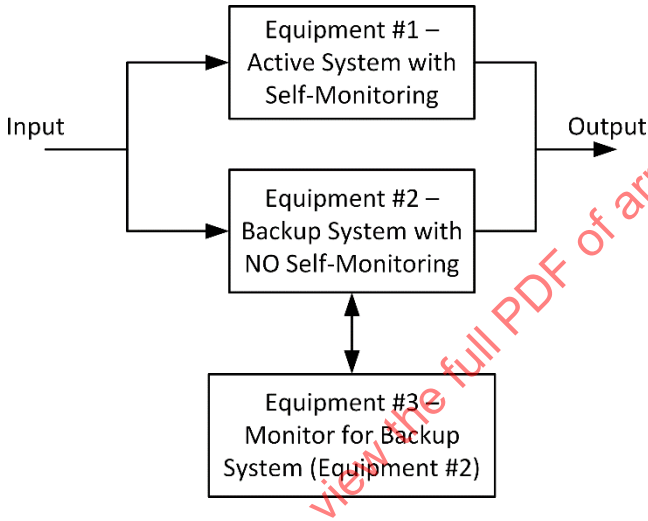


Figure I22 - Diagram of active system with self-monitoring and back-up system with an independent monitor

SAENORM.COM : Click to view the full PDF of arp4761a

Assume the following system description, logic, and data are given:

a. λa is the failure rate for the active system, equipment #1. The active system has full time self-monitoring and it is checked for operability prior to every flight. If the system is found to be faulty or inoperative, it is repaired before dispatch.

b. λb is the failure rate for the back-up system. The backup system has no self-monitoring, but is monitored by an independent monitor equipment. If the backup system fails in a flight and the monitor is working, the backup is repaired before the next dispatch. If the monitor is not working the backup can fail latently, but it is checked every ten flights. If found faulty, and there was no monitor indication of a back-up system failure, then the monitor is failed also. Repair both before the next flight.

c. λm is the failure rate for the monitor. If it fails, it can be repaired in one of two ways. First is the repair when the backup system is found failed at its periodic inspection and there was no monitor indication of a backup system failure, in which case both the back-up and monitor are repaired before the next flight; second, there is a 100-flight check on the operability of the monitor. If it is checked at the 100-flight interval and found failed, it is repaired.

d. Tflt is the average flight time. Assume 5 hours.

Also assume that the following failure rates are given:

a. λa = 5.0E-05 failures per hour.

b. λb = 2.5E-05 failures per hour.

c. λm = 2.5E-05 failures per hour.

Even though the repair actions are described as discrete, periodic inspections and repairs, the following solution will use the continuous TSF repair rate approach because the calculations are much simpler to complete and the solution for the average system failure rate will be just as accurate as a solution using periodic discrete repair.

The MM diagram for the system is given in Figure I23.

In Figure I23, P1 is the probability of the active equipment being failed, P2 is the probability of the back-up being failed, P3 is the probability of the monitor being failed, P4 is the probability of having both the monitor and back-up equipment failed at the same time, and P5 is the probability of having both the monitor and the active system failed at the same time. If the back-up and active equipment are failed at the same time, the system is failed.

μflt is the repair rate for the active system and the back-up system when the monitor is not failed. Since the periodic inspection time of 5 hours is far less than the MTBF of the active and back-up equipment, respectively, the continuous repair time for each of these single equipment failure cases is set to 1/2 of the flight time, or 2.5 hours.

Hence, μflt = 1/2.5 = 0.4 repair events per hour.

In Figure I23, the μflt repair rate is also used for state P5, because if the monitor equipment is unknowingly failed and the active system fails, or vice versa, only the active system would be repaired before the next flight. The repair of the monitor is addressed by its own repair rate, μm. The discrete periodic repair time for the monitor is 100 flights, or 500 hours. Since 500 hours is far less than the MTBF of the monitor equipment (40000 hours), the TSF repair time for the monitor is set to one half of the 500-hour periodic inspection/repair time, which is 250 hours.

SAENORM.COM : Click to view the full PDF of arp4761a

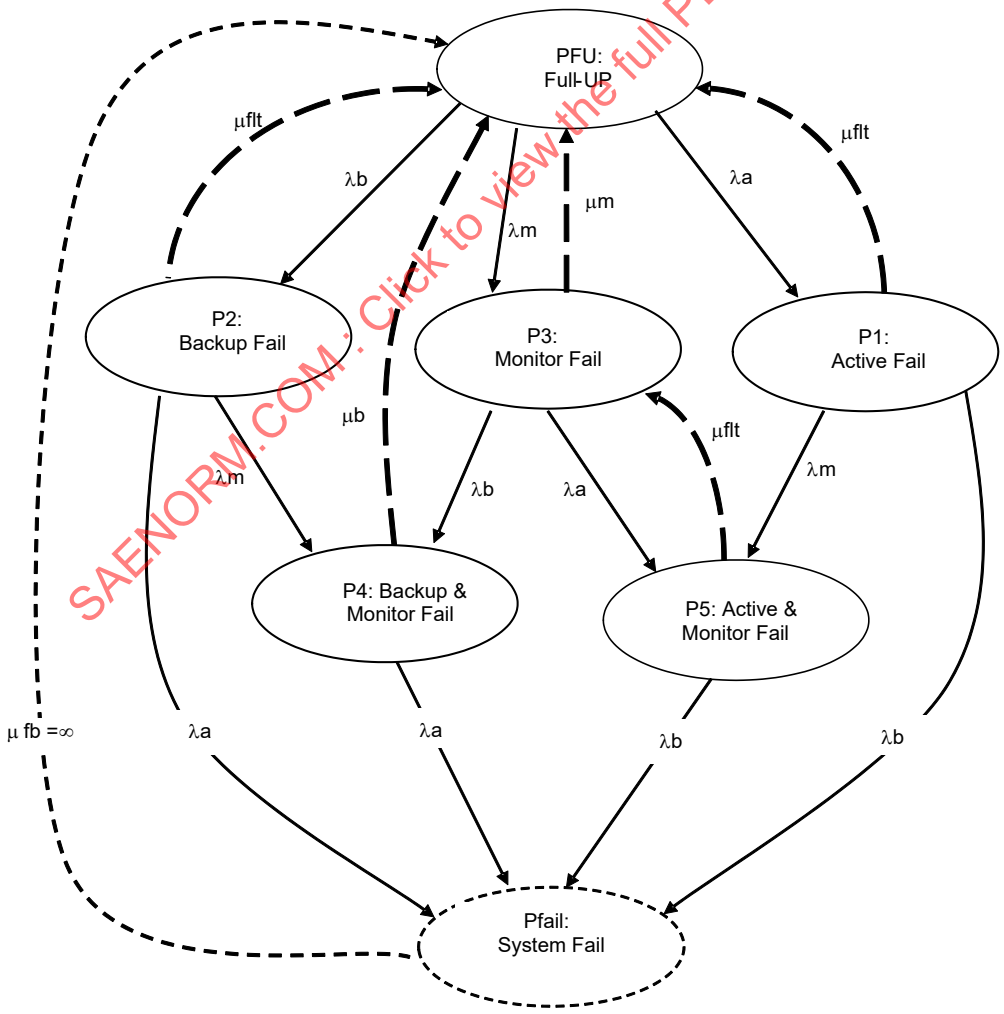


Figure I23 - Markov Model for an active system with internal self-monitoring and a backup system with independent monitor

Hence, μm = 1/250 = 0.004 repair events per hour.

As indicated above, even though there may be no indicated failure of the back-up equipment, the equipment is checked every ten flights (50 hours) for operability. If found failed, the monitor should be failed as well, and both are repaired before the next flight. Since the 50-hour check period is far smaller than the MTBF of the back-up system, which is 40000 hours, the continuous TSF repair time is very close to 1/2 the 50-hour check period.

Hence, μb = 1 /25 = 0.04 repair event per hour.

The steady-state equations for this system model are shown in Equations I82 through I86:

For state P1: $$\lambda a*PFU = (\lambda b + \lambda m + \mu flt)*P1 \quad \text{(Eq. I82)}$$

For state P2: $$\lambda b*PFU = (\lambda m + \lambda a + \mu flt)*P2 \quad \text{(Eq. I83)}$$

For state P3: $$\lambda m*PFU + \mu flt*P5 = (\lambda a + \lambda b + \mu m)*P3 \quad \text{(Eq. I84)}$$

For state P4: $$\lambda m*P2 + \lambda b*P3 = (\lambda a + \mu b)*P4 \quad \text{(Eq. I85)}$$

For state P5: $$\lambda m*P1 + \lambda a*P3 = (\lambda b + \mu flt)*P5 \quad \text{(Eq. I86)}$$

Conservation equation: $$1 = PFU + P1 + P2 + P3 + P4 + P5 \quad \text{(Eq. I87)}$$

Or: $$1/PFU = 1 + (P1 + P2 + P3 + P4 + P5)/PFU \quad \text{(Eq. I88)}$$

The system failure rate equation is shown in Equation I89:

$$\lambda(\text{avg sys-fail}) = \lambda b\,(P1 + P5) + \lambda a\,(P2 + P4) \quad \text{(Eq. I89)}$$

The system equations can be written in matrix form as shown in Equation I90:

$$C\,P = U \quad \text{(Eq. I90)}$$

Where C is the coefficient matrix:

λa	-(λb+λm+μflt)				
λb		-(λm+λa+μflt)			
λm			(λa+λb+μm)		μflt
		λm	λb	-(λa + μb)	
	λm		λa		-(λb+μflt)
1	1	1	1	1	1

P is the column vector [PFU, P1, P2, P3, P4, P5]^T, and U the column vector [0, 0, 0, 0, 0, 1]^T

And the failure rate equation can be represented by the simple algebraic/vector Equation I91.

$$\lambda(\text{avg sys-fail}) = L\,C - 1\,U \quad \text{(Eq. I91)}$$

Where L is the row vector [0, λb, λa, 0, λa, λb].

It is straight forward to use a matrix solver program to invert the C matrix and do the indicated multiplications to determine the system failure rate.

SAENORM.COM : Click to view the full PDF of arp4761a

In many cases, this system of algebraic equations can be solved by hand. This is shown as follows:

Divide the system failure rate Equation I89 by PFU, and use Equation I87 in the denominator to obtain Equation I92:

$$\text{I (avg sys-fail)} = \frac{(\lambda b\ (P1/PFU + P5/PFU) + \lambda a\ (P2/PFU + P4/PFU))}{(1 + (P1 + P2 + P3 + P4 + P5)/PFU)} \quad \text{(Eq. I92)}$$

Divide the system Equations I82 through I86 by PFU to obtain Equations I93 through I97:

$$P1/PFU = \lambda a/(\lambda b + \lambda m + \mu flt) \quad \text{(Eq. I93)}$$

$$P2/PFU = \lambda b/(\lambda a + \lambda m + \mu flt) \quad \text{(Eq. I94)}$$

$$P3/PFU = (\lambda m + \mu flt*(P5/PFU))/(\lambda a + \lambda b + \mu m) \quad \text{(Eq. I95)}$$

$$P4/PFU = (\lambda m*(P2/PFU) + \lambda b*(P3/PFU))/(\lambda a + \mu b) \quad \text{(Eq. I96)}$$

$$P5/PFU = (\lambda m*(P1/PFU) + \lambda a*(P3/PFU))/(\lambda b + \mu flt) \quad \text{(Eq. I97)}$$

Substituting (P5/PFU) from Equation I97 into Equation I95 and re-arranging terms, yields Equation I98:

$$P3/PFU = \frac{(\lambda m + (\mu flt*\lambda m/(\lambda b + \mu flt))*(P1/PFU))}{(\lambda a + \lambda b + \mu m - \mu flt*\lambda a/(\lambda b + \mu flt)))} \quad \text{(Eq. I98)}$$

At this point, Equations I93 through I97 can be evaluated sequentially to obtain values for P1/PFU through P5/PFU, and those values can be substituted into Equation I92 to obtain the value for the system failure rate.

Also, noted in Equations I93 through I97, no values for state probabilities are involved in the failure rate calculations. Only the values for the failure rates and repair rates are involved. Again, that is a good illustration of why an MM is (in many cases) really a failure rate model, not a probability model.

Table I5 shows the calculations.

Table I5 - Spreadsheet for system failure rate calculations for active/back-up/monitor system of Figures I22 and I23

This is the spreadsheet for the active/passive/monitor system
Mu(flt) is repair for active and backup (when monitor is working),
Mu(b) is the repair for monitor and back-up failed (state P4)
Mu(m) is repair rate for just monitor failed.

lambda(a)	lambda(b)	lambda(m)	Flt. Time	Mu(flt)	Mu(b)	Mu(m)
5.00E-05	2.50E-05	2.50E-05	5	0.4	0.04	0.004
	P1/PFU	P2/PFU	P3/PFU	P4/PFU	P5/PFU	Lambda Fail
	1.250E-04	6.249E-05	6.212E-03	3.917E-06	7.843E-07	6.423E-09

Using the various failure rates and repair rates, Equations I93 through I97 yield the probability ratios P1/PFU through P5/PFU. Using these values, Equation I92 yields the system failure rate as: λ(avg sys-fail) = 6.423*E^{-9} failure events per hour.

SAENORM.COM : Click to view the full PDF of arp4761a

This approach is much simpler than integrating the first order time differential state equations (as shown in Table I4 for the two-equipment system with discrete repair) for P1 through P5 of this system and simulate discrete repairs of (1) the active equipment, back-up equipment (when the monitor is working), and active/monitor failed state at 5 hours; and (2) the combined back-up/monitor failed state at 50 hours, until the 500-hour time point is reached. Even with a large 1-hour integration time, that would take 500 time steps involving 100 resets of the P1, P2, and P5 states, and ten resets of the P4 state.

In addition, using the closed-loop, steady-state, continuous TSF approach allows a much easier understanding of the impact of various repair rates on the system failure rate. For example, it is easy to determine the system failure rate when the repair rates for the back-up equipment, μb, and the monitor, μm, are the same. These calculations are shown in Table I6.

It is interesting to plot the results shown in Table I6 (for the system failure rate as a function of the repair rates for the back-up and monitor equipment), with the original problem definition (where the back-up and monitor inspection time were specified as 50 hours and 500 hours, respectively). Figure I24 presents the comparison.

This is interesting because the data shows that the failure rate of the system is nearly the same when the repair rates for both the back-up and monitor equipment are equal and occur at a rate of 0.01 repairs/hour or greater. This is a TSF repair interval of a 100 hours or less, or a periodic inspection/repair period of 200 hours or less. Assume an inspection interval of 200 hours and at that inspection time, both the back-up and monitor equipment are checked for operability. If either or both are found failed, they are repaired.

Table I6 - Active/back-up/monitor system failure rates as a function of the back-up and monitor equipment repair rate when those repair rates are the same

lambda(a)	lambda(b)	lambda(m)	Flt. Time	Mu(flt)		
5.00E-05	2.50E-05	2.50E-05	5	0.4		
Mu(b) = Mu(m)	P1/PFU	P2/PFU	P3/PFU	P4/PFU	P5/PFU	Lambda Fail
0.00100	1.250E-04	6.249E-05	2.439E-02	5.823E-04	3.057E-06	3.457E-08
0.00200	1.250E-04	6.249E-05	1.235E-02	1.513E-04	1.551E-06	1.368E-08
0.00300	1.250E-04	6.249E-05	8.265E-03	6.826E-05	1.041E-06	9.606E-09
0.00400	1.250E-04	6.249E-05	6.212E-03	3.873E-05	7.843E-07	8.153E-09
0.00500	1.250E-04	6.249E-05	4.976E-03	2.494E-05	6.297E-07	7.473E-09
0.00600	1.250E-04	6.249E-05	4.150E-03	1.741E-05	5.265E-07	7.102E-09
0.00700	1.250E-04	6.249E-05	3.559E-03	1.284E-05	4.527E-07	6.877E-09
0.00800	1.250E-04	6.249E-05	3.116E-03	9.870E-06	3.972E-07	6.730E-09
0.00900	1.250E-04	6.249E-05	2.770E-03	7.826E-06	3.541E-07	6.629E-09
0.01000	1.250E-04	6.249E-05	2.494E-03	6.360E-06	3.196E-07	6.557E-09
0.01100	1.250E-04	6.249E-05	2.268E-03	5.272E-06	2.913E-07	6.504E-09
0.01200	1.250E-04	6.249E-05	2.079E-03	4.443E-06	2.677E-07	6.463E-09
0.01300	1.250E-04	6.249E-05	1.920E-03	3.797E-06	2.477E-07	6.431E-09
0.01400	1.250E-04	6.249E-05	1.783E-03	3.283E-06	2.306E-07	6.406E-09
0.01500	1.250E-04	6.249E-05	1.664E-03	2.868E-06	2.158E-07	6.386E-09

SAENORM.COM : Click to view the full PDF of arp4761a

Compare this with the original repair definition, which was an inspection of the back-up equipment every 50 hours, and an inspection of the monitor equipment every 500 hours. In the original system definition, 1000 hours of operation would have involved 22 inspections; 20 for the back-up system and two for the monitor. However, if the inspection period for both the back-up and monitor are set to 200 hours, then there would only be ten inspections involved; five for the monitor and five for the back-up system. This may be a significant reduction in maintenance labor.

The ability to do these types of comparisons readily and easily is associated with using a steady-state, closed-loop MM approach and continuous TSF repair rates. When open-loop time dependent MMs are used and there are several different repair times for the different elements in the system, the calculations can become quite tedious, unless the analysis is performed using a computer program designed for the task.

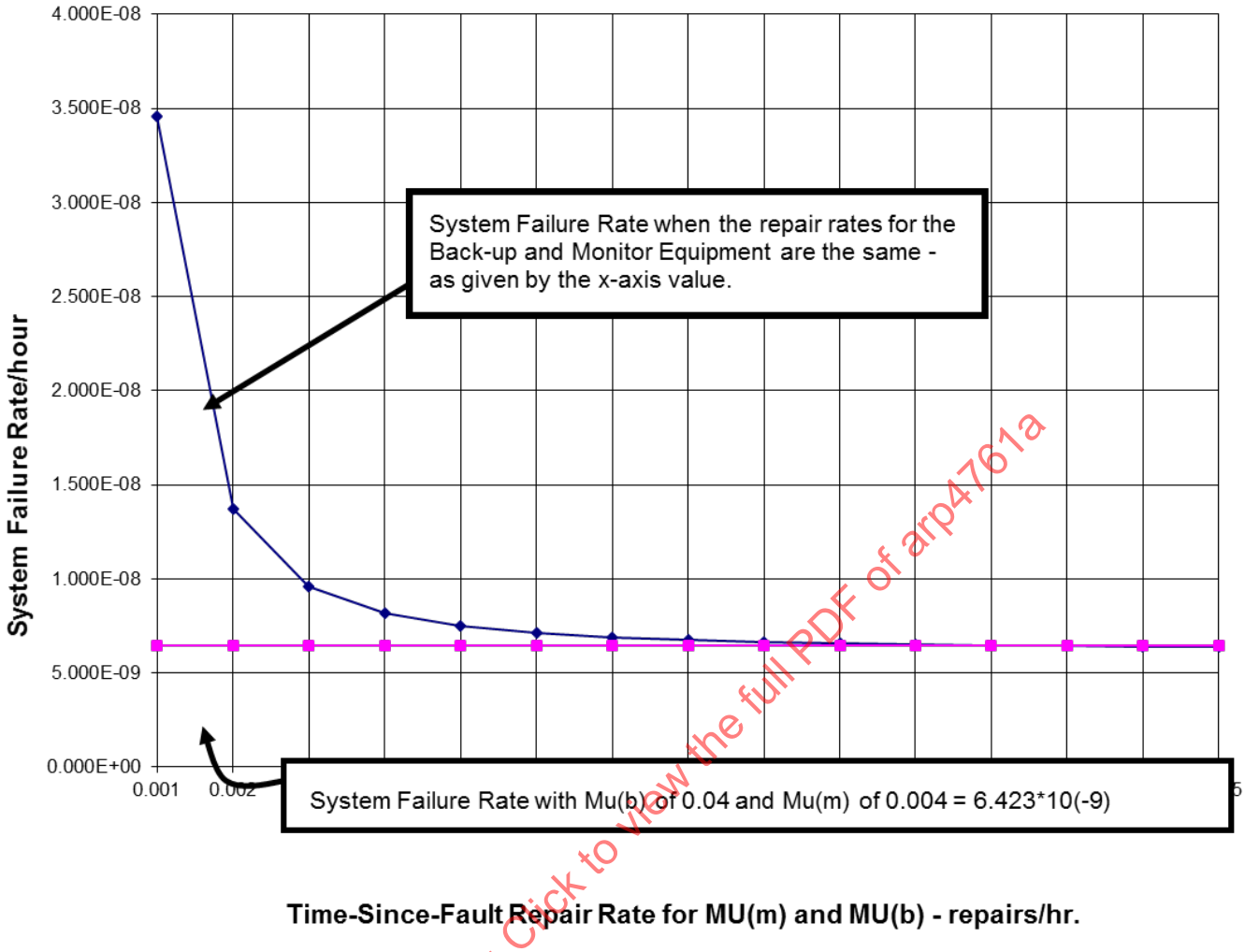


Figure I24 - Impact of equal repair rates for the back-up and monitor system on the system failure rate

I.4.6 A Discussion of Model Completeness

It is always difficult to check the completeness of an MM. This is not necessarily because assembling a complete model is difficult, but rather, it's a question as to whether a simplified model—which may be much easier to work with—is sufficiently complete in its definition to yield a reasonably accurate result. Namely, have all significant failure states been included in the model, and are the significant transition paths between those various states adequately represented.

As with any modeling effort, an MM is an idealization of the system, and often the model creator can simplify the model to focus on those parameters of interest. Because of the state space explosion associated with higher numbers of modeled equipment, reduction of complexity is particularly important in Markov modeling. An experienced user can simplify an MM without compromising accuracy.

MMs do NOT have to be complete to be reasonably accurate. Consider, for example, the last example of the active/back-up/monitor system shown in Figures I22 and I23.

Consider the possibility of deleting the P5 state from the model. This is the dual failure state where both the monitor and active equipment are failed. In looking at the model, the probability of being in the P5 state is probably quite small. The system can transition to this state from the active equipment failed (P1) state, which should occur initially in that flight, and then in the remainder of that flight the monitor fails, or alternately, dispatching with the monitor failed and then having the active equipment fail. The second case is more likely of the two, as the monitor could be in unknowingly failed for several flights. In either case, the P5 state is repaired back to the P3 state at the end of that flight because the active equipment must be replaced before the next dispatch.

SAENORM.COM : Click to view the full PDF of arp4761a

Thus, the time spent in the P5 state would normally be approximately 1/2 of a flight. In addition, the back-up equipment should fail during that period to cause a total system failure. Hence, the impact of retaining this state, although it does provide “completeness,” is considered small.

The MM diagram for the system without the P5 state is shown in Figure I25.

The steady-state system equations without the P5 state are shown in Equations I99 through I102:

$$P1/PFU = \lambda_a/(\lambda_b + \lambda_m + \mu_{flt}) \quad \text{(Eq. I99)}$$

$$P2/PFU = \lambda_b/(\lambda_a + \lambda_m + \mu_{flt}) \quad \text{(Eq. I100)}$$

$$P3/PFU = \lambda_m/(\lambda_a + \lambda_b + \mu_m) \quad \text{(Eq. I101)}$$

$$P4/PFU = (\lambda_m*(P2/PFU) + \lambda_b*(P3/PFU))/(\lambda_a + \mu_b) \quad \text{(Eq. I102)}$$

The conservation equation is shown in Equation I103:

$$1/PFU = 1 + (P1 + P2 + P3 + P4)/PFU \quad \text{(Eq. I103)}$$

The spreadsheet calculations for the system without the P5 state are given in Table I7.

SAENORM.COM : Click to view the full PDF of arp4761a

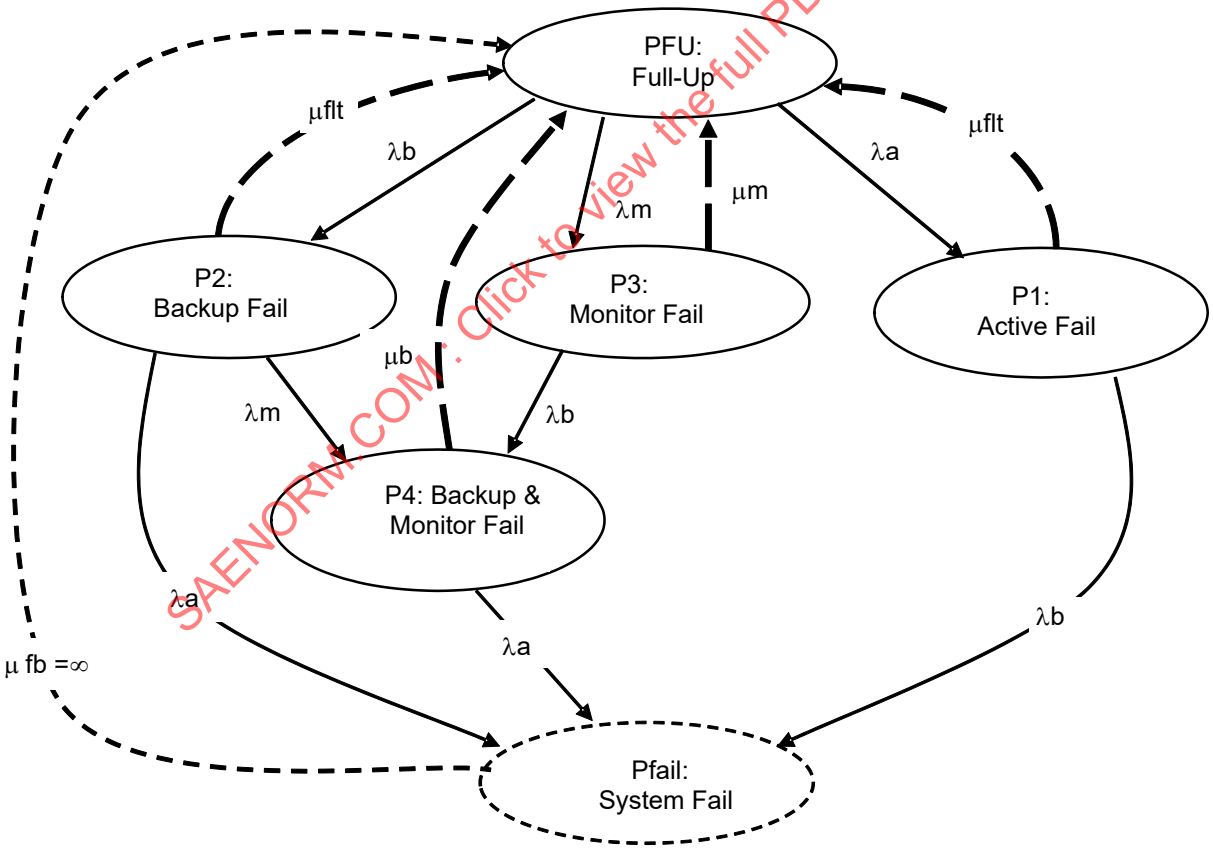


Figure I25 - MM for active/back-up, monitor system of Figure I23 without the active/monitor (P5) dual equipment failure state

Column F in Table I7 represents the system failure rate without the P5 state, and Column G represents the system with the P5 state included. The Table I7 Column G calculations are the same as those given in the “lambda fail” column of Table I6. The difference between the calculated results with and without the P5 state is less than 0.5%. This is adequate accuracy.

This is a good example where a model does not have to be “complete” to yield an accurate failure rate calculation. There are many models where the higher order states, meaning those states that involve multiple failures, are only present for small periods (i.e., before a repair transitions the state to another one). These higher order, multiple failure element states do not have a significant contribution to the calculated failure rate result. However, if the repair interval for an equipment (a) failure were to be significantly lengthened, deleting the P5 state from the model would yield increasingly inaccurate results, as the probability of being in the P5 state increases significantly as the repair time for a failed equipment or element is lengthened.

Table I7 - Comparison of system failure rate calculation results with and without P5 state

lambda(a)	lambda(b)	lambda(m)	Flt. Time	Mu(flt)			
5.00E-05	2.50E-05	2.50E-05	5	0.4			
Column	⟶						
A	B	C	D	E	F	G	H
					Lambda Fail	Lambda Fail	Percent
Mu(b) =					without P5	with P5	Error
Mu(m)	P1/PFU	P2/PFU	P3/PFU	P4/PFU	State	State	
0.001	1.250E-04	6.249E-05	2.439E-02	5.822E-04	3.449E-08	3.457E-08	2.24E-01
0.002	1.250E-04	6.249E-05	1.235E-02	1.513E-04	1.364E-08	1.368E-08	2.85E-01
0.003	1.250E-04	6.249E-05	8.264E-03	6.825E-05	9.580E-09	9.606E-09	2.71E-01
0.004	1.250E-04	6.249E-05	6.211E-03	3.873E-05	8.133E-09	8.153E-09	2.39E-01
0.005	1.250E-04	6.249E-05	4.975E-03	2.494E-05	7.457E-09	7.473E-09	2.09E-01
0.006	1.250E-04	6.249E-05	4.149E-03	1.740E-05	7.089E-09	7.102E-09	1.83E-01
0.007	1.250E-04	6.249E-05	3.559E-03	1.284E-05	6.865E-09	6.877E-09	1.62E-01
0.008	1.250E-04	6.249E-05	3.115E-03	9.869E-06	6.720E-09	6.730E-09	1.45E-01
0.009	1.250E-04	6.249E-05	2.770E-03	7.825E-06	6.621E-09	6.629E-09	1.31E-01
0.010	1.250E-04	6.249E-05	2.494E-03	6.359E-06	6.550E-09	6.557E-09	1.19E-01
0.011	1.250E-04	6.249E-05	2.268E-03	5.272E-06	6.497E-09	6.504E-09	1.09E-01
0.012	1.250E-04	6.249E-05	2.079E-03	4.443E-06	6.457E-09	6.463E-09	1.01E-01
0.013	1.250E-04	6.249E-05	1.919E-03	3.797E-06	6.425E-09	6.431E-09	9.34E-02
0.014	1.250E-04	6.249E-05	1.783E-03	3.283E-06	6.401E-09	6.406E-09	8.70E-02
0.015	1.250E-04	6.249E-05	1.664E-03	2.868E-06	6.381E-09	6.386E-09	8.15E-02

SAENORM.COM : Click to view the full PDF of arp4761a

There are no set guidelines or rules as to when to include multiple equipment failure states in a model when those states are intermediate failure states and not the fully failed state. In general, if multiple equipment failure states do not exist for any significant time period because the repair times for single equipment failures are reasonably small with respect to the failure rates of those equipment, they may be ignored without incurring significant error. However, this is not a general rule or conclusion. The choice to ignore, or not include multiple equipment failure states, is very dependent on the rest of the model. Unfortunately, as with most reliability analyses, experience is the best guideline.

This example simply shows that an acceptably accurate answer can be obtained from a model that does not include all failure states. This is also illustrated in ARP5107C, where for FADEC systems, it is shown that it is adequate to build an MM based on initial single failures; then, only consider those second failures—in combination with the first ones—that cause the system to result in a loss-of-thrust-control event. In the models discussed in ARP5107C, consideration of multiple failure states increases the accuracy of the model by about 2%, which is small in comparison with the difficulty involved in including all possible dual failure states that do not result in an LOTC event.

I.4.7 Examples of System Analyses Where Sequential Calculations Are and Are Not Immediately Available

In many systems, if repairs are always made from any state to the full-up state, the calculation procedure for determining the failure rate of the system is quite simple. This is because the calculations for each failure state can be completed in a sequential manner. That is, the probability ratio (or fraction) for each state is only dependent on the states “before” that state, and not on the ones after.

Consider a quad-redundant system with all channels being essentially the same. If repairs from all of the states take the system back to the full-up state, the MM diagram would look like that shown in Figure I26.

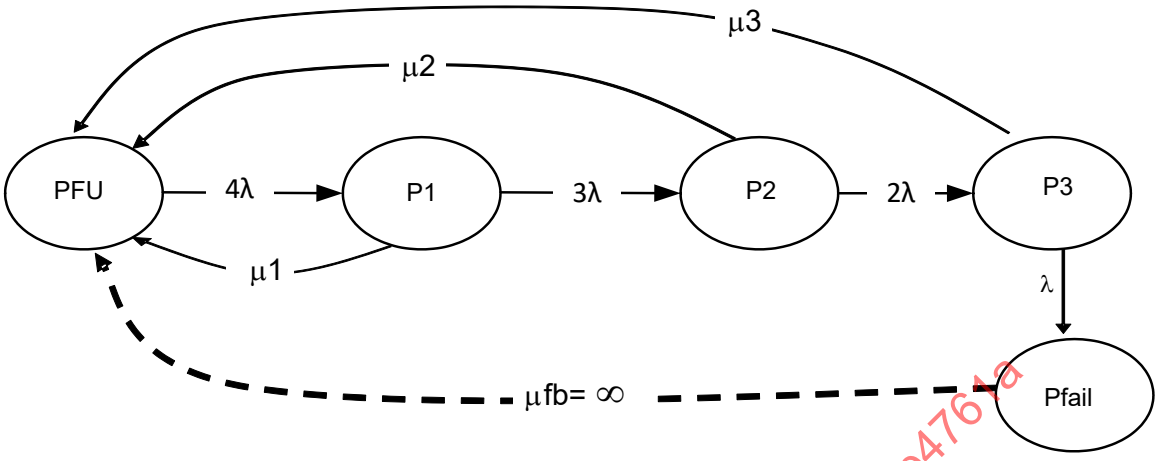


Figure I26 - Four-channel system with all repairs to full-up state

Where the PFU state represents all channels working (full-up state), the P1 state has one channel failed, the P2 state has two channels failed, etc. λ is the failure rate of a channel, and μ1, μ2, and μ3 represent the repair rates for the P1, P2, and P3 states, respectively.

Of course, this is a very simply model, but because the repair paths from all failure states are back to the full-up state, the probability ratios of each state can be calculated based on the state preceding it. That is:

$$P1/PFU = \text{constant} = (4\lambda)/(3\lambda + \mu 1)$$

$$P2/PFU = \text{constant}*(P1/PFU) = [3\lambda/(2\lambda + \mu 2)]*(P1/PFU)$$

$$P3/PFU = \text{constant}*(P2/PFU) = [2\lambda/(\lambda + \mu 3)]*(P2/PFU)$$

The failure rate equation is:

$$\lambda(fail) = \lambda * (P3/PFU)/(1 + P1/PFU + P2/PFU + P3/PFU)$$

Thus, knowing the channel failure rate λ and repair rates μ1, μ2, and μ3, calculations for P1/PFU, then P2/PFU, and then P3/PFU can be performed sequentially made and the results substituted into the failure rate equation to obtain the system failure rate.

However, if the repair paths do not take the model back to the full-up state, sequential calculations cannot be easily made.

SAENORM.COM : Click to view the full PDF of arp4761a

Consider the same four-channel system with repair paths not always going to the full-up state. An MM of the system might look like Figure I27:

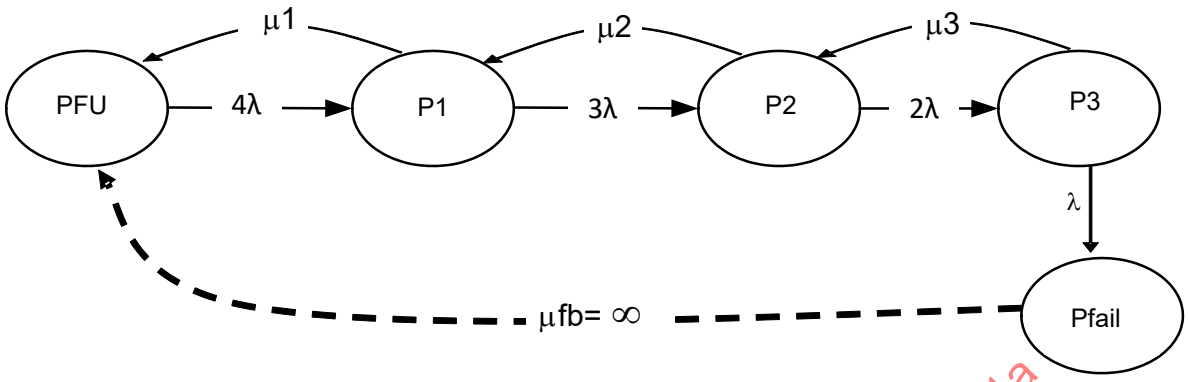


Figure I27 - Four-channel system with repairs to intermediate states

In this system, sequential calculations are not so easily made because P1 depends on P2 as well as PFU, and P2 depends on P3 as well as P1.

The P1 state equation is:

$$P1/PFU = (4\lambda)/(3\lambda + \mu1) + [\mu2/(3\lambda + \mu1)]*(P2/PFU)$$

The P2 state equation is:

$$P2/PFU = [3\lambda/(2\lambda + \mu2)]*(P1/PFU) + [\mu3/(2\lambda + \mu2)]*(P3/PFU)$$

The P3 state equation is:

$$P3/PFU = [2\lambda/(\lambda + \mu3)]*(P2/PFU)$$

As these equations stand, a sequential calculation for the probability ratios cannot be made. However, it is recognized that given values for the channel failure rate λ and the repair rates μ1, μ2, and μ3, an algebraic equation solver will readily yield the probability ratio values for P1/PFU, P2/PFU, and P3/PFU.

In this simple example, the state equation for P3/PFU could be substituted into the P2/PFU state equation and terms collected to obtain P2/PFU as a function of P1/PFU only. Then that equation could be substituted into the state equation for P1/PFU and terms collected to obtain an equation for the constant value of P1/PFU. In this simple example, this is possible; however, in a complex system where there are more than four equipment and repairs are made from one failure state to another state, which is not the full-up state, the algebra of setting up the equations so that sequential calculations can be made can be quite tedious and error prone.

If an algebraic equation solver is not readily available and the problem is more difficult than the one example given here, a spreadsheet iterative technique to calculate the probability ratios has shown itself to work quite well in many cases.

The iterative technique is illustrated as follows.

Assume the following data:

- $\lambda = 10^{-4}$ failures per hour.
- μ1 = 1/500.
- μ2 = 1/600.
- μ3 = 0.4 repairs per hour.

SAENORM.COM : Click to view the full PDF of arp4761a

Start out with P1/PFU = P2/PFU = P3/PFU = 0.0 and 1/PFU = 1.0.

Then set up the following iterative equations, where the superscript $(_n)$ means the new calculation for that value and the superscript $(^{n-1})$ means the previous iteration's value for that parameter.

$$(P1/PFU)^n = (4\lambda)/(3\lambda + \mu1) + [\mu2/(3\lambda + \mu1)]*(P2/PFU)^{(n-1)} \quad \text{(Eq. I104)}$$

$$(P2/PFU)^n = [3\lambda/(2\lambda + \mu2)]*(P1/PFU)^n + [\mu3/(2\lambda + \mu2)]*(P3/PFU)^{(n-1)} \quad \text{(Eq. I105)}$$

$$(P3/PFU)^n = [2\lambda/(\lambda + \mu3)]*(P2/PFU)^n \quad \text{(Eq. I106)}$$

$$(1/PFU)^n = 1 + (P1/PFU)^n + (P2/PFU)^n + (P3/PFU)^n \quad \text{(Eq. I107)}$$

And the system failure rate equation is simply:

$$\lambda(\text{avg system fail})^n = \lambda*(P3/PFU)^n/(1/PFU)^n \quad \text{(Eq. I108)}$$

Table I8 shows the iterative solution. Observe how quickly the iteration converges on the final solution for the probability ratios and the system's estimated failure rate—just six iterations.

This iterative technique provides a very quick and easy approach for calculating the solution to MMs where a sequential calculation technique in not possible. When using this iterative approach, there is no guarantee that the calculations will be stable, but experience with the method has shown it to be successful in many systems where sequential calculations are not possible.

Table I8 - Spreadsheet for solving system of equations where a sequential calculation of the probability ratios is not immediately possible

		lambda	MU1	MU2	MU3	
		0.0001	0.002	0.00166667	0.4	
Iteration #		P1/PFU	P2/PFU	P3/PFU	1/PFU	Lambda system fail
0		0.000E+00	0.000E+00	0.000E+00	1.000E+00	0
1		1.739E-01	2.795E-02	1.397E-05	1.202E+00	1.162E-09
2		1.942E-01	3.420E-02	1.710E-05	1.228E+00	1.392E-09
3		1.987E-01	3.560E-02	1.779E-05	1.234E+00	1.442E-09
4		1.997E-01	3.591E-02	1.795E-05	1.236E+00	1.453E-09
5		1.999E-01	3.598E-02	1.798E-05	1.236E+00	1.455E-09
6		2.000E-01	3.599E-02	1.799E-05	1.236E+00	1.456E-09

SAENORM.COM : Click to view the full PDF of arp4761a

I.4.8 Non-Homogeneous versus Homogeneous MMs

MMs are classified into homogeneous and non-homogeneous based on the probability distributions assumed for the transitions from state to state. One property of all the MM seen so far is the memoryless property—in time and state-space. This corresponds to constant failure and repair rates which also imply the exponential failure or repair probability distributions. Such MM are called “time-homogeneous” where the probability that the system transitions after being in a state at time t in a time interval h to another state is dependent on only the elapsed time interval h and not on the time value t. So, for example, if it is known that a dual-redundant system has operated with both equipment for 100 hours, then the probability it will become a simplex in the next 10 hours is the same as if the system just started operating; the probability that it will become a simplex in the first 10 hours. The knowledge of 100 hours of operation has no impact. This is the memoryless in time property and is a characteristic of time-homogeneous MM as considered so far in this appendix. On the other hand, if the dual equipment can age with time, then the knowledge that the system has operated without any failures for 100 hours or if it just started working will determine the chance the system becomes a simplex in the next 10 hours. Typically, aging distributions such as Weibull are used to describe the equipment failures. In the MM this results in having time-dependent transition rates where the time is from the time when the system is started. The failure probabilities of a system with no repair can be obtained using transient analysis of the MM and computer codes may be necessary to integrate the Kolmogorov equations. Figure I28 shows a two-equipment system with both equipment having same failure rates that are functions of time.

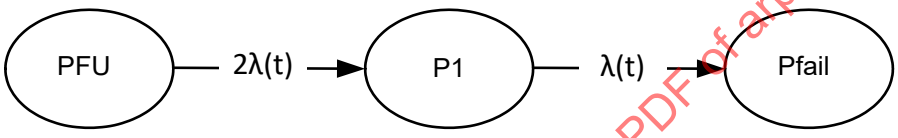


Figure I28 - Non-Homogeneous MM for dual-redundant system with aging equipment

The state probability equations using the flow balance can be written as Equations I109 and I110:

$$\frac{dpfu\,(t)}{dt} = -2\,\lambda\,(t)\,pfu\,(t) \qquad \text{(Eq. I109)}$$

$$\frac{dp_1(t)}{dt} = 2\,\lambda\,(t)\,pfu\,(t) - \lambda\,(t)\,p_1(t) \qquad \text{(Eq. I110)}$$

The third equation can be the conservation equation as before (pFU+p1+pfail=1).

I.4.9 Transient Analysis

Transient analysis is the technique of solving the Kolmogorov state probability equations for different time points where probabilities are of interest. These can be done many different ways depending on if the MM is small or large. Small MMs can be solved by hand using the standard techniques of solving ODEs. These techniques include:

a. Time domain solution using previously tabulated mathematical functions.

b. Laplace transforms or other transforms to convert to frequency domain and then inverting the transforms to time domain.

Other integral equation techniques such as convolution integrals and Volterra integrals. For larger MMs, or even for small MMs, numerical integration of the equations is always possible using standard numerical integration techniques or solvers for ODEs. Observe that the robust techniques consider different arithmetic solutions, such as numerical stiffness, truncation and round-off error control, automatic step size determination, and numerical stability.

SAENORM.COM : Click to view the full PDF of arp4761a

I.4.10 Solution of Markov Chains

The MC solution aims to determine probabilities associated to the system states. These probabilities can then be used to determine other metrics. For instance, the system reliability at time t is given by the sum of the probabilities of being in the operational states in the system at time t. Metrics that require the identification of a time instant (e.g., reliability) require the transient solution of the MC. A steady-state solution of the MC sometimes is required to support other types of metrics (e.g., steady-state availability).

The transient solution of a CTMC with states {1, 2, 3, …, n} determines the probabilities $p_i(t)$ of the system being in state i at time t for all MC states. The solution process proceeds as follows:

Identify the system states and create the state transition diagram to capture the dynamic of system behavior.

Create the initial state probability vector p(0) by attributing the probabilities of being in each state $p_i(0)$ at time 0. For instance, if the states are numbered as shown in Figure I1 from left to right and top to bottom and assume <1,1,1> to be the initial system condition, then:

$$p(0) = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$$

Construct the infinitesimal generator matrix Q. The generator matrix is a square matrix summarizing all admissible state transitions in the system.

$$Q = \begin{bmatrix} q_{11} & q_{12} & q_{13} & \cdots & q_{1n} \\ q_{21} & q_{22} & q_{23} & \cdots & q_{2n} \\ q_{31} & q_{32} & q_{33} & \cdots & q_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ q_{n1} & q_{n2} & q_{n3} & \cdots & q_{nn} \end{bmatrix}$$

The entries q_{ij} ($i \neq j$) in the matrix correspond to the transition label between states i and j in the state transition diagram. For instance, if the states are numbered as shown in in Figure I1 from left to right and top to bottom, then $q_{12} = \lambda_1$ since this is the transition rate between states <1,1,1> and <0,1,1>. The diagonal entries in the generator matrix are calculated by:

$$q_{ii} = -\sum_{j \neq i} q_{ij}$$

and its module represents the rate at which the state is leaving state i.

Solve the system of first-order ODEs:

$$\frac{dp(t)}{dt} = p(t)Q$$

with initial value p(0). The final solution is then given by:

$$p(t) = p(0)e^{Qt} = p(0)\sum_{i=0}^{\infty} \frac{(Qt)^i}{i!}$$

SAENORM.COM : Click to view the full PDF of arp4761a

The steady-state solution of the CTMC aims to determine the state probabilities π_i after the system reaches steady-state, that is:

$$\pi = \lim_{t \to \infty} p(t)$$

If the limiting state probabilities exist then:

$$\lim_{t \to \infty} \frac{dp(t)}{dt} = 0 \Rightarrow \lim_{t \to \infty} [p(t)Q] = 0 \Rightarrow \pi Q = 0$$

Hence, for each state j the result is the linear equation:

$$\sum_{i \neq j} \pi_i q_{ij} - \pi_j \left(\sum_{i \neq j} q_{ji} \right) = 0 \Rightarrow \sum_{i \neq j} \pi_i q_{ij} = \pi_j \left(\sum_{i \neq j} q_{ji} \right)$$

This is also known as the “balance equation” for state j. The semantics comes from the fact that on the left-hand side of the equation, the expected rate of the flows converging into state j from all other states, while on the right-hand side, the expected rate of the flow leaving state j. One nice property of the balance equations is that they can be easily derived directly from the state transition diagram. For instance, the balance equation for state <1,0,1> in Figure I1 is:

$$\pi_1\lambda_2 = \pi_3(\lambda_1 + \lambda_3)$$

This assumes that the system states are numbered as before.

The steady-state CTMC modeling proceeds as follow:

a. Identify system states and create the state transition diagram.

b. Define the initial state probability vector.

c. Construct the infinitesimal generator matrix Q.

d. Solve the system of linear equations $\pi Q = 0$, subject to the condition:

$$\sum_{i=1}^{n} \pi_i = 1$$

SAENORM.COM : Click to view the full PDF of arp4761a

I.4.11 Reliability Metrics (Rates, Probabilities)

It is important to go over some key differences in reliability metrics as it relates to transient analysis of MM and how to interpret the results of such an analysis. Consider an equipment or a system. Suppose the time to failure probability distribution of this equipment or system is denoted by F(t) which is also called the Cumulative Distribution Function. The following lists these metrics, definitions, and their properties and relationships.

I.4.11.1 Failure Distribution Cumulative Distribution Function F(t)

The probability system fails in time t, P(X ≤ t), where X is the life time of system:

- R(t) = 1-F(t) is the reliability function.
- 0 ≤ F(t) ≤ 1.

Example: $F(t) = 1 - e^{-\lambda t}$ for exponential distribution.

I.4.11.2 Failure Density (PDF) f(t)

f(t) = dF(t)/dt

f(t)dt = unconditional probability the system fails in incremental time interval t and t+dt.

f(t) can be > 1.0; tends to go to 0.0 with large t; for small enough t typically, it is linear in t.

Example: $f(t) = \lambda e^{-\lambda t}$ for exponential distribution.

I.4.11.3 Hazard Rate (Instantaneous Failure Rate)

h(t) = f(t)/R(t) ≥ f(t).

h(t)dt = conditional probability the system fails in incremental time interval t and t+dt assuming it is operational at time t = P (t < X <= t+dt | X > t). The condition implies that the system has not failed even once in the interval (0,t). Also observe that the conditional probability is larger than the unconditional probability f(t)dt; therefore h(t) is equal or larger than f(t).

The above metric applies to systems where the system is not repaired from failure. It includes cases where the equipment in the system can be repaired (due to periodic inspection or due to on-board indication), but there is at least one absorbing state in the MM, i.e., the MM is an open-loop MM.

Example: h(t) = λ for exponential distribution which implies a constant hazard rate.

Equipment wear out is modeled by distributions that have an increasing hazard rate with age. For example, using Weibull distribution with a shape factor of β and characteristic life η, the hazard rate is given as:

$$h(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1}$$

which is an unbounded increasing failure fate function of t for β > 1.0.

I.4.11.4 Cumulative Hazard Rate (Cumulative Failure Rate)

$$H(t) = \int_0^t h(s)\,ds = -\ln(R(t))$$

The above metric applies to systems where the system is not repaired from failure. It includes cases where the equipment in the system can be repaired but there is one or more absorbing states in the MM, i.e., the MM is an open-loop MM.

Example: H(t) = λt for exponential distribution which implies a linear accumulation of hazard with time t for any value of t.

SAENORM.COM : Click to view the full PDF of arp4761a

I.4.11.5 Time Averaged Hazard Rate (Average Failure Rate)

$$\bar{h}(t1,t2) = \frac{1}{t2-t1}\int_{t1}^{t2} h(t)dt = \frac{H(t2)-H(t1)}{t2-t1} = \frac{\ln\left(R(t1)\right)-\ln\left(R(t2)\right)}{t2-t1}$$

The above metric applies to systems where the system is not repaired from failure. It includes cases where the equipment in the system can be repaired but there is one or more absorbing states in the MM, i.e., the MM is an open-loop MM.

Example: $\bar{h}(t1,t2) = \lambda$ for exponential distribution and $\bar{h}(0,t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1}$ for Weibull with shape factor β and characteristic life η.

I.4.11.6 Instantaneous Renewal Rate

$$m(t) = \frac{d(E[N(t)])}{dt}$$

It is the time derivative of the average number of system renewals in time t evaluated at time t.

This implies that there is a possibility of complete system renewal in the interval under consideration. Renewal means repair or replacement to perfect working condition of the entire system which is equivalent to having an instantaneous repair from the system failure state to the full-up state in the MM. The renewal equation is:

$$m(t) = f(t) + \int_{o}^{t} m(t-x)f(x)dx$$

It is clear m(t) > f(t) the unconditional failure density because f(t) assumes only one failure is possible while m(t) allows repeated failures and repairs of the system. For small t, m(t) is equal to f(t) which is equal to h(t).

m(t) tends to 1/MTBF of the system for large t. For systems with hazard rate h(t), which is increasing failure rate, this implies that m(t) < h(t) for large t.

I.4.11.7 Average Renewal Rate

$$\bar{m}(t) = \frac{1}{t}\int_{0}^{t} m(s)ds = \frac{E[N(t)]}{t}$$

It is the average number of renewals or replacements of the system in time t divided by t.

Example: m(t) = λ for exponential distribution.

This implies that there is complete system renewal possible in the interval under consideration. Renewal means repair or replacement to perfect working condition of the entire system which is equivalent to having an instantaneous repair from the system failure state to the full-up state in the MM.

The appropriate metric of interest for reliability and safety analysis is the average hazard (failure) rate $\bar{h}(t)$ for systems with no repair from the system failure state and the average renewal rate $\bar{m}(t)$ for systems with repair from the system failure state. The first has units of failures/unit time and the second has units of renewals/unit time. Since for every renewal there is a matched failure that triggers the renewal both measures have failures/unit time. Although they essentially have same units they are two different quantities.

SAENORM.COM : Click to view the full PDF of arp4761a

I.4.11.8 Dual-Redundant System

Consider the two-equipment discrete-repair simulation example considered in I.3.1 and Table I1. In this case, the system is not inspected until 100 hours and failures of both equipment are latent. At 100 hours the system is completely renewed. This is a case where there is no repair until 100-hour period and the system is back to full-up state after 100 hours. The state probabilities are therefore periodic with period of 100 hours. It is clear the system can fail only once in 100 hours. Therefore, the right measure to apply is the average hazard (failure) rate $\bar{h}(t)$. This can be obtained using a numerical integration technique as shown in Table I1. Another way would be to see that the system is a dual-redundant system with identical equipment both equal failure rate of 50E-06. The system fails if both equipment fail. Therefore:

System Unreliability $F(t) = (1 - e^{-\lambda t})^2$

Reliability: $R(t) = 1 - (1 - e^{-\lambda t})^2$

Average failure rate: $$\bar{h}(t) = \frac{-\ln(R(t))}{t} = \frac{-\ln\left(1 - (1 - e^{-\lambda t})^2\right)}{t}$$

Using λ = 50E-06 and t = 100 in the above equation obtains $\bar{h}(100)$ = 2.4876E-07 failures/hour, which is identical to the numerical integration result in Table I1. One also can observe that for small λt, as it is in this case, $\bar{h}(t)$ can be approximated by $\lambda^2 t$ and therefore is linear in t as shown in Figure I8. Also, it is easily shown that $\bar{h}(\infty) = \lambda$, which implies that if this system is operated with no inspection, then after a long time the system will essentially be a simplex one.

Now consider the same dual-redundant system of two identical equipment but where the failure of a single equipment is not indicated in a flight but the system failure (loss of both equipment) is identified because of the resulting loss of function and therefore the system will be fixed within a flight (near instantaneous) after its failure. Suppose the failure rates are the same as before (50E-06) and the impact of an inspection/scheduled maintenance interval for the system is considered. This is a case where the system has the possibility of getting renewed multiple times during the inspection interval depending on the length of the interval. If the interval is too long one encounters the risk of multiple unscheduled failures of the system. On the other hand, if the interval is too short then the cost of schedule maintenance goes up. In this scenario the metric that is the most appropriate is the average renewal rate $\bar{m}(t)$ in an inspection interval.

The average renewal rate can be obtained from a transient analysis of the MM for the system.

The MM for the dual-redundant system with system repair on failure is shown in Figure I29.

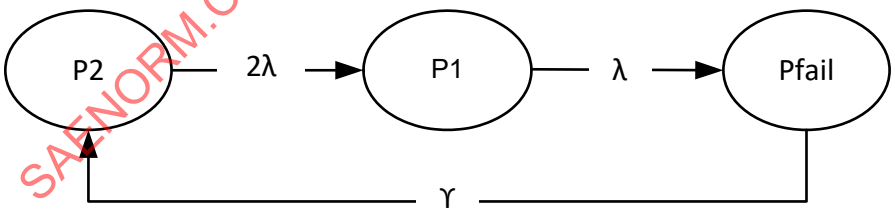


Figure I29 - MM for two-equipment system with no repair to a single equipment failed

The flow into the failure state is P_1*λ. If repair rate γ is taken to be infinite (i.e., the repair is instantaneous), failure state F can be mapped to the starting State 2, yielding the simpler MC, Figure I30.

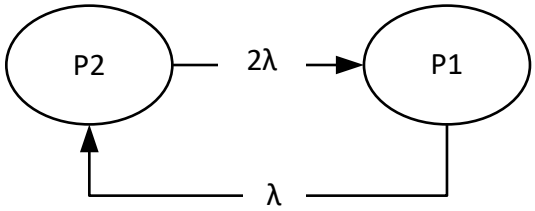


Figure I30 - Two-equipment MM with instantaneous return to fully failed state

SAENORM.COM : Click to view the full PDF of arp4761a

The state probability equations for this MM are:

$$\frac{dp_1(t)}{dt} = -\lambda p_1(t) + 2\lambda p_2(t) \quad \text{(Eq. I111)}$$

Using the conservation equation p1 + p2 = 1.0, results in p2 = 1 - p1 and substituting for p2 in the differential Equation I111 to obtain Equation I112.

$$\frac{dp_1(t)}{dt} = -\lambda p_1(t) + 2\lambda(1 - p_1(t)) = -3\lambda p_1(t) + 2\lambda \quad \text{(Eq. I112)}$$

The solution to this one variable simple ODE can be obtained easily as:

$$p_1(t) = \frac{2}{3}(1 - e^{-3\lambda t}) \quad \text{(Eq. I113)}$$

The instantaneous renewal rate is:

$$m(t) = \lambda * p_1(t) = \frac{2\lambda}{3}(1 - e^{-3\lambda t}) \quad \text{(Eq. I114)}$$

The average renewal rate is:

$$\bar{m}(t) = \frac{1}{t}\int_0^t m(s)ds = \frac{2\lambda}{3t}\int_0^t (1 - e^{-3\lambda s})ds = \frac{2\lambda}{3}\left[1 - \frac{1 - e^{-3\lambda t}}{3\lambda t}\right] \quad \text{(Eq. I115)}$$

Observe that $m(\infty) = \frac{2\lambda}{3}$, which is the inverse of the MTBF of the dual-redundant system, is as highlighted before. Also, it can be derived from the above expression for $\bar{m}(t)$ that $\bar{m}(\infty) = \frac{2\lambda}{3}$. This is the steady-state value for the system average renewal rate. Figure I31 shows the ratio of the average renewal rate to its steady-state value. It shows that the transient solution attains steady-state value of $\frac{2\lambda}{3}$ to within 5% if λt > 10. For λ = 50E-06 if the scheduled inspection interval is greater than 200000 hours then the steady-state solution can be used.

SAENORM.COM : Click to view the full PDF of arp4761a

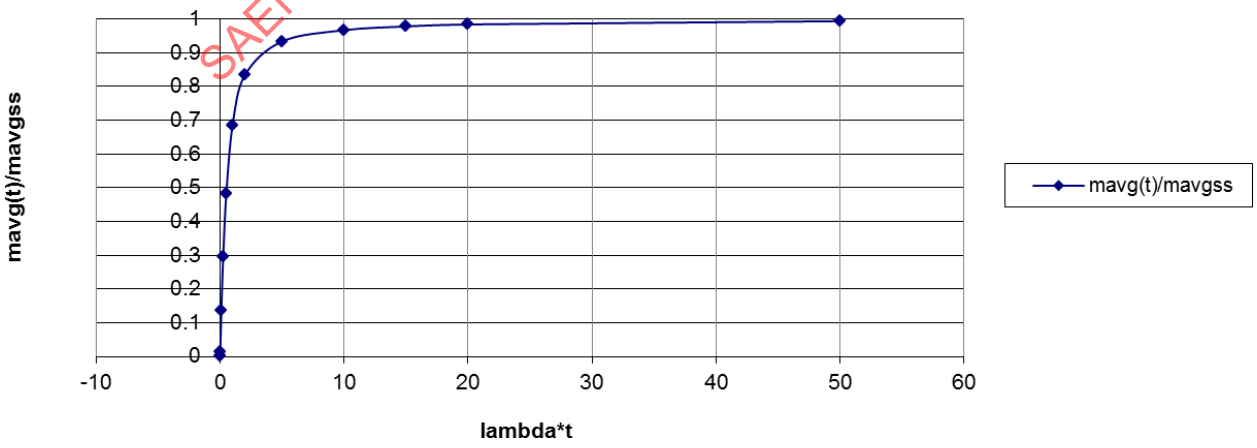


Figure I31 - Ratio of average renewal rate to the steady-state renewal rate at t = ∞

For λ = 50E-6, the Figure I32 chart compares the average failure rate and the average renewal rate. It is seen that the renewal rate is lower than the failure rate and both attain steady-state with different values. Both are nonlinear and monotonically increasing functions. It is interesting that m̄(100) = 2.487547E-07 renewals/hour, which is very close to h̄(100) = 2.4876E-07 failures/hour. Thus, it does not make much difference for small t whether one uses the hazard rate or the renewal rate.

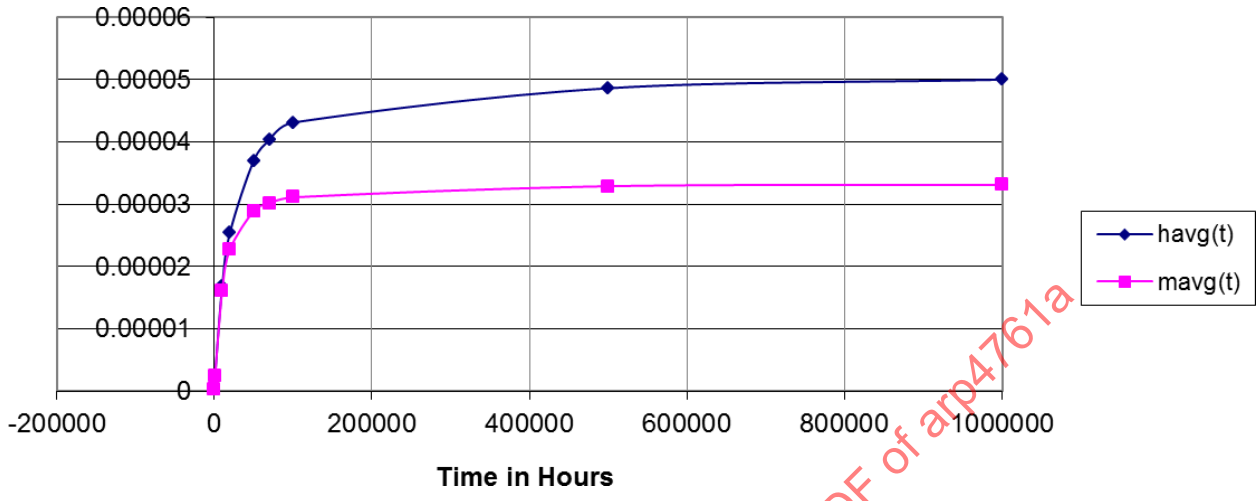


Figure I32 - Average hazard rate and renewal rates as a function of time

I.4.11.9 Triple Redundant System

Now consider a triple redundant system with identical equipment where none of the equipment are inspected. Assume a constant failure rate of λ for the three-equipment. Like before for the dual system assume that the loss of function due to system failure will be detected which will trigger a system renewal where all three-equipment are restored to full working condition almost instantaneously within a flight. The loss of one or two equipment is latent and is not detected.

The MM for this case is shown in Figure I33.

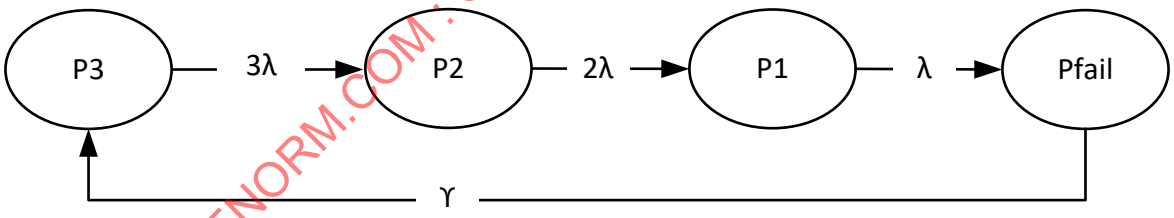


Figure I33 - Three-equipment System with no repair until all equipment failed

The flow into the failure state is P1*λ. If repair rate γ is taken to be infinite, i.e., the repair is instantaneous, failure state F can be mapped to the starting state 3, yielding the simpler MC (Figure I34):

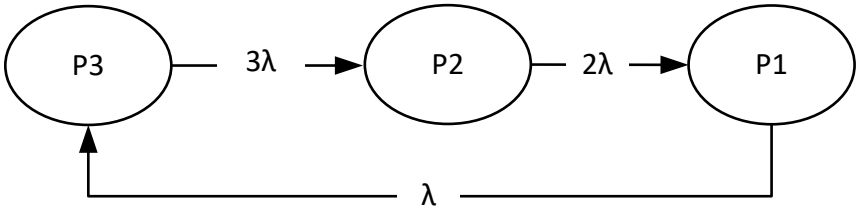


Figure I34 - MM for three-equipment system with instantaneous repair

SAENORM.COM : Click to view the full PDF of arp4761a

The state probability equations for the Figure I34 MM are:

$$\frac{dp_1(t)}{dt} = -\lambda p_1(t) + 2\lambda p_2(t) \quad \text{(Eq. I116)}$$

$$\frac{dp_2(t)}{dt} = -2\lambda p_2(t) + 3\lambda p_3(t) \quad \text{(Eq. I117)}$$

Using the conservation equation p1 + p2 + p3 = 1.0, results in p3 = 1-p1 -p2 and substituting for p3 in the differential equation above to obtain Equation I118.

$$\frac{dp_1(t)}{dt} = -\lambda p_1(t) + 2\lambda p_2(t) \quad \text{(Eq. I118)}$$

$$\frac{dp_2(t)}{dt} = -3\lambda p_1(t) - 5\lambda p_2(t) + 3\lambda \quad \text{(Eq. I119)}$$

The above is a simultaneous set of two coupled ODEs. To solve it the analyst may use many techniques. The Laplace transform technique is used herein to transform the ODE into a system of algebraic equations. Laplace transform of a time dependent function f(t) is defined as:

$$L_f(s) = \int_0^\infty e^{-st} f(t)dt$$

Observe that the Laplace transform will exist depending on the function f (t) and some functions may not have a transform. One useful property of Laplace transforms is the relationship that the transform of the time derivative of a function has with respect to the transform of the function. Thus, if g(t) = df(t)/dt, then:

$$L_g(s) = \int_0^\infty e^{-st} \frac{df(t)}{dt} dt = sL_f(s)$$

Applying the Laplace transform on the ODEs, the following algebraic equations in the s-domain are obtained.

$$sL_{p_1}(s) = -\lambda L_{p_1}(s) + 2\lambda L_{p_2}(s)$$

$$sL_{p_2}(s) = -3\lambda L_{p_1}(s) - 5\lambda L_{p_2}(s) + \frac{3\lambda}{s}$$

Solving for $L_{p_1}(s)$ from the algebraic set of equations to obtain:

$$L_{p_1}(s) = \frac{6\lambda^2}{s\left[(s+\lambda)(s+5\lambda)+6\lambda^2\right]}$$

SAENORM.COM : Click to view the full PDF of arp4761a

Inverting the transform for $L_{p_1}(s)$ is the next step to get back $p_1(t)$ from above. This can be done by the method of partial fraction expansion. The result for the renewal rate is obtained then as:

$$m(t) = \lambda * p_1(t) = \frac{6\lambda}{11}\left[1 - e^{-3\lambda t}\left(\cos\sqrt{2}\lambda t + \frac{3}{\sqrt{2}}\sin\sqrt{2}\lambda t\right)\right] \quad \text{(Eq. I120)}$$

The average renewal rate is then:

$$\bar{m}(t) = \frac{1}{t}\int_0^t m(s)ds = \frac{6\lambda}{11}\left[1 - \frac{6}{11\lambda t} + \frac{e^{-3\lambda t}}{11\sqrt{2}\lambda t}\left\{7\sin\left(\sqrt{2}\lambda t\right) + 6\sqrt{2}\cos\left(\sqrt{2}\lambda t\right)\right\}\right] \quad \text{(Eq. I121)}$$

The chart in Figure I35 plots the average renewal rate scaled with its steady-state value of 6λ/11. It shows that the transient solution attains steady-state value of 6λ/11 to within 5% if λt > 15.

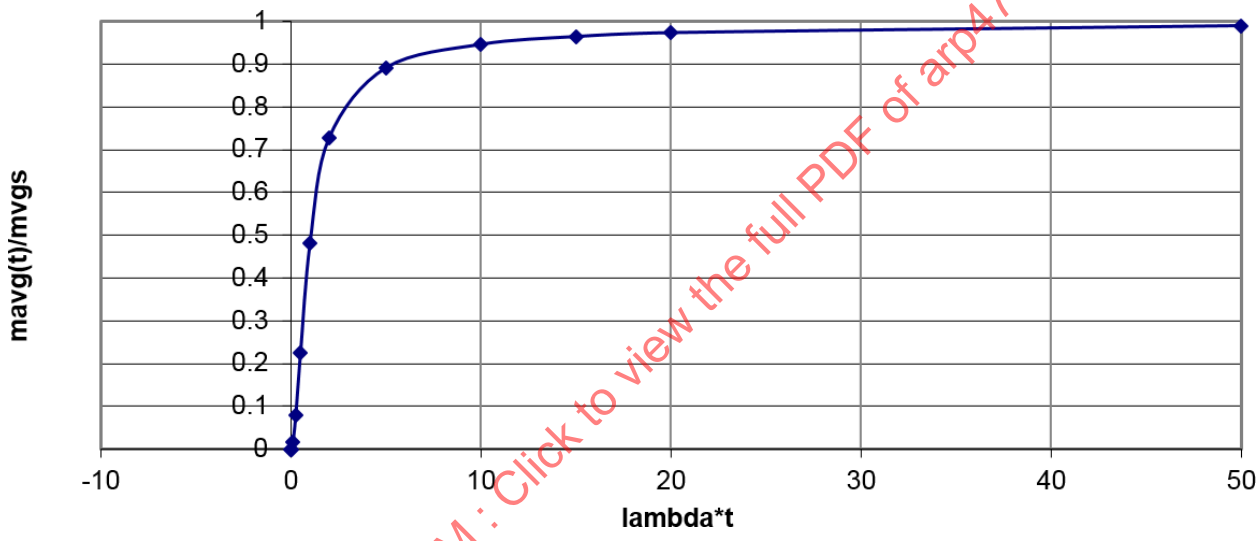


Figure I35 - Ratio of average renewal rate at time t to average renewal rate at t = ∞

For λ = 50E-06, if the scheduled inspection interval is greater than 300000 hours, then the steady-state solution can be used.

I.4.11.10 System with Aging Equipment

We now consider the dual-redundant system with no repair with equipment whose failure rates are not constant, i.e., they can increase with age. The MM for this system was shown in Figure I28. It was earlier mentioned that the MM is a non-homogeneous MM. Transient analysis can be done by use of numerical integration or convolution integral type analytical approaches. The state equations are shown below.

$$\frac{dp_2(t)}{dt} = -2\lambda(t)p_2(t)$$

$$\frac{dp_1(t)}{dt} = 2\lambda(t)p_2(t) - \lambda(t)p_1(t)$$

SAENORM.COM : Click to view the full PDF of arp4761a

If a Weibull type wear out distribution (shape = β, characteristic life = η) for the equipment is assumed with $\lambda(t) = \lambda\beta\, t^{\beta-1}$, where $\lambda = \frac{1}{\eta^{\beta}}$ and that the system starts in the full-up state is assumed, i.e., $p_2(0) = 1$, then integrating the first equation obtains:

$$p_2(t) = e^{\int_0^t -2\lambda\beta x^{\beta-1} dx} = e^{-2\lambda t^{\beta}}$$

This can also be obtained by noting that $p_2(t)$ is the probability that both equipment are operational of the dual equipment system with one equipment having the reliability of:

$$R(t) = e^{-\lambda t^{\beta}}$$

and thus:

$$p_2(t) = R^2(t) = (e^{-\lambda t^{\beta}})^2$$

The probability $p_1(t)$ can be obtained by integrating the second differential equation:

$$p_1(t) = \int_0^t \Psi(t,x) 2\lambda(x) p_2(x) dx = \int_0^t \Psi(t,x) 2\lambda\beta x^{\beta-1} e^{-2\lambda x^{\beta}} dx$$

where the kernel is:

$$\Psi(t,x) = e^{\int_x^t -\lambda(\tau) d\tau} = e^{\int_x^t -\lambda\beta\tau^{\beta-1} d\tau} = e^{-\lambda t^{\beta}} e^{\lambda x^{\beta}}$$

In this case, the kernel is separable in x and t which makes it simple to integrate $p_1(t)$. Substituting for the kernel in the integral for $p_1(t)$ to obtain:

$$p_1(t) = \int_0^t \Psi(t,x) 2\lambda(x) p_2(x) dx = \int_0^t e^{-\lambda t^{\beta}} e^{\lambda x^{\beta}} 2\lambda\beta x^{\beta-1} e^{-2\lambda x^{\beta}} dx = -2e^{-\lambda t^{\beta}} \int_0^t d\left(e^{-\lambda x^{\beta}} \right) = 2e^{-\lambda t^{\beta}} (1 - e^{-\lambda t^{\beta}})$$

This result can also be obtained by noting that $p_1(t)$ is the probability one out of two equipment is working and there are two possible ways this can happen and for each possibility the probability is the product of the reliability of one equipment and the unreliability of the other.

The example illustrates the complexity in the analytical methods to obtain transient solutions for aging systems. Numerical integration methods are relatively simpler but they are still more complex than those needed for time-homogeneous MM. A simple approach to numerical integration would use the rectangular rule as shown:

SAENORM.COM : Click to view the full PDF of arp4761a

$$\frac{p_2(t+h)-p_2(t)}{h} = -2\lambda\beta t^{\beta-1} p_2(t)$$

$$\frac{p_1(t+h)-p_1(t)}{h} = 2\lambda\beta t^{\beta-1} p_2(t) - \lambda\beta t^{\beta-1} p_1(t)$$

where h is a suitably chosen small numerical integration time step. The integration is started with p2(0) = 1.0 and p1(0) = 0.0. The following spreadsheet shows the system simulation using β=2.0, η=1000 hours (MTTF=886.22 hours) and h= 1.0 up to a time of 100 hours.

Table I9 - Probabilities for being in states of operation of a two-equipment system where each equipment has Weibull failure distribution with shape beta of 2.0 and a characteristic life eta (η) of 1000 hours

Beta	2		
MTTF	886.22		
h	1		
Time	p1	p2	pf = 1 - p1 - p2
0.00	0.00000E+00	1.00000E+00	0.00000E+00
1.00	0.00000E+00	1.00000E+00	0.00000E+00
2.00	4.00000E-06	9.99996E-01	0.00000E+00
3.00	1.20000E-05	9.99988E-01	1.60001E-11
4.00	2.39997E-05	9.99976E-01	8.79998E-11
5.00	3.99992E-05	9.99960E-01	2.79998E-10
6.00	5.99980E-05	9.99940E-01	6.79989E-10
7.00	8.39958E-05	9.99916E-01	1.39996E-09
8.00	1.11992E-04	9.99888E-01	2.57591E-09
9.00	1.43987E-04	9.99856E-01	4.36778E-09
10.00	1.79979E-04	9.99820E-01	6.95955E-09
11.00	2.19968E-04	9.99780E-01	1.05591E-08
12.00	2.63954E-04	9.99736E-01	1.53984E-08
13.00	3.11935E-04	9.99688E-01	2.17333E-08
14.00	3.63910E-04	9.99636E-01	2.98436E-08
15.00	4.19880E-04	9.99580E-01	4.00331E-08
16.00	4.79842E-04	9.99520E-01	5.26295E-08
17.00	5.43796E-04	9.99456E-01	6.79845E-08
18.00	6.11741E-04	9.99388E-01	8.64735E-08
19.00	6.83674E-04	9.99316E-01	1.08496E-07
20.00	7.59597E-04	9.99240E-01	1.34476E-07
21.00	8.39505E-04	9.99160E-01	1.64860E-07
22.00	9.23400E-04	9.99076E-01	2.00119E-07
23.00	1.01128E-03	9.98988E-01	2.40748E-07
24.00	1.10314E-03	9.98897E-01	2.87267E-07
25.00	1.19898E-03	9.98801E-01	3.40218E-07
26.00	1.29880E-03	9.98701E-01	4.00167E-07
27.00	1.40260E-03	9.98597E-01	4.67704E-07
28.00	1.51037E-03	9.98489E-01	5.43445E-07
29.00	1.62212E-03	9.98377E-01	6.28025E-07
30.00	1.73783E-03	9.98261E-01	7.22108E-07
31.00	1.85752E-03	9.98142E-01	8.26378E-07
32.00	1.98117E-03	9.98018E-01	9.41544E-07
33.00	2.10879E-03	9.97890E-01	1.06834E-06
34.00	2.24038E-03	9.97758E-01	1.20752E-06

SAENORM.COM : Click to view the full PDF of arp4761a

Beta	2		
MTTF	886.22		
h	1		
Time	p1	p2	pf = 1 - p1 - p2
35.00	2.37592E-03	9.97623E-01	1.35987E-06
36.00	2.51542E-03	9.97483E-01	1.52618E-06
37.00	2.65888E-03	9.97339E-01	1.70729E-06
38.00	2.80629E-03	9.97192E-01	1.90405E-06
39.00	2.95765E-03	9.97040E-01	2.11732E-06
40.00	3.11295E-03	9.96885E-01	2.34802E-06
41.00	3.27221E-03	9.96725E-01	2.59706E-06
42.00	3.43540E-03	9.96562E-01	2.86538E-06
43.00	3.60253E-03	9.96394E-01	3.15395E-06
44.00	3.77360E-03	9.96223E-01	3.46377E-06
45.00	3.94861E-03	9.96048E-01	3.79585E-06
46.00	4.12754E-03	9.95868E-01	4.15122E-06
47.00	4.31040E-03	9.95685E-01	4.53096E-06
48.00	4.49718E-03	9.95498E-01	4.93613E-06
49.00	4.68789E-03	9.95307E-01	5.36786E-06
50.00	4.88251E-03	9.95112E-01	5.82728E-06
51.00	5.08104E-03	9.94913E-01	6.31553E-06
52.00	5.28349E-03	9.94710E-01	6.83379E-06
53.00	5.48984E-03	9.94503E-01	7.38328E-06
54.00	5.70009E-03	9.94292E-01	7.96520E-06
55.00	5.91424E-03	9.94077E-01	8.58081E-06
56.00	6.13229E-03	9.93858E-01	9.23138E-06
57.00	6.35423E-03	9.93636E-01	9.91819E-06
58.00	6.58005E-03	9.93409E-01	1.06426E-05
59.00	6.80976E-03	9.93179E-01	1.14059E-05
60.00	7.04334E-03	9.92944E-01	1.22094E-05
61.00	7.28081E-03	9.92706E-01	1.30546E-05
62.00	7.52214E-03	9.92464E-01	1.39429E-05
63.00	7.76734E-03	9.92218E-01	1.48756E-05
64.00	8.01640E-03	9.91968E-01	1.58543E-05
65.00	8.26931E-03	9.91714E-01	1.68804E-05
66.00	8.52608E-03	9.91456E-01	1.79554E-05
67.00	8.78670E-03	9.91194E-01	1.90809E-05
68.00	9.05117E-03	9.90929E-01	2.02583E-05
69.00	9.31947E-03	9.90659E-01	2.14892E-05
70.00	9.59160E-03	9.90386E-01	2.27753E-05
71.00	9.86757E-03	9.90108E-01	2.41181E-05
72.00	1.01474E-02	9.89827E-01	2.55193E-05
73.00	1.04310E-02	9.89542E-01	2.69806E-05
74.00	1.07184E-02	9.89253E-01	2.85035E-05
75.00	1.10096E-02	9.88960E-01	3.00898E-05
76.00	1.13047E-02	9.88664E-01	3.17412E-05
77.00	1.16035E-02	9.88363E-01	3.34595E-05
78.00	1.19061E-02	9.88059E-01	3.52465E-05
79.00	1.22125E-02	9.87750E-01	3.71038E-05
80.00	1.25227E-02	9.87438E-01	3.90334E-05
81.00	1.28367E-02	9.87122E-01	4.10371E-05
82.00	1.31545E-02	9.86802E-01	4.31166E-05

SAENORM.COM : Click to view the full PDF of arp4761a

Beta	2		
MTTF	886.22		
h	1		
Time	p1	p2	pf = 1 - p1 - p2
83.00	1.34760E-02	9.86479E-01	4.52739E-05
84.00	1.38013E-02	9.86151E-01	4.75110E-05
85.00	1.41303E-02	9.85820E-01	4.98296E-05
86.00	1.44631E-02	9.85485E-01	5.22317E-05
87.00	1.47996E-02	9.85146E-01	5.47194E-05
88.00	1.51398E-02	9.84803E-01	5.72945E-05
89.00	1.54838E-02	9.84456E-01	5.99591E-05
90.00	1.58315E-02	9.84106E-01	6.27152E-05
91.00	1.61830E-02	9.83751E-01	6.55649E-05
92.00	1.65381E-02	9.83393E-01	6.85102E-05
93.00	1.68969E-02	9.83032E-01	7.15532E-05
94.00	1.72595E-02	9.82666E-01	7.46960E-05
95.00	1.76257E-02	9.82296E-01	7.79408E-05
96.00	1.79956E-02	9.81923E-01	8.12897E-05
97.00	1.83693E-02	9.81546E-01	8.47449E-05
98.00	1.87465E-02	9.81165E-01	8.83085E-05
99.00	1.91275E-02	9.80781E-01	9.19828E-05
100.00	1.95121E-02	9.80392E-01	9.57701E-05

The final values are slightly different than if p2(100) = $R^2(100) = (e^{-(1E-06)(100)^2})^2$ were used, but the numerical integration can be made more accurate by choosing a smaller value for h.

I.4.11.11 Phased Mission System

Consider a system of two equipment which operates in two distinct mission phases. Suppose in the first phase of the mission both equipment are necessary for the system to perform its function and in the second phase only one is necessary. Also assume that once the system fails to function in the first phase then it is considered failed for the complete mission and cannot be used in the second phase even though only one equipment failed in the first phase. Suppose the operating time for first phase is T_1 and the second phase is T_2. Let the failure rate of the equipment in both phases be identical and equal λ.

The MM for the first phase is shown in Figure I36:

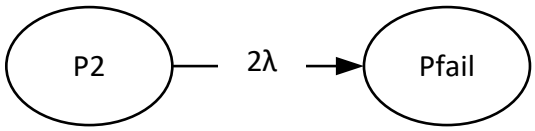


Figure I36 - Two-equipment system for first phase where either equipment failed yields system failure

The MM for the second phase is shown in Figure I37:

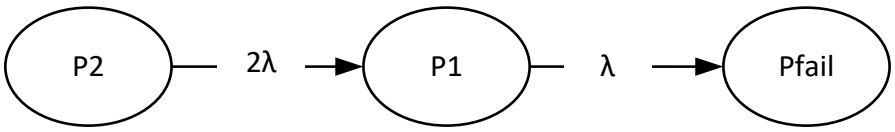


Figure I37 - Two-equipment system for second phase

SAENORM.COM : Click to view the full PDF of arp4761a

The system starts in the full-up state (state 2) in phase 1, i.e., $p_2(0) = 1.0$. The state probability equation for phase 1 MM is:

$$\frac{dp_2(t)}{dt} = -2\lambda p_2(t) \quad \text{(Eq. I122)}$$

This yields $p2(t) = e^{-2\lambda t}$. At the end of the first phase, $p2(T_1) = e^{-2\lambda T_1}$. This is the probability of system still being operational at the end of first phase. The system failure probability in first phase is then $p_F(t) = 1 - e^{-2\lambda t}$.

For the second phase the state probability equations are:

$$\frac{dp_2(t)}{dt} = -2\lambda p_2(t) \quad \text{(Eq. I123)}$$

$$\frac{dp_1(t)}{dt} = -\lambda p_1(t) + 2\lambda p_2(t) \quad \text{(Eq. I124)}$$

The initial condition for second phase is the final condition for first phase. Thus $p2(0) = e^{-2\lambda T_1}$.

This yields $p2(t) = e^{-2\lambda t} p2(0) = e^{-2\lambda t} e^{-2\lambda T_1}$. Similarly, p1(t) is obtained from the second differential equation as follows:

$$p1(t) = \int_0^t e^{-\lambda(t-x)} 2\lambda\, e^{-2\lambda x} e^{-2\lambda T_1} dx = 2e^{-\lambda t}(1 - e^{-\lambda t}) e^{-2\lambda T_1}$$

At the end of phase two: $p2(T_2) = e^{-2\lambda T_2} e^{-2\lambda T_1}$ and $p1(T_2) = 2e^{-2\lambda T_2}(1 - e^{-2\lambda T_2}) e^{-2\lambda T_1}$.

The probability that the system fails in second phase is $p_F(T_2) = e^{-2\lambda T_1} - p2(T_2) - p_1(T_2)$. This is the probability that the system fails exclusively in second phase. For Cumulative Distribution Function of system life, one will add the failure probability in first phase to this value. Thus, if X represents system life then:

$$\Pr ob(X <= t) = \begin{cases} (1 - e^{-2\lambda t}); & 0 \le t \le T_1 \\ \left(1 - e^{-2\lambda T_1}\right) + \left(e^{-2\lambda T_1} - e^{-2\lambda (t-T_1)} e^{-2\lambda T_1} - 2e^{-\lambda (t-T_1)}(1 - e^{-\lambda (t-T_1)}) e^{-2\lambda T_1}\right); & T_1 \le t \le T_1 + T_2 \end{cases}$$

I.5 ANALYSIS TOOLS

Software tools are available to assist some or all the steps in the transient or steady-state solution of CTMCs. Markov modeling tools automate various steps, freeing the analyst to concentrate in the design aspects of the MM. The expected input to these tools is just the initial state probability vector and definition of state transitions, which is usually done in a textual form of the type (source state, destination state, transition rate). Some Markov modeling tools also provide a specialized graphical user interface (GUI) to allow for the easy construction of state transition diagrams which then replaces the textual input of transition rates. Apart from the transparent solution of the system of ODEs and linear equations, the Markov modeling tools also incorporate special numerical solution engines to cope with stiffness problems commonly associated to the transient analysis of reliability models where transition rates can differ in several orders of magnitude. Due to its inherent nature, Markov modeling tools can provide basic model verification such as: guaranteeing that probabilities and transition rates are within the expected ranges, confirming that probabilities in the initial state probability vector add up to one and that the row sums of the matrix Q are equal to zero, preventing self-loop transitions in CTMCs, etc.

SAENORM.COM : Click to view the full PDF of arp4761a

I.5.1 Spreadsheet Calculations

Several examples of spreadsheet calculations are contained in this appendix. Spreadsheets are particularly easy to use for problems that are not too complex, and especially those where the calculations can be computed sequentially, as shown in the first example in I.4.7. The advantage (or disadvantage, depending on your viewpoint) of using spreadsheet calculations is that the user has to put in the equations for the computations. This can help the user get a feel for the various state probabilities and failure rates. The disadvantage, of course, is that this generally requires more effort as compared to using a solution program.

I.6 SUMMARY

The use of an MM to estimate the average failure rate of a system is quite straight forward. The differential equations representing the system are readily assembled. The big advantage of MMs is that repair rates can be easily simulated and included in the model. The solving of an MM of a system yields the probabilities of being in the various failure states of the system, along with the failure rates into those states.

One of the significant difficulties found in the various publications and papers describing the use of MMs is that there is little information on how to simulate repairs. An accurate and representative modeling of repairs is much less understood than the modeling of failures, and the correct modeling of repairs, from intermediate failure states, can have a very significant impact on the failure rate of the system.

Many of the redundant elements in aircraft systems involve electronic or other elements that have constant failure rates. In these systems the modeling of failures is done using transitions from one system state to another with a constant (failure) rate. The analyst tends to implicitly understand this. So, even though failures occur as random, discrete events in-service, the analyst appears to understand the use of a continuous transition path in an MM to represent these failures. In-service, repairs are similar to failures in that they are completed as discrete events. However, unlike failures, the analyst tends to believe that repairs should be modeled as discrete events. In doing this, the analyst wants to “stop the model” at a given point in time, and reset the probabilities of being in the various failure states to simulate the repair scenario that is occurring in-service.

Simulating discrete repairs makes the solution of an MM much more tedious, as a time history calculation of the probabilities of being in the various failure states has to be made and the average system failure rate calculated from the data in that time history. As explained in this appendix, a continuous repair path can always be used to model a discrete repair action, just as a continuous failure path is used to represent a discrete failure. There are two types of repair actions used in-service. The first is called “time since fault” or “on-condition” repair. In this repair scenario, the time of the fault is known, and the repair is scheduled to occur within a given time following the failure. The second repair scenario is herein called “periodic inspection and repair.” In this scenario, the time of occurrence is not known, but the system is periodically inspected for a fault/failure. If a fault is found at inspection, the repair requirement may be immediate, or within a given number of operating hours. How to use a continuous repair path to represent both of these different repair scenarios is discussed herein.

In addition, it is pointed out that when continuous repair paths are used to represent the two different discrete repair scenarios, and a continuous feedback (i.e., repair) path is used to return the system from the fully failed state to the full-up state, the MM reduces to a steady-state model of algebraic equations, rather than a system of first order differential equations. These equations allow the overall average system failure rate to be directly determined—without having to analyze a time history of the probabilities of being in the various failure states—by simply solving the algebraic equations. As the examples herein show, this makes the task of determining/calculating the steady-state, fleet average failure rate of a system substantially easier. An MM with a feedback path from the fully failed state to the full-up state is herein called a “closed-loop” model.

Data and calculations for all of the examples contained herein have been included so that the reader might more easily understand what is being explained and how the models are assembled and analyzed, so that the analyst may be able to more readily apply the MM analysis method to their problem.

SAENORM.COM : Click to view the full PDF of arp4761a

Many analysts believe that if you are constructing an MM to analyze a system whose failure leads to a Hazardous or Catastrophic event, that the model has to be extremely “complete,” or the result would not be accurate. As pointed out herein, and particularly in ARP5107C, this is not the case at all. If the system is a redundant one, and the first (or single) failure states are repaired reasonably quickly following the fault/failure, the higher order, multiple event/multiple failure states need not be modeled to have an accurate overall model. Because when the first failure states are repaired reasonably quickly, the probability of being in a multiple condition failure state decreases very quickly, and those higher order states add little to the answer. Hence, they can usually be disregarded with little loss in accuracy.

Lastly, phased mission analyses, where the actual configuration of a system, in terms of what operative equipment are needed to complete that phase, are discussed. See the example in I.4.22 for an illustration of such an analysis.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX J - FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

J.1 INTRODUCTION 243

J.2 SCOPE 243

J.3 FMEA PROCESS 243
J.3.1 FMEA Preparation 243
J.3.2 Performing the Analysis 244

J.4 DOCUMENTATION 251
J.4.1 FMEA Report 251
J.4.2 FMES Report 252
J.4.3 FMEA/FMES Checklist 255

Figure J1 Example of FMEA to FMES relationship 252

Table J1 Example Functional FMEA worksheet 247
Table J2 Example piece-part FMEA worksheet 249
Table J3 Example FMES worksheet 254

SAENORM.COM : Click to view the full PDF of arp4761a

J.1 INTRODUCTION

A Failure Modes and Effects Analysis (FMEA) is a bottom-up, systematic method for identifying failure modes and failure effects. An FMEA may be initiated at any indenture level; system, product, function, equipment, or part. An FMEA may be either quantitative or qualitative and may be performed on all types of systems (e.g., electrical, electronic, or mechanical systems).

An FMEA may be performed for reasons other than to support safety analyses. This appendix addresses FMEAs used to support the safety assessment process.

FMEA results are tabulated in worksheets enumerating the failure modes and failure effects determined, failure detection methods discovered, if any, and failure rates associated with the failure mode if a quantitative analysis is being performed.

FMEA effects that are common may be used to generate a Failure Modes and Effects Summary (FMES). The FMES may then be used to support the other analysis techniques of the System Safety Assessment (SSA) process such as Fault Tree Analysis (FTA), Dependence Diagram (DD), Markov Analysis (MA), or Model-Based Safety Analysis (MBSA). In the context of this appendix where FTA is identified, references to the other analysis techniques is implied.

Combinations of failures are not considered as part of the FMEA.

J.2 SCOPE

An FMEA is performed at a given level (e.g., system, equipment), by postulating the ways the chosen level's specific implementation may fail. The effects of a single failure mode are determined and described at the given level and usually for the next higher level considering each operating mode of the equipment. Sometimes an FMEA may be focused towards a specific operating scenario as required to support a top-down safety analysis such as FTA.

The FMEA should be performed at the level which will provide the requested goals and expectations. In cases where it is not possible to identify the specific nature of a failure mode, the worst-case effect must be assumed. If the worst-case effect is unacceptable for the fault tree, the failure modes may be re-examined at the next lower indenture level. For example, if the FMEA is being conducted at the functional level, re-examine at the piece-part level and exclude parts with no effect on the event under consideration. If the analysis is being conducted at a Piece-Part FMEA level, it may be possible to consider specific output failure mechanisms of the parts.

Regardless of the level at which the FMEA is to be performed, the major steps of an FMEA include preparation, analysis, and documentation.

J.3 FMEA PROCESS

J.3.1 FMEA Preparation

The preparation of an FMEA includes determining the requestor's goals for the FMEA, obtaining current documentation, and understanding the operation of the function at the indenture level being analyzed.

An FMEA has applications in addition to supporting the safety assessment. It is important to know the goals and expectations for the FMEA before beginning the analysis. If the FMEA expectations are not known, the FMEA may not meet the needs of the requestor and may have to be re-done.

Goals and expectations for an FMEA usually originate from a safety assessment activity such as an FTA. The analyst needs to know the analysis level if specified (e.g., functional versus piece-part), safety-related effects, other failure effects, and operational modes of interest. The depth of the analysis, if not provided, may be determined by what failure rates are required to meet the safety objectives for the FTA or by the need for single failure effect identification. An FMEA is used to support the safety assessment process by providing failure rates in support of the basic events of the FTA. It is important for the FMEA to consider the use of the failure mode information in the FTA in order to optimize failure rate application to the FTA basic events.

SAENORM.COM : Click to view the full PDF of arp4761a

However, an FMEA may also be used to support verification of the FTA through a comparison of the FMEA failure modes with the basic events of the fault tree. Care should be taken in this comparison, however, since the FTA top-down analysis structure may contain architectural mitigations at levels above the FMEA evaluation. The FMEA described herein (or FMES, as discussed in J.4.2) does not consider these architecture factors and may result in a more pessimistic effect description. An FMEA/FMES which considers the architectural factors (multiple failure combinations) will generate erroneous basic event failure rates and mask detection methods.

The final step before performing the FMEA is to obtain the following information (or create if unavailable) which may be necessary to complete the analysis, or may simplify the analysis activity.

a. FMEA goals and expectations, including safety-related and requested failure effects and specific operating modes of interest.

b. Specifications (i.e., requirements).

c. Implementation definitions (e.g., current drawings, schematics).

d. Parts lists for each system, function or equipment.

e. Functional block diagrams.

f. Explanatory materials including the theory of operation.

g. An applicable list of failure rates (J.3.2).

h. The FMEA on the previous generation of equipment, equipment with a similar function or a list of failure modes from previous FMEAs, if available.

i. Any design changes and revisions that have not yet been included on the schematic. (Note that designs may change frequently and having the most up-to-date material will reduce FMEA updates).

j. Preliminary list of part failure modes from previous FMEAs, if applicable.

k. Failure mode detection mechanisms (e.g., electronic hardware or software monitors).

For FMEAs performed early in the design stage, some of the above information will not be available and assumptions or estimates may have to be made. Detailed documentation of these assumptions should be maintained for traceability and to simplify future updates. As new information becomes available during development, FMEAs should be updated and documented accordingly.

SAENORM.COM : Click to view the full PDF of arp4761a

J.3.2 Performing the Analysis

The analyst needs to review and understand the information gathered during the preparation stage previously described. The analyst will also find it useful to understand the functions that the design being analyzed performs within the next higher level. After the analyst has gained sufficient knowledge, failure modes are identified. Every feasible failure mode is postulated at the level of the design being analyzed. Consideration is given to failure modes of the parts or functions that make up the given level. Information to aid in determining the failure modes of the functions or parts is provided in J.3.2.1 and J.3.2.2.

Every identified failure mode is analyzed to determine its effect on the given level. The effect on higher levels may also be captured with detection or mitigation mechanisms described, as appropriate. Failure effect categories are created for each different type of effect and a code may be assigned to each effect category. Defining these codes will simplify the FMEA worksheet by moving the description of each effect from the worksheet to the body of the report.

The FMEA worksheet provides a list of failure modes, effects and rates. Examples of FMEA worksheets are provided in J.3.2.1 and J.3.2.2. Each effect category should have only one higher-level effect; otherwise, the effect categories should be defined in more detail. For example, if the effect category is originally defined as “causes signal xyz to be out of specification” but an out of specification high condition causes a different effect from an out of specification low condition, then the effect category should be split to “... out of specification high” and “... out of specification low.” Similarly, if the failure mode is found to cause two higher-level effects (e.g., “Loss of signal A” and “Loss of signal B”), then these two should be combined to form a new effect category “Loss of both signals A and B.”

The means by which the failure is detected is usually determined and documented within the FMEA worksheets. Examples of detection methods include detection by hardware or software monitors, flight crew detection, power up tests, and maintenance checks.

For a quantitative FMEA, a failure rate is assigned to each failure mode based on the failure mechanism irrespective of detection or mitigation. Whenever possible, these failure rates should be determined from failure data of similar equipment already in field use. Industry sources of failure rate data may be found in U.S. military handbooks, reliability analysis references, and industry reliability data exchange references.

Failure rate predictions may be generated using commercial off-the-shelf reliability software packages. Where these packages allow for user-defined reliability factors, the selected values for these variable factors should be documented for substantiation of their applicability and allow for repeatability across reliability prediction toolsets. These variable factors should also be consistent throughout the system under evaluation. The total failure rate for each failure effect category may be detailed in a summary sheet or can be summarized in an FMES as discussed in J.4.2.

There are two basic types of FMEAs on physical products: Functional and Piece-Part. Functional FMEAs are typically performed to support the safety analysis effort with Piece-Part FMEAs performed as necessary to provide further refinement of the failure rate or to enhance the understanding of specific failure effect(s). Piece-Part FMEAs are typically done when the more conservative failure rates from a Functional FMEA will not allow the system, function, or equipment to meet the FTA probability of failure budget. A Piece-Part FMEA may also be useful for systems that rely on redundancy or monitoring functions, since a Functional FMEA may not reveal single part failures affecting more than one redundant element. Piece-Part FMEAs are also useful for safety analysis of mechanical equipment and assemblies.

SAENORM.COM : Click to view the full PDF of arp4761a

J.3.2.1 Functional FMEA

A Functional FMEA may be performed at any indenture level. The appropriate level of subdivision is determined by the complexity of the system and the objectives of the analysis. If the required analysis is on a section of circuitry or mechanical devices larger than a particular function, it should be broken down into functional blocks. From an aircraft or system level, this may mean defining each LRU or equipment as a functional block. From the system or lower levels, it may involve breaking down equipment into many blocks. The FMEA task is simplified if each block has as few outputs as possible. Once the functional blocks have been determined, a functional block diagram should be created and each block labeled with its functional name. For each functional block, internal and interface functions should be analyzed relative to system operation. Typically, functional blocks are defined such that a function and its monitor or redundant functions are not in the same functional block. It might also be beneficial to have the interface between a function and its monitor or between redundant functions defined as a separate block.

Once the functional blocks have been defined, the failure modes for each functional block are postulated. Determine the failure modes by thinking about the intent of the functional block and trying to determine how that function might fail regardless of the specific parts used. The analyst should know the operation of the functional block well enough to be positive that no significant failure modes have been overlooked, including single part failures that could affect more than one redundant functional block. Often, given a clear description of the block’s function, many of the failure modes will become apparent.

The effect of each failure mode is determined by considering how the function fits into the overall design. Failure effect categories are generally created for each effect type and a failure effect category code may be assigned. All failure modes that cause this identical effect are assigned to the effect category. The effect category code, if assigned, can then be entered into the FMEA worksheet for each failure. Software or hardware failure monitoring must be considered when determining failure effects and means of detection. As part of this analysis, the analyst should verify that the monitoring can indeed detect the failure mode. In order to properly perform this analysis, the analyst should have detailed knowledge of the system requirements and software design including internal failure management techniques as applicable.

If a quantitative analysis is being performed, a failure rate is assigned to each failure mode. One technique is to perform a failure rate prediction for each block and apportion the failure rate across the various failure modes based on past experience of similar functions or other sources allowing determination of probability of occurrence. The failure rate is assigned to the failure mode regardless of any architecture features or detection mechanisms. Guidelines for failure distribution of parts is provided in J.3.2.2.1. It may also be possible to use the entire failure rate of some blocks as the rate of the failure mode of interest. Alternately, it may be possible to use the entire failure rate of the block for the failure mode of interest.

The results of the Functional FMEA are recorded in a worksheet similar to Table J1. This example table can be modified to meet the needs of the analyst. Different requirements may result in addition or deletion of some of the information. The analyst should ensure that the FMEA worksheet form and content meets the specific needs of the requester before beginning the analysis.

As the analysis progresses, the following should be retained for future maintenance of the FMEAs and to assist in resolving questions regarding the FMEA:

a. Justification of each failure mode.

b. Rationale for the assigned failure rate.

c. Rationale assigning a particular failure to a failure effect category.

d. Documentation of any assumptions made.

This supporting documentation is usually not included in the FMEA report, but is retained for reference.

J.3.2.1.1 Determining Functional Failure Modes

Typical functional failure modes to consider include, but are not limited to, the following:

a. Complete loss of function.

b. Over performance of function.

c. Under performance of function.

d. Spurious operation of function.

e. Intermittent function operation.

f. Erroneous (including oscillatory) function operation.

Following is a simple example of functional failure modes:

The power supply circuitry that generates the 5V can be called a functional block. Some examples of functional failure modes would be as follows:

a. Loss of 5V.

b. Voltage less than 5V (including reversed polarity).

c. Voltage greater than 5V.

d. Noise on 5V.

e. Short to ground or other voltage.

There may be other function failure modes based on function implementation.

SAENORM.COM : Click to view the full PDF of arp4761a

Table J1 - Example Functional FMEA worksheet

Failure Modes and Effects Analysis (FMEA)							
System:	FMEA Description:					Date:	
Subsystem:						Sheet of	
Equipment ATA:						File:	
Author:	FTA References:					Rev:	
Function Names	**Function Code**	**Failure Mode**	**Mode Failure Rate**	**Flight Phase**	**Failure Effect**	**Detection Method**	**Comments**

SAENORM.COM : Click to view the full PDF of arp4761a

NOTE: Should be revised to fit analysis level and program needs.

J.3.2.2 Piece-Part FMEA

A Piece-Part FMEA is similar to a Functional FMEA, except that instead of analyzing at the functional or block diagram level, the failure modes of each individual part contained in the equipment or function are analyzed. A Piece-Part FMEA can be used to determine the failure effects of potential electrical, electronic, or mechanical failures. For example, the effect of failures of a resistor or a motor shaft can be considered as part of a Piece-Part FMEA. Piece-Part FMEAs on electronic equipment are usually performed only as necessary when the more conservative results of a Functional FMEA will not allow the equipment to meet the FTA probability of failure budget. This is due in part to the difficulty in determining the failure modes for complex parts.

The first step in a Piece-Part FMEA is to create a list of all parts to be covered by the FMEA. The next step is to determine the failure modes of each part type. This is the most difficult part of the Piece-Part FMEA, particularly FMEAs performed on electronic equipment containing complex integrated circuits. Determining all the failure modes of any but the simplest parts (where industry data is available) is extremely difficult and sometimes impossible. In products with complex integrated circuits such as FPGAs, microprocessors or ASICs, it is usually best to perform a Functional FMEA to the level required to support the safety analysis. Piece-Part FMEAs can then be performed as required on some functions if further refinement is required. When in doubt the worst-case assumptions of part failure modes must be made. Information to assist in determining part failure modes is contained in J.3.2.2.1.

Once a part's failure modes have been determined, they are entered into the FMEA worksheet as shown in Table J2. This example worksheet can be modified to meet individual needs. Different FMEA goals and expectations may result in addition or deletion of some of the information in the worksheet. The analyst should ensure that the FMEA form and content meets the specific needs of the requester before beginning the analysis.

The next step is to determine the effect of the failure on the next higher level assembly and assign a failure effect category to the failure. Failure effect codes may be assigned to each category to simplify the table. The detailed description of each failure effect category can then be included in the text of the report. All failure modes that cause this identical effect are assigned to the effect category. The effect category code can then be entered into the Table J2 FMEA worksheet "Failure Effect" column for each failure. Software or hardware failure monitoring must be considered when determining failure effects and means of detection. As part of this analysis, the analyst should verify that the monitoring can indeed detect the failure mode. In order to properly perform this analysis, the analyst should have detailed knowledge of the system requirements and software design including internal failure management techniques as applicable.

If a quantitative analysis is being performed, a failure rate is assigned to each failure mode. The failure rate is assigned to the failure mode irrespective of any architecture features or detection mechanisms. Guidelines for failure distribution of parts is provided in J.3.2.2.1.

As the analysis progresses, the following should be informally recorded for future maintenance of the FMEAs and to assist in resolving questions regarding the FMEA:

a. Justification of each failure mode.

b. Rationale for the assigned failure rate.

c. Rationale assigning a particular failure to a failure effect category.

d. Documentation of any assumptions made.

This supporting documentation is usually not included in the FMEA report, but is retained for reference.

SAENORM.COM : Click to view the full PDF of arp4761a

Table J2 - Example Piece-Part FMEA worksheet

Failure Modes and Effects Analysis (FMEA)							
System:	FMEA Description:					Date:	
Subsystem:						Sheet of	
Equipment ATA:						File:	
Function:	FTA References:					Rev:	
Author:							
Part Number	**Part Type**	**Failure Mode**	**Mode Failure Rate**	**Flight Phase**	**Failure Effect**	**Detection Method**	**Comments**

NOTE: Should be revised to fit analysis level and program needs.

SAENORM.COM : Click to view the full PDF of arp4761a

J.3.2.2.1 Determining Piece-Part Failure Modes and Failure Distributions

In general, the function of the part must be considered and all potential ways that the part can fail to perform that function correctly must be considered for inclusion in the list of part failure modes. Unintended behavior of the part must also be considered. Industry references cited later in this section provide a good basis for the analyst to determine potential failure modes of the parts being analyzed.

While the failure rate and mode source documents provide a basis for failure modes of some part types, there will be many device types that are not included in these documents. This is especially true for complex digital integrated circuits (ICs) which need to be considered on a part by part basis. Determining the failure modes of digital devices generally requires engineering judgment and it is unlikely that all of the failure modes can be determined for a complex digital IC.

A method for establishing the failure modes of complex digital devices is to model the complex device under consideration with constituent functional blocks for which a better definition of failure modes may exist. Identify the constituent functional block pin level failure effects as the device failure modes, if possible. Some failures may affect single or multiple output pins and/or combinations of output pins. Particular attention should be paid to potential complex device failure modes that may lead to FTA basic events.

Trying to determine the actual failure mechanisms and the associated effects through a physics of failure approach is not recommended for ICs as it forces the analyst to perform an “FMEA” on each digital IC. This “FMEA” may be more complex than the higher-level FMEA being completed and may not even be possible for complex ICs. In addition, an undisclosed design enhancement by the chip manufacturer could render the entire effort obsolete. Complex IC failure modes can include intermittent failures and various failure combinations possibly affecting multiple pins.

Failure modes of other part types are more readily available than for ICs. However, a look at several sources will yield different failure mode distributions for the same part type and sometimes even different failure modes. This points out that even for simple parts it is difficult to determine which potential failure modes are valid and which ones cannot happen. The conservative approach is to assume the entire failure rate of the part can result in the failure modes of interest.

Typical failure modes to consider for simple parts include, but are not limited to, the following:

a. Open.

b. Short.

c. Parameter shifts.

d. Out of adjustment.

e. Dielectric breakdown.

f. Intermittent operation.

g. Inoperative.

h. Spurious operation.

i. Wear.

j. Mechanical failure.

k. Sticking.

l. Loose.

m. Fracture.

SAENORM.COM : Click to view the full PDF of arp4761a

When conducting Piece-Part FMEAs, it may be necessary to further break down the failure rates for parts to identify percentages of failure rates applicable to specific failure modes. Guidelines for failure rate and failure mode decomposition may be found in industry reliability data references (e.g., U.S. military handbooks, reliability analysis references or reliability data exchanges), or from appropriately assessed service experience of similar hardware operating in a similar environment. Engineering judgment is a necessary part of the failure mode determination process.

J.3.2.3 Substantiation

J.3.2.3.1 For Determining Failure Effects

If the analytical method of determining failure effects for a failure mode is difficult, service experience on similar hardware or laboratory verification should be performed when possible as a way to determine failure effects. Unfortunately, the most difficult failure modes to analyze are sometimes difficult to identify through testing. For example, it is impossible to insert internal failures into most ICs. Computer aided design software may also be used to simulate these IC failures. This software simulation allows the equivalent of the failure to be inserted into the circuit simulation and the failure effect determined.

J.3.2.3.2 For FMEA Effect Validation

It is desirable to confirm correctness of the captured failure effects to ensure FMEA result integrity. A minimum set of FMEA failure modes are selected for substantiation of failure effects. The following guidelines for selection of a minimum set of the FMEA failure modes are suggested:

a. Critical monitoring as defined in the safety assessments.

b. Ensure functional diversity in the selected set.

c. Consider each monitor is represented in the selected substantiation set.

d. Avoid substantiation failure injection cases that would result in damage to the system being evaluated.

Examples of FMEA substantiation may include analysis, simulation, test, or other means depending upon the indenture level of the FMEA. Results that indicate inconsistencies between the expected FMEA failure effect and an actual substantiation case result should be investigated to determine if additional design or analysis action is required.

Analysis of failures which occur during testing and in actual use may also be used to substantiate the results of the FMEA. This failure data may be used to create a library of failure modes for future FMEAs.

For electrical or electronic systems, failures may be inserted by opening leads or shorting leads together or to ground. If device outputs can be tri-stated, other logic combinations may be easily inserted.

J.4 DOCUMENTATION

The results of the FMEA can be documented in two similar type reports: the FMEA report and the FMES report.

J.4.1 FMEA Report

The report for an FMEA should include:

a. A document number allowing the report to be referenced by other analyses.

b. An introduction containing a brief statement about the purpose and the objective of the FMEA.

c. A brief overview of operation and a block diagram.

d. A section describing the analysis approach. (This section should include a description of how the analysis was performed, definitions of the levels used, and a listing of pertinent assumptions with associated rationale.)

SAENORM.COM : Click to view the full PDF of arp4761a

e. A complete listing of the results of the FMEA. (FMEA forms similar to the examples included in J.3.2.1 and J.3.2.2 can be used.)

f. Identifying part numbers and revision status of hardware and software analyzed.

g. Appendices should also include the following information:

1. Drawings or schematic diagrams.

2. Any failure mode distributions for lower-level parts defined during analysis or obtained from other sources. (Include justification for all modes considered).

3. A list of failure rates and failure rate source used in the analysis.

J.4.2 FMES Report

The Failure Modes and Effects Summary (FMES) is a summary of lower-level failure modes with the same effects and same detection mechanisms from the FMEAs. The failure effects from the FMEA are failure modes for the FMES. The higher-level effect is listed in the effect column of the FMES. Identical failure effects and detection from the FMEA are categorized as one mode in the FMES.

The failure rate for each failure mode in the FMES is the sum of the failure rates coming from the failure modes of the individual FMEA(s). An FMES need not necessarily be a separate analysis; it can be done as a part of an FMEA. If the FMES is used as an aid to simplify the FTAs (reduce the number of OR-gates at the lowest level) and to combine the effects of equipment or functional failures that have the same effect as one single event, it is important to understand how fault tree basic events use data from the FMES. For calculation of failure rates, it should be remembered that an FMEA considers single failures, whereas an FTA considers both single failures and combinations of failures.

The relationship between the FMEAs and FMES is shown in Figure J1.

SAENORM.COM : Click to view the full PDF of arp4761a

Circuit X FMEA

Failure Mode	Failure Rate	Failure Effect
R5 Open	**A**	**Loss of +5V**
R5 Short	**B**	**+5V tied to GND**

Circuit Y FMEA

Failure Mode	Failure Rate	Failure Effect
C5 Short	**C**	**+5V tied to GND**
C5 Open	**D**	
U58 P2 Open	**E**	

Item FMES

Failure Mode	Failure Rate	Failure Effect	Potential Failure Cause
+5V tied to GND	**B + C**	**No Command Signals**	**Circuit X – R5 Short Circuit Y – C5 Short**

Figure J1 - Example of FMEA to FMES relationship

J.4.2.1 Performing an FMES

The analyst should review the existing FMEA(s), and check all failure effects for consistency (i.e., is the same failure effect always described with the same wording and does different wording for the failure effect always mean a different failure?). This check should be done with special care when an FMES on the system-level is performed (i.e., summarizing effects from installation failure modes and equipment failure modes). The failure effect from the FMEAs is entered in the “Failure Mode” column of the FMES form similar to the example shown in Table J3. Note that the FMES form may be altered to add or delete specific data entries as necessary to support the specific FMES customer requirement and the specific FMEA format being used.

The analyst identifies all failure modes having the same failure effect and sums their individual failure rates. The calculated failure rate is entered in the “FAILURE RATE” column of the FMES. The references to the individual failure mode in the FMEA may be identified in the FMES “Potential Failure Cause” column. The effect of the failure mode on the next higher level, the systems of that failure and the relevant phase of flight may also be entered in the relevant columns of the FMES form.

J.4.2.2 FMES Documentation

Each FMES should include the following information:

a. A document number allowing the FMES to be referenced by other analyses (if prepared as a separate document).

b. A brief description of the system or equipment being analyzed, giving design philosophy, including monitoring devices and principal design features. (This should be supported by suitable diagrams, schematics, and block diagrams.)

c. A listing of primary and secondary system or equipment functions.

d. A list of references, part numbers, and revision identification to identify the hardware and software releases analyzed.

e. A section containing a concise description of the results of the analysis.

f. A list of failure rate sources.

g. References to FMEAs used to generate the FMES.

The results are documented in FMES tables providing an uncluttered overview of the results of the FMEA. See Table J3 for an example FMES worksheet format. The summary should present top-level failure effects, causal failure identifications, causal failure references, and means of detection. Flight phase information and detection methods may also be included.

SAENORM.COM : Click to view the full PDF of arp4761a

Table J3 - Example FMES worksheet

Failure Modes and Effects Summary (FMES)									
Aircraft:	FMES No:						Date:		
ATA:	Supplier:						Sheet of		
System:	Supplier Part Number:						Rev:		
Subsystem or Unit:	Supplier Drawing Ref:						Prepared by:		
Ref	**Failure Mode**	**Failure Rate**	**Phase**	**Effects On System**	**Symptoms 1. Flight Crew 2. Ground Crew**	**1. Causal Failure 2. Remarks**	**Causal Failure Ref**	**Check Ref**	**Failure Condition Ref**

SAENORM.COM : Click to view the full PDF of arp4761a

NOTE: Should be revised to fit analysis level and program needs.

J.4.3 FMEA/FMES Checklist

The following checklist will ensure that the correct steps are taken in the proper order to perform a cost effective and accurate FMEA.

a. Obtain written specification of FMEA goals and expectations, if possible, from customer or requester defining:

   1. Failure effects of interest.
   2. Outputs to be considered.
   3. Allowable failure detection methods.
   4. Final report format.
   5. Schedule.

b. Prepare for the analysis by:

   1. Obtaining and understanding documentation.
   2. Generating parts lists.
   3. Partitioning equipment into different levels and documenting the partitioning.
   4. Collecting failure modes of parts if a Piece-Part FMEA is required.

c. Perform detailed analysis by:

   1. Determining failure modes and assigning failure effect codes.
   2. Avoiding poorly defined failure modes so that confusion will not occur when going from the current level to higher levels.
   3. Determining detection means, if required, for each failure effect category.
   4. Making detailed notes documenting why a failure category was assigned.

d. Verify analysis conclusions (with lab or aircraft data if possible) for any issues in question.

e. Document the FMEA/FMES results.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX K - ZONAL SAFETY ANALYSIS (ZSA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

K.1 INTRODUCTION 257

K.2 SCOPE 257

K.3 INPUTS TO ZSA 257
K.3.1 Physical Hazards Inherent to the System Equipment 258

K.4 ZSA METHODOLOGY 258
K.4.1 Partition Aircraft into Zones 259
K.4.2 Preparation of ZSA Installation Questionnaire and Checklist 261
K.4.3 Develop Independence Related Installation Requirements 263
K.4.4 Organize List of Inherent Hazards per Aircraft Zone 263
K.4.5 Zonal Inspection 263
K.4.6 ZSA Outputs 265

K.5 Decision on Acceptability of Results 265

Figure K1 Zonal Safety Analysis flow 259
Figure K2 Example of aircraft zones: major zones 260
Figure K3 Example of aircraft zones: major sub-zones 261

Table K1 Potential installation questionnaire/checklist 262

SAENORM.COM : Click to view the full PDF of arp4761a

K.1 INTRODUCTION

The Zonal Safety Analysis (ZSA) evaluates the physical installation of equipment and systems in order to identify potential hazards caused by mutual influence/interference between equipment and between equipment and structure as well as the influence of the operating environment on installed equipment. Such influences include those originating from system equipment themselves or other system parts and inherent to their design and embedded technology; e.g., heat transfer, vibration, mechanical interference, electromagnetic radiation.

The ZSA analysis will generally be performed by an airframe manufacturer. The ZSA complements the System Safety Assessment (SSA) and Aircraft Safety Assessment (ASA) processes by ensuring there are no foreseeable physical interactions between installed equipment, or between the equipment and its operating environment, capable of compromising safety. The ZSA may also be useful during a Preliminary Aircraft Safety Assessment (PASA) or Preliminary System Safety Assessment (PSSA) process to aid in the generation of installation requirements.

The ZSA contributes to the common causes, together with the Common Mode Analysis (CMA) and the Particular Risk Analysis (PRA). The ZSA is intended to identify whether there are any zonal issues that could compromise intended independence e.g., zone overheat affecting multiple pieces of equipment simultaneously.

A ZSA should be carried out for each zone of the aircraft. The partitioning of an aircraft into zones is a task that is accomplished in order to perform the ZSA. Partitioning is further discussed in K.4.1.

The ZSA should be performed throughout the development process of a new aircraft or when necessary, on the partial re-design of existing aircraft. During the requirements-generation-and-validation phase, ZSA tasks will primarily consist of preparing installation guidelines and questionnaire as discussed in K.4.3.

Early ZSA may employ mockup representation of the basic aircraft design. Later phases of the ZSA are able to be performed on the completed aircraft, as and when it becomes available as discussed in K.4.5.

The reader should note that this appendix distinguishes between “questionnaire” and “checklist.” Both of these entities will contain a list of potential technical issues that should prompt further consideration/analysis by the ZSA specialists. Despite their resemblance in terms of content and application the distinction concerns the phase of application: “questionnaire” being used during the aircraft development phase and “checklist” being used during the aircraft verification phase.

K.2 SCOPE

This appendix contains the information and procedures necessary to perform a ZSA. The ZSA is composed of two primary activities:

a. During the aircraft development phase, it may assist in the establishment of safety-related installation requirements.

b. During the aircraft verification phase, it is used to verify that the implementation conforms with specific installation requirements and with established installation guidelines.

K.3 INPUTS TO ZSA

There are three broad categories of input to the ZSA methodology:

a. General guidelines.

b. Installation requirements applicable to the aircraft.

c. Technical support data.

SAENORM.COM : Click to view the full PDF of arp4761a

General guidelines are mainly composed of generic data accumulated on previous programs (both during development and in-service). These guidelines include:

a. Lessons learned from in-service experience.

b. Lessons learned from manufacturing and maintenance relative to access and replacement of equipment and systems.

c. Basic design and installation standards.

The above inputs should be added to the existing checklist in order to provide a more complete list of points to consider during the verification phase of the current program.

Installation requirements applicable to the aircraft comprises program-specific safety-related installation requirements coming from other parts of the development/safety process and includes installation requirements derived from PASA/PSSA Independence Principles and those coming from PRA. These inputs should be added to the existing checklist in order to provide a more complete list of points to consider during the verification phase of the current program.

Technical support data is mainly composed of data specific to the aircraft under development and in particular, safety-related data such as Failure Modes and Effects Analysis (FMEA), Failure Modes and Effects Summary (FMES), and any available data concerning known hazards inherent to the system technology. This support data also includes any program specific design data relevant to installation such as digital mockup of installation conditions, installation drawings, and system descriptions.

K.3.1 Physical Hazards Inherent to the System Equipment

For each system or equipment, identify physical hazards inherent to the system/equipment potentially having external effects. This should be done regardless of functional hazard classification in order to ensure inclusion of physical hazards inherent in functionally non-critical equipment and functions. This list can be based on general knowledge of physical hazards inherent to the system equipment technology, and/or more detailed information being available from sources such as FMEAs when they specifically identify these hazards.

Note that some well-established physical inherent hazards may be analyzed by use of PRAs. Typically, this will include significant physical hazards that are both well-known and may extend beyond a single aircraft zone.

K.4 ZSA METHODOLOGY

The objective of the ZSA is to evaluate design and installation of equipment and systems to identify specific interactions that may compromise aircraft safety. In order to achieve this, the ZSA methodology is applied early in the development and considers:

a. The effect of equipment and systems on other equipment installed within the equipment sphere of influence.

b. The effect of maintenance errors relative to access and replacement of equipment and systems.

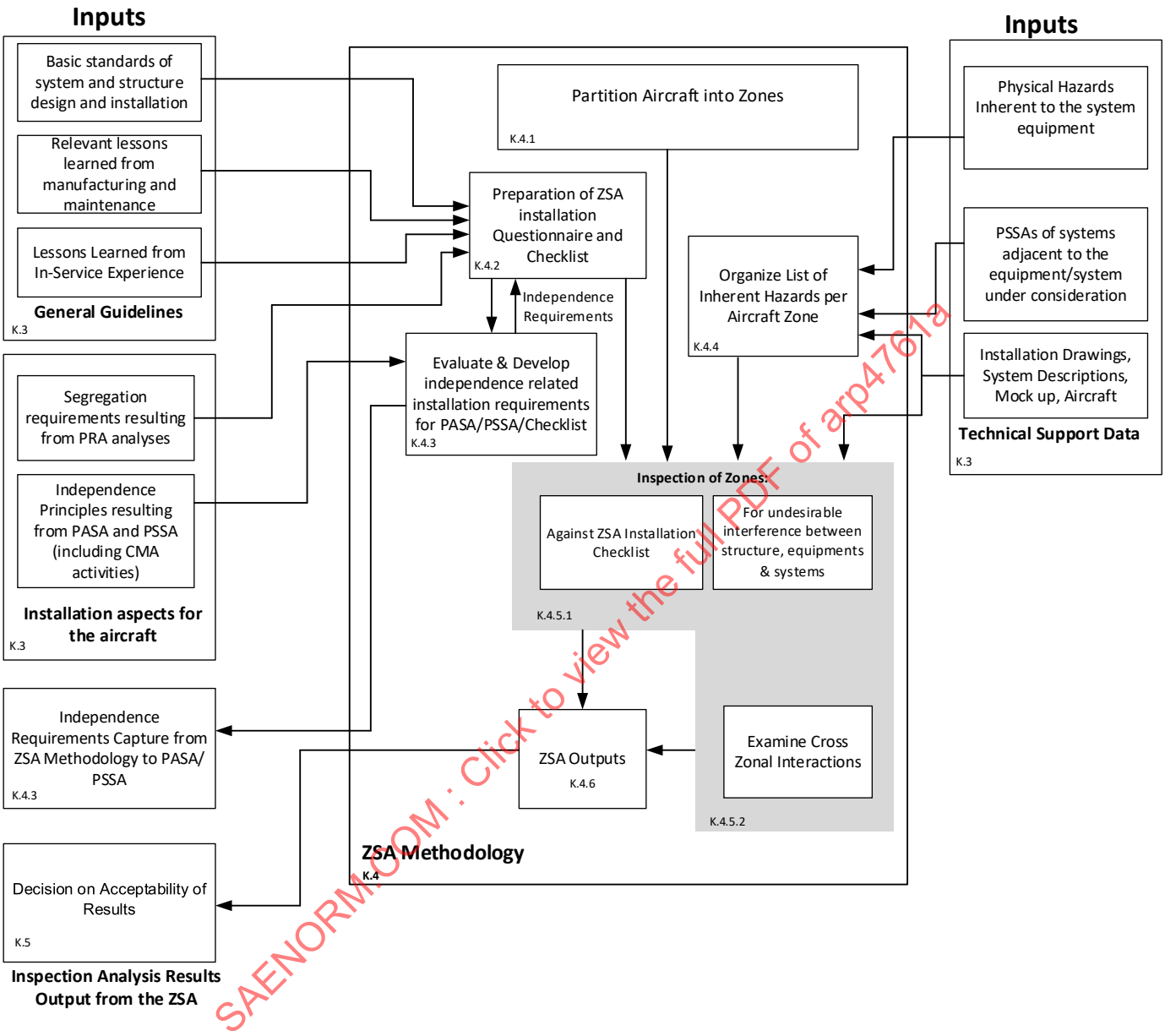
c. The effects of the operating environment on equipment and systems e.g., ventilation, drainage, vibration, temperature, acceleration-loads, differential pressures.

d. Whether independence related installation requirements intended to ensure independence claims made in the PSSA, PASA, or elsewhere are acceptably implemented.

e. Whether aircraft manufacturer specified and/or general installation guidelines have been respected in the aircraft implementation.

SAENORM.COM : Click to view the full PDF of arp4761a

The ZSA may also be used to help generate installation requirements supporting the Independence Principles developed in the PASA/PSSA. Figure K1 shows which tasks should be undertaken during the ZSA process.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure K1 - Zonal Safety Analysis flow

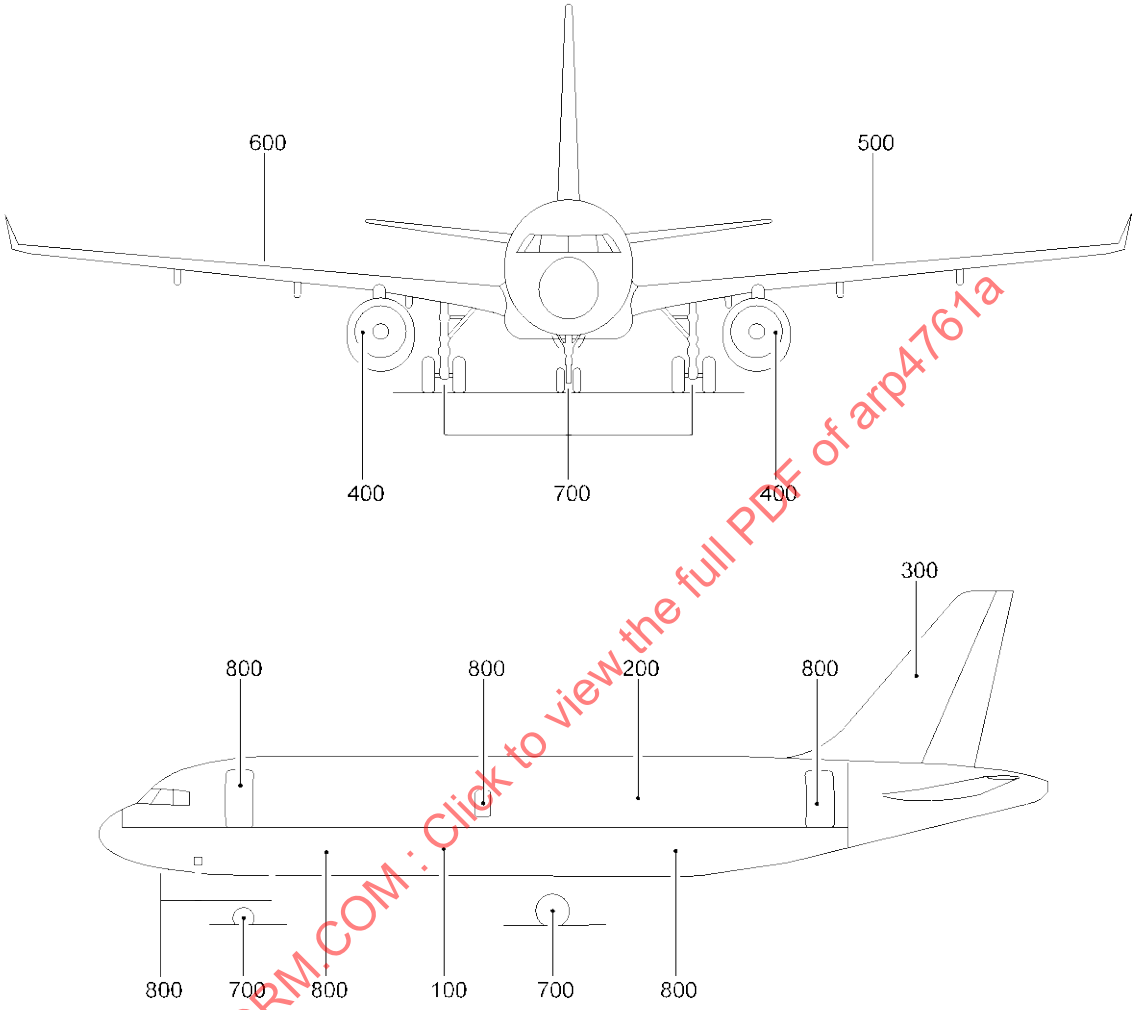
K.4.1 Partition Aircraft into Zones

The aircraft should be partitioned into distinct zones. The aircraft zones may be defined outside the scope of the ZSA and should be consistent with the zone designations selected for purposes other than ZSA. Selecting zones that are consistent throughout the aircraft will aid the analysts' understanding and identification of cross-boundary threats and help to reduce or eliminate any potential areas of concern from being omitted. Typically, zones are initially defined by identifying compartments that are isolated from each other by aircraft structures (e.g., pressurized cabin, wheel wells, area within a fairing). Zones may be further segmented by the presence or absence of certain threats (e.g., flammable fluids), or simply to maintain a manageable scope of analysis (e.g., segmenting the passenger cabin in large aircraft).

The environment within a zone should be fairly uniform. If one section of a zone has an environment that is significantly different from another section of the same zone, consider sub-partitioning the zone.

Conversely, excessive partitioning should be avoided. If there is no physical boundary between two zones and their environment is fairly similar, consider consolidating the zones.

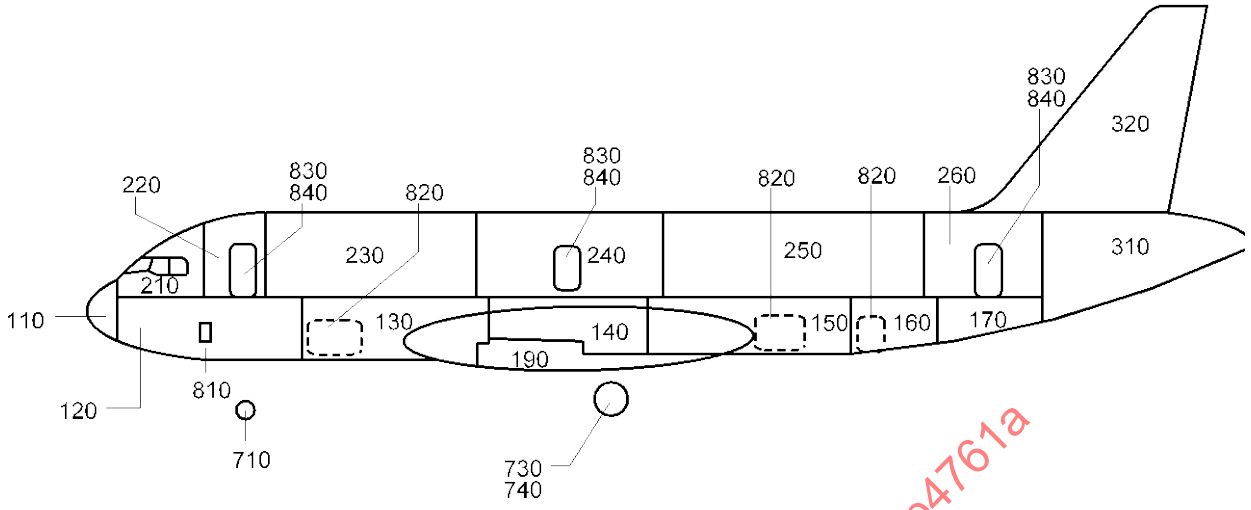
Figures K2 and K3 present how a typical aircraft may be partitioned into major zones and sub-zones for the purposes of a ZSA.



SAENORM.COM : Click to view the full PDF of arp4761a

Major Zones	Description/Boundaries	Major Zones	Description/Boundaries
100	Lower half of fuselage (below cabin floor) including radome to forward face of aft pressure bulkhead.	400	Power plant nacelles and pylons.
		500	Left Wing
200	Upper half of fuselage (above cabin floor) to forward face of aft pressure bulkhead.	600	Right Wing
		700	Landing gears and landing gear doors.
300	Stabilizer and fuselage rear section from rear of aft pressure bulkhead (including rudder & elevators)	800	Passenger/crew doors, cargo compartment doors and emergency exits (pressurized doors).

Figure K2 - Example of aircraft zones: major zones



Major Sub-Zones	Description/Boundaries	Major Sub-Zones	Description/Boundaries
110	Radome.	160	Lower deck bulk cargo compartment: aft partition of aft cargo compartment to aft partition of bulk cargo compartment.
120	Avionics compartment: forward pressure bulkhead to aft partition of avionics compartment.	170	Aft cabin underfloor compartment: aft partition of bulk cargo compartment to aft pressure bulkhead.
130	Lower deck forward cargo partition compartment: aft of avionics compartment to forward pressure bulkhead of wing center box.	190	Belly fairing, air conditioning compartment, hydraulic compartment.
140	Wing center box, air cond, hyd compartment: forward pressure bulkhead of wing center box to forward pressure bulkhead of aft cargo compartment.	210	Flight Deck from forward pressure bulkhead to flight deck partition.
150	Lower deck aft cargo compartment: forward pressure bulkhead to aft partition of aft cargo compartment.	220	Forward cabin utility area aft of flight deck partition to front of forward cabin.

Figure K3 - Example of aircraft zones: major sub-zones

SAENORM.COM : Click to view the full PDF of arp4761a

K.4.2 Preparation of ZSA Installation Questionnaire and Checklist

A ZSA installation questionnaire and checklist should be prepared for new aircraft programs. This questionnaire/checklist should take into account any particularities associated with individual zones. For derivative aircraft modifications, the changed areas or additional systems/functionality introduced should be validated against the existing questionnaire/checklist and installation guidelines of the baseline aircraft. The intent is to utilize the baseline questionnaire/checklist as much as possible and modify as necessary based on the presence of new systems, new functionality, new fuselage sections, and new technology.

The ZSA installation checklist should extract all relevant installation rules from the following inputs:

a. Basic standards of system and structure design and installation.

b. Relevant lessons learned from manufacturing and maintenance (relative to access and replacement of equipment and systems).

c. Lessons learned from in-service experience.

The ZSA installation questionnaire/checklist can be grouped into general checkpoints, system specific design and installation checkpoints or zone-specific design and installation checkpoints. The ZSA installation questionnaire/checklist should be used by the ZSA analyst during inspection of the installation.

Table K1 provides examples of potential installation concerns that should be considered. It should be noted that this table is intended as an example and does not attempt to provide an exhaustive list of all potential installation concerns.

Table K1 - Potential installation questionnaire/checklist

#	Type
1	**Separations and clearances**
1.1	Independence of systems redundancies
1.1.1	Separation of related systems—mutual and from others
1.1.2	Separation between routes categories
1.1.3	Separation between networks
1.2	Interferences
1.2.1	Minimum clearance: moving rigid mechanical parts (mutual)
1.2.2	Minimum clearance: moving mechanical parts/structure
1.2.3	Minimum clearance: moving parts/flexible hydraulic hoses
1.2.4	Minimum clearance: control cables (mutual)
1.2.5	Minimum clearance: control cables/structure
1.2.6	Minimum clearance: harnesses/pipes (e.g., oxygen, air, water, fuel, hydraulic)
1.2.7	Minimum clearance: harnesses/structure
2	**Maintenance and servicing**
2.1	Fool proofing
2.2	Loose packing (installation of wiring, hoses, etc.; e.g., chafing prevention on electrical raceways)
2.3	Accessibility
2.4	Damage or hazard likely from servicing/maintenance
2.5	Hand/footholds (hand/footholds to be minimized or protection to be added)
2.6	Damage or hazard likely from unattached parts (flyaway kit, standby connectors, etc.)
2.7	Injury/damage to personnel/equipment, especially if power “on”
2.8	Accumulation of debris—check for traps
3	**Drainage**
3.1	Effect of incorrect installation of drainage
3.2	Drainage where accumulation is dangerous
3.3	Leakage path down to drain (ignition source on the path)
3.4	Drain outlet (ignition source or re-ingestion)
4	**Materials compatibility**
4.1	Compatibility with fluid susceptibility
5	**Failure consequences**
5.1	Damage from flailing torque shafts
5.2	Disconnection or failures leading to jams
5.3	Damage from debris of rotating equipment
5.4	High pressure and/or high temperature leak (hydraulics, air pipes, etc.) impacting the environment (structure and systems, electrical wire interconnect system (EWIS))
5.5	Electrical shorting impacting the environment (structure and systems, EWIS)
5.6	Burst of accumulator causing secondary damage
5.7	Release of stored energy by failed equipment
5.8	Robustness to loss of fixation points (mechanical attachment points)
5.9	Thermal effects
5.10	Inflammable fluid leaks close to heat source
5.11	Contamination of air conditioning due to fluid
5.12	Contamination by fluid (drip loop, sealing plugs, umbrellas/covers, etc.)

SAENORM.COM : Click to view the full PDF of arp4761a

K.4.3 Develop Independence Related Installation Requirements

Independence Principles coming from the PASA and PSSA processes may also need to influence the physical installation of systems within the aircraft. In conjunction with aircraft installation specialists and the ZSA questionnaire, the PASA and PSSA processes are able to define physical installation requirements aimed at supporting the Independence Principles previously developed. This activity is graphically represented in Figure K1 as being an integral part of the ZSA methodology; however, it is a shared activity with the PASA and PSSA processes. In order to graphically represent the exchange of Independence Principles; independence requirements; aspects for inclusion in the ZSA installation questionnaire and checklist; Figure K1 uses a bi-directional arrowhead between PASA/PSSA and ZSA methodology.

The ZSA installation questionnaire addressing potential common causes is used to support the PASA and PSSA creation of independence related installation requirements. Independence related installation requirements should be created when the safety risk is considered unacceptable due to potential installation common causes. Other possible sources of independence related installation requirements include the PRAs and CMA.

One area of particular interest concerns the potential for human error during maintenance actions and the potential for such errors to either compromise intended independence and/or induce latent failures in the physical installation. The aircraft development phase should address this concern and should result in requirements intended to prevent such error occurrence.

K.4.4 Organize List of Inherent Hazards per Aircraft Zone

Using installation drawings, aircraft mockups or other sources of aircraft installation data, the data input described K.3.1 should be organized by zone to detail the list of systems and equipment whose inherent technology represents hazards that may become zonal threats.

The inherent hazards of such systems and equipment potentially have an effect on structures, other systems or equipment installed within the same zone or adjacent zones. These lists will facilitate the ZSA of such inherent hazards undertaken in K.4.5.1.

K.4.5 Zonal Inspection

Two aspects of zonal inspection are considered in the ZSA process:

a. Inspection within zones.

b. Cross zonal interactions.

Both of these aspects are further developed in this section.

Initially, ZSA will be undertaken on a virtual representation of the basic design and installation guidelines. The virtual representations may be drawings but are more likely to be computer-based models. In the final phases of the project, the aircraft, as built, should be inspected to verify zonal requirements have been achieved. This verification may be accomplished by inspection of early production aircraft. If a digital model of the aircraft zone exists, and has been confirmed as matching the aircraft as built, this verification may be accomplished by inspection of the digital model.

K.4.5.1 Inspection of Zones (Within Zones)

The inspection within each zone of the aircraft should:

a. Check that design and installation guidelines and recommendations have been properly addressed through use of the ZSA installation questionnaire/checklist.

b. Confirm that independence related installation requirements have been properly implemented through use of the ZSA installation checklist.

c. Confirm that existing protections are sufficient to prevent a compromise in safety (e.g., drainage and ventilation providing mitigation and detectability of a flammable fluid leak). Assess acceptability of deviations and, if necessary, propose design improvement.

SAENORM.COM : Click to view the full PDF of arp4761a

d. Identify features of the design that could be vulnerable to manufacturing or maintenance error.

e. Identify features of the design that could contribute to or introduce manufacturing or maintenance error.

f. Identify any undesirable interactions between equipment and systems within a zone that could influence the physical or functional safety of the aircraft, e.g., equipment with known electromagnetic signature in close proximity to equipment sensitive to the same frequency spectrum.

g. Identify interactions between zone environment conditions and the installed equipment that could influence the physical or functional safety of the aircraft.

For each of the above points, update the ZSA installation questionnaire/checklist, installation guidelines and recommendations, and list of physical hazards inherent to the system technology wherever relevant.

The following are examples of what to check for:

a. Mechanical clearance to prevent damage from abrasion (chafing) and interference with moving parts. Consider variability in the assembly, and the flexibility of equipment (e.g., wiring and hoses) and of the aircraft structure itself.

b. Environmental and material compatibility to prevent damage from exposure to environmental factors such as temperature, humidity, contamination. Consider zone characteristics and equipment qualification.

c. Accessibility to prevent damage from tools or ground support equipment during manufacturing or maintenance. Consider the potential for human error caused by the removal of equipment when performing maintenance, the potential for incorrect reinstallation of equipment, etc. Also consider the spatial relationship of operators to the equipment, use of tools and ground support equipment, potential use of equipment and structures as hand or footholds.

d. Non-conformance to standard installation guidelines such as insufficient or inappropriate installation fixtures, cables routed such that condensation can track down to connectors, excessively tight cable bend radii.

e. Equipment including lithium-ion batteries and the hazard their flammability represents to neighboring system and structure installations.

Table K1 shows an example of a simplified ZSA installation questionnaire/checklist with aspects of physical implementation that should be checked during the zonal and inter-zonal inspections.

The results of the inspection of the zone against the design and installation guidelines and the resulting identified effects on the aircraft of systems/equipment external failures should be considered in the ASA, and should reflect the aircraft configuration being summarized therein. The results of the ZSA may also be considered in relevant SSAs.

In addition, any issues raised and subsequent actions to resolve these issues should be recorded for future reference on the program. This information may also prove useful for future programs and may be integrated into an update to the installation guidelines and recommendations.

It is recommended that the zonal inspection phase of the ZSA includes some participation from appropriate maintenance specialists. The zonal inspection should ensure that accidental damage while conducting maintenance on the system, engine or aircraft has been considered. Consideration may be achieved by documented participation of appropriate maintenance specialists or by providing references to an existing maintenance report.

K.4.5.2 Inspection of Zones (Cross-Zonal Interactions)

As an extension to the activities described in K.4.4, consideration should be given to any effects that are able to cross zonal boundaries and potentially affect systems/equipment in adjacent zones if not accomplished in a PRA. Equipment or systems in one zone may have effects that propagate into other zones. This cross-zone interaction should be considered, especially where zone boundaries do not coincide with physical boundaries defined by the aircraft structure. For example, water leaking from the galley flows into and affects equipment in the fairing zone.

SAENORM.COM : Click to view the full PDF of arp4761a

K.4.6 ZSA Outputs

Records of the analysis should be made on an ongoing basis and should include a list of any relevant specialists assisting the responsible ZSA analyst. In addition to working systematically through the guidelines and checklists, the following details should be included:

a. How and when the assessment was made (e.g., detail use of models, modelling techniques such as MBSA, mockups, aircraft).

b. The responsible ZSA specialist and any other relevant supporting specialists.

In addition to these preliminary results (and subsequent mature results) for each zone of analysis, the data detailed in K.4.6.1 should be submitted to the relevant development process and safety process (as applicable).

K.4.6.1 ZSA Outputs of Analyses Results

Analysis results output from the ZSA should include any identified installation issue that could compromise aircraft safety. In particular the following points should be detailed:

a. Confirmation should be given that the ZSA has been completed.

b. Any deviations from the installation guidelines.

c. Potential installation related maintenance errors.

d. Non-conformance with specific installation requirements.

e. The correct identification of any system or equipment that is highlighted as a potential problem.

f. Graphical evidence of any issues discovered (e.g., digital mockup screen shots, photographs).

g. Potential failures that could result from physical hazards inherent to system technology.

Note that for systems or equipment whose technology has been identified as an inherent source of physical hazard in the zone, the following information should be captured:

a. References for the source of any physical hazard (including components failed and unfailed).

b. Rationale for the potential failure effect on the neighboring systems, equipment, or structures.

c. Inherent failure mode descriptions for the system or equipment where applicable.

d. Description of inherent risks identified in components operating in a non-failed state.

The results from the ZSA inspection analyses should be submitted to the overall development process and safety process (as applicable).

K.5 DECISION ON ACCEPTABILITY OF RESULTS

The ZSA results are reviewed by the overall development program and safety process actors to determine acceptability of the physical installation. Foreseeable operational or environmental effects, item interactions and violation of required independence/separation capable of compromising safety are considered. Possible resolutions of any identified issues by the development program may include identification and documentation of additional mitigating factors within the current design or a design change may be implemented. It should be understood that the ZSA assessment is iterative in nature and that all issues identified are eventually resolved. Such installation issues and their associated resolution should be captured in ZSA results documentation.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX L - PARTICULAR RISK ANALYSIS (PRA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

L.1 INTRODUCTION 267
L.1.1 Particular Risks 267
L.1.2 Particular Risk Analysis 267
L.1.3 List of Commonly Considered Particular Risks 268

L.2 SCOPE 269

L.3 PRA METHODOLOGY 269

L.4 OUTPUTS 272
L.4.1 Outputs to the Development Process 272
L.4.2 PRA Documentation 272

Figure L1 PRA activities 270

SAENORM.COM : Click to view the full PDF of arp4761a

L.1 INTRODUCTION

L.1.1 Particular Risks

Particular risks are defined as physical risks/hazards:

a. Originating from system equipment or other parts and inherent to their design and embedded technology, such as rapid release of energy from concentrated sources, storage of flammable fluids or mixtures, heat transfer, capacity to provide ignition source, capacity to deliver unintended mechanical energy (e.g., vibratory), emission of electromagnetic radiation, or

b. Originating from a source external to the aircraft, e.g., atmospheric conditions, impact from foreign objects, or

c. Originating from structural failures, e.g., rupture of a pressure bulkhead.

Many of the particular risks are subject to specific airworthiness requirements (e.g., uncontained engine rotor failure, tire burst).

Particular risks are able to affect:

a. Both aircraft structures and systems.

b. One or more aircraft sections, and even the entire aircraft.

c. One or more aircraft functions.

d. One or more aircraft systems.

e. One or more aircraft system installations.

Particular risks may compromise aircraft structural integrity, system safety margins, and intended independence, thus impairing aircraft survivability and safety.

L.1.2 Particular Risk Analysis

Particular risks are the subject of Particular Risk Analyses (PRA).

PRAs are safety activities managed from an aircraft-level perspective. The PRA differs from other analyses that are performed to assure the safety of the aircraft, as it is an aircraft survivability analysis. Each particular risk is analyzed as a threat to the aircraft. The objective is not to determine how often these threats occur, but to establish the survivability of the aircraft in the presence of each threat, considering all its potential effects, and ensure hazards relevant to the particular risk have been minimized/prevented to the extent practical, in accordance with specific regulatory requirements. Sometimes a probabilistic analysis may be used to support that the threat has been adequately mitigated, but the use of these analyses does not obviate the need for the aircraft survivability analysis performed in the PRA.

Having identified the appropriate particular risks with respect to the design under consideration, each risk should be subject to a separate study using a format similar to that outlined in this appendix. The objective of the analysis of each particular risk is to ensure that any safety effects are either eliminated, minimized, or shown to be acceptable.

Owing to the potential consequences of the PRA on the overall aircraft design (structure design, system design, system installation design) particular risks should be considered as early as possible during the development process.

The PRA should be carried out throughout the aircraft development process for a new aircraft. Any modification to the aircraft should be analyzed to determine potential impacts on each PRA, and any identified impact should result in a PRA update. Initially, drawings or models should be analyzed. But as the project progresses, the analysis should be based on mockups and then the actual aircraft wherever suitable.

SAENORM.COM : Click to view the full PDF of arp4761a

Each PRA should examine various constraints associated with aircraft design and implementation, ranging from structural integrity requirements to independence requirements.

The PRA techniques in this document may also be used to analyze other aspects of the aircraft design for threat response.

L.1.3 List of Commonly Considered Particular Risks

This section provides a list of particular risks classified per type of source. This list is indicative of industry collective experience at the time of writing of this appendix, but can be completed considering any relevant additional in service or development experience and potential risks introduced by new technologies.

L.1.3.1 Risks Originating from System Equipment or Other Parts and Inherent to Their Design and Embedded Technology

Such risks include, but are not limited to the following:

a. Fire and smoke.

b. Leaking fluids.

c. Tread separation from tire (flailing tread or tread shed).

d. Wheel flange release.

e. Uncontained rotary mechanism.

f. Rotor burst.

g. Fan blade out/sustained engine imbalance (wind milling).

h. Ram Air Turbine blade release (RAT burst).

i. High pressure storage bottles rupture.

j. Hazardous chemical storage containers leakage or rupture.

k. High pressure ducts leakage or rupture.

l. Fuel tanks and lines leakage or rupture.

m. Accumulator burst.

n. Battery leakage or fire or thermal runaway.

o. Failure of mechanical equipment or part (e.g., actuators, control arms, linkages, cables, belts) potentially leading to interference with adjacent systems or structures.

L.1.3.2 Risks Originating from a Source External to the Aircraft

Such risks include, but are not limited to the following:

a. Hail, ice, snow.

b. Bird strike.

c. Lightning strike.

d. High-Intensity Radiated Fields (HIRF).

SAENORM.COM : Click to view the full PDF of arp4761a

L.1.3.3 Risks Originating from Structural Failures

Such risks include, but are not limited to the following:

a. Pressure bulkhead rupture.

b. Rapid decompression.

Note that in addition to the above three categories Particular Risk Analysis techniques may be deemed suitable for analysis of certain security related risks like survivability of systems (see 14 CFR/CS Part 25.795(c)(2)).

L.2 SCOPE

This appendix provides a methodology for performing a PRA. The objective is not to determine how often the particular risks occur, but to establish the survivability and safety of the aircraft. The PRA methodology uses a top-down approach and a bottom-up approach. The top-down approach is used to develop proposed safety requirements at an early stage in the development process. The bottom-up approach starts with particular risk physical effects and assesses whether the cumulative physical and functional effects are acceptable against top-level safety and certification objectives.

L.3 PRA METHODOLOGY

The PRA is usually performed on a risk-by-risk basis and is primarily a qualitative analysis performed iteratively.

The analysis steps described in Figure L1 are appropriate for most PRA. However, for some PRA, specific approaches might be necessary which cannot all be described in this document.

The described methodology combines:

- A top-down approach, using failure conditions, failure conditions classifications, and Independence Principles identified by Aircraft Functional Hazard Assessment (AFHA), Preliminary Aircraft Safety Assessment (PASA), System Functional Hazard Assessment (SFHA), and Preliminary System Safety Assessment (PSSA), and lessons learned from previous experience to develop at an early stage proposed requirements for the development process.

- A bottom-up approach, reviewing a proposed design, starting with identifying particular risk physical effects (e.g., physical aircraft elements damaged by a given debris trajectory), then determining the resulting functional effects, if any, and assessing whether the cumulative physical and functional effects are acceptable against top-level safety and certification objectives.

SAENORM.COM : Click to view the full PDF of arp4761a

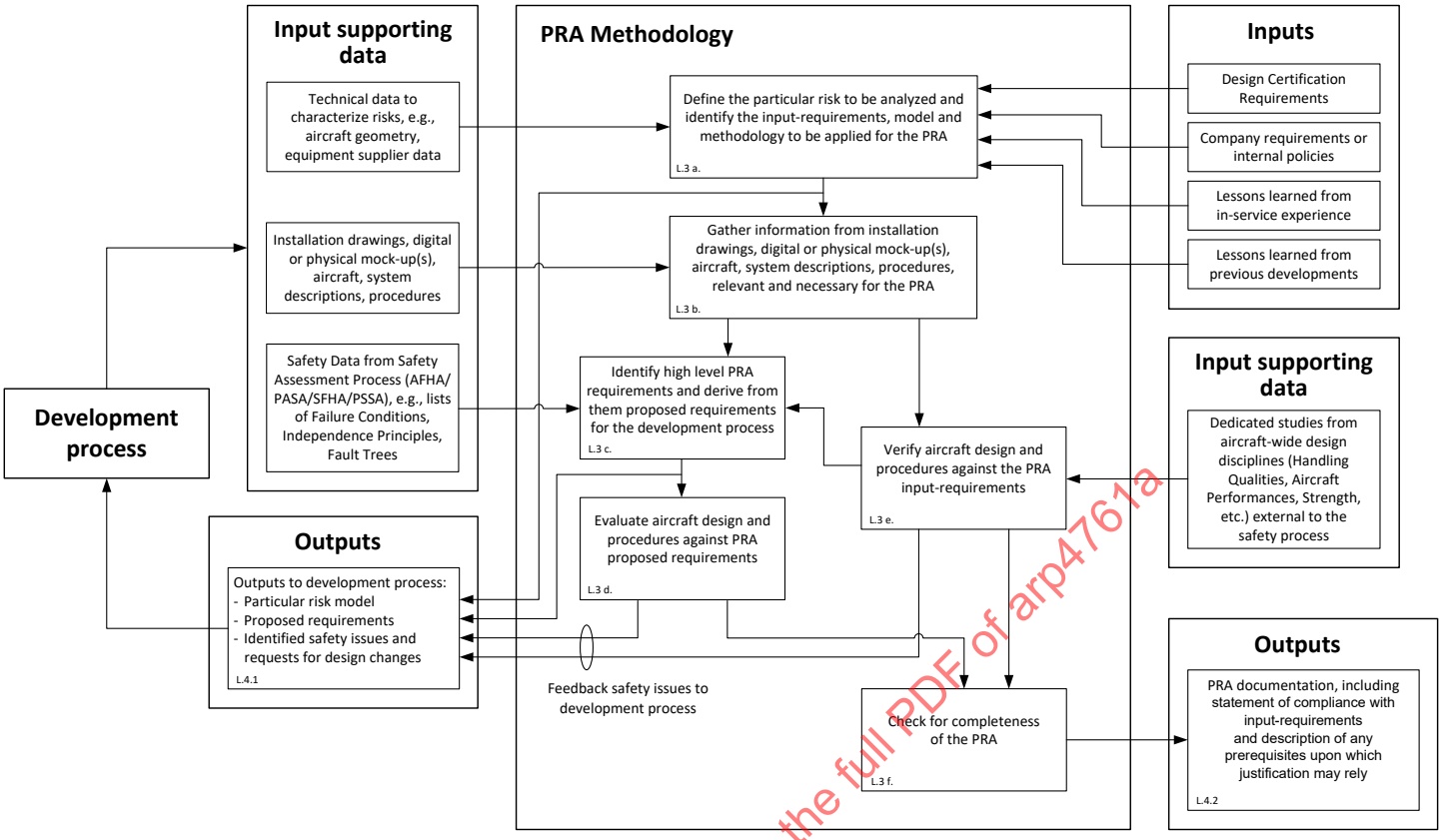


Figure L1 - PRA activities

SAENORM.COM : Click to view the full PDF of arp4761a

The following details the typical activities that should be undertaken for each particular risk:

a. Define the particular risk to be analyzed and identify the input-requirements, model and methodology to be applied for the PRA:

   1. Identify the particular risk to be analyzed (e.g., tire/wheel burst).

   2. Identify the input-requirements to be fulfilled based on design certification requirements (e.g., 14 CFR/CS Part 25.729(f) or CS 25.734), company requirement(s) or internal policies, lessons learned from in-service experience and lessons learned from previous developments.

   3. Define the methodology and the general assumptions to be used for the analysis using the information gathered in a.2.

   4. Define the model (e.g., tire burst model and wheel burst model, which would include failure mechanism, debris size, energy and trajectories, position of the debris source in the aircraft) to be used for the analysis using the information gathered in a.2. and additional technical data (e.g., aircraft geometry, equipment supplier data), as needed to characterize the risks.

   The information defined in a., in particular the model to be used for the analysis, should be provided to the development process which will use it to develop solutions fulfilling the input-requirements identified in a.2. and the proposed requirements from c., if any.

b. Gather information from installation drawings, digital or physical mockup(s), aircraft, system descriptions, or procedures relevant and necessary for the PRA.

c. Identify high-level PRA requirements and derive from them proposed requirements for the development process:

1. Gather information from the safety process AFHA/PASA/SFHA/PSSA (e.g., lists of Catastrophic and Hazardous failure conditions, Independence Principles developed by PASA/PSSA to satisfy “no single failure” requirement associated with Catastrophic failure conditions, fault trees).

   Note that Catastrophic failure conditions will be considered. Hazardous failure conditions will be considered only if specifically required by regulations or company requirement(s) or internal policies.

2. Select from the list of Catastrophic and Hazardous (if any) failure conditions gathered in c.1. which are relevant in the context of the particular risk under study.

3. Identify any early high-level PRA requirements using information gathered in a., b., and information related to the failure conditions selected in c.2.

4. Derive proposed requirements for the development process from high-level PRA requirements identified in c.3.

5. As the design and PRA activities become more mature (considering feedback from step e.) new particular risk scenarios may be identified that are not covered by the set of proposed requirements developed in c.4. Identify additional PRA proposed requirements for these new scenarios.

Consistency of the proposed requirements identified in c.4. and c.5. with those coming from other safety activities performed in parallel (other PRA, Zonal Safety Analysis (ZSA), system safety activities) should be ensured as part of the development process. The corresponding activity is not described in this appendix.

Note that some organizations may elect to ensure fulfillment of input-requirements using other equivalent approaches. For example, this goal can be met by means of providing recommendations to the development process, and whose implementation would be regularly monitored throughout the development process, until the final verification phase.

d. Evaluate aircraft design and procedures against the PRA proposed requirements developed in c.

In the event that the PRA analyst identifies that PRA proposed requirements have not been implemented, the issue is communicated to the organizations responsible for the development of the involved systems, equipment, and structures, in order to ensure the issue is resolved as part of the development process (design change or acceptable mitigation provided).

If PRA proposed requirements cannot be implemented, they should be revisited or a deviation should be shown acceptable against the PRA input-requirements identified in step a.2.

e. Verify aircraft design and procedures against the PRA input-requirements:

1. Identify sets of systems/equipment/structures that are affected together (e.g., by a given trajectory or in a given damage area) considering all existing mitigating design features relevant to the particular risk (e.g., structural barrier or shielding for flying debris, ventilation for thermal risk), using information gathered in a. and b.

2. Identify the effects (functional and/or physical) on each individual affected part.

3. From the identified effects on each individual affected part, determine the relevant particular risk scenarios at aircraft-level, taking into account potential interdependencies and cumulative effects. The Cascading Effects Analysis (CEA) method from Appendix O can be used as necessary to support this activity.

4. Assess the consequences on aircraft of the particular risk scenarios and determine if the consequences are acceptable against the PRA input-requirements identified in step a.2.:

   i. If consequences are acceptable, prepare justification documentation and identify any prerequisites upon which it may rely. These prerequisites may include structural items to withstand a particular risk impact, or implementation of an additional dedicated monitoring function (to be considered in PASA/PSSA).

   ii. If consequences are unacceptable, document rationale and initiate a design change.

SAENORM.COM : Click to view the full PDF of arp4761a

Note that when assessing the consequences of the particular risk scenarios, ensure consistency, when relevant, between the “Effect on Aircraft” and “Failure Condition Classification” entries in the PRA and PASA/PSSA/ASA/SSA data. Dedicated studies from aircraft-wide design disciplines (such as aircraft’s handling and performance, structural strength, human factors) might be necessary to support the assessment.

f. Check for completeness of the PRA:

The analysis of each particular risk is complete when:

1. The PRA has verified that the implemented design under consideration meets the input-requirements and the proposed requirements, if any.

2. The PRA has verified that any safety effects are either eliminated, minimized, or shown to be acceptable.

3. All necessary PRA outputs have been generated and captured as part of the documentation set.

4. The design justified in the PRA documentation is representative of the production model.

L.4 OUTPUTS

L.4.1 Outputs to the Development Process

The outputs to the development process mainly include:

a. The model used for the analysis.

b. PRA proposed requirements.

c. Communication of identified safety issues and requests for design changes, as relevant, with associated rationale.

This information will be used by the development process to develop solutions fulfilling the PRA input-requirements.

L.4.2 PRA Documentation

For each particular risk, the results of the PRA should be recorded.

Typically, for PRA following the analysis steps described in Section L.3, the PRA documentation should include the following information:

a. The description of the analyzed particular risk.

b. The input-requirements to be fulfilled, the model and methodology used for the analysis.

c. The area of the aircraft impacted by the particular risk.

d. Any prerequisites used by the PRA and upon which justification may rely, typically:

1. General assumptions.

2. Any mitigating design features, whether implemented to fulfill a proposed requirement identified by the PRA, or present for any reason independent from the PRA.

3. Any other mitigation feature, like a specific procedure.

SAENORM.COM : Click to view the full PDF of arp4761a

e. The description of each identified PRA scenario, including:

   1. The systems/equipment/structures which are affected together.

   2. The resulting effect on the aircraft and the failure condition classification of that effect.

   3. References to the specific documentation used to analyze and classify the effects.

   4. Statement of acceptability of the PRA scenario against input-requirements.

f. For the failure conditions input from the safety process (AFHA/PASA/SFHA/PSSA) which are deemed relevant in the context of the particular risk (see Section L.3.c.), evidence that requirements have been derived to the development process, and that the design and other implemented mitigation features are fulfilling these requirements.

   Note that this information may be used as input by PASA/PSSA (in early phases of the development), then by SSA/ASA (during final system and aircraft integration and verification phases).

g. Overall conclusion/statement of compliance with input-requirements.

For PRA not following the analysis steps described in Section L.3, the PRA documentation may have a different format and content which cannot all be described in this document.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX M - COMMON MODE ANALYSIS (CMA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

M.1 INTRODUCTION 275

M.2 SCOPE 275

M.3 COMMON MODE ANALYSIS FIELD OF APPLICATION 275
M.3.1 Tailoring CMA Activities to the Specific Project 277
M.3.2 CMA Performed for Aircraft Level 280
M.3.3 CMA Performed for System Level 285

Figure M1 CMA activities and boundaries 276

Table M1 CMA questionnaire examples 277
Table M2 Example CMA evaluation table 282

SAENORM.COM : Click to view the full PDF of arp4761a

M.1 INTRODUCTION

Common Mode Analysis (CMA) is a qualitative analytical method used to support evaluation of independence. In a CMA, engineering experience is systematically applied to review function, architecture, development/design, implementation, manufacturing, maintenance and operation in a logical way. This appendix describes the CMA activity used to support the following:

a. Development Phase (as part of PASA Appendix B and PSSA Appendix D), which refers to activities prior to implementation. (The full name for this phase is “requirements development and validation phase.”)

b. Verification Phase (as part of SSA Appendix E and ASA Appendix F), which refers to activities occurring after implementation.

c. Assignment of development assurance levels associated with architecture consideration.

While this appendix illustrates the CMA performed during the development and verification phases as separate activities, in practice the iterative nature of development means that each of these phases may be an input into the other (see Figures 5 and 7 in ARP4754B/ED-79B). Accordingly, through this iterative process, the CMA as part of the Preliminary Aircraft Safety Assessment/Preliminary System Safety Assessment (PASA/PSSA) or Aircraft Safety Assessment/System Safety Assessment (ASA/SSA) may identify independence shortcomings (e.g., in architectures or requirements), thereby initiating changes to be made. These changes would then be re-evaluated iteratively until the safety process substantiates, with sufficient confidence, that the Independence Principles can be achieved.

The activities described in this appendix may be applied at any indenture level (aircraft, system, equipment, function, or item). The CMA provides techniques to support the definition of requirements from the Independence Principles and the subsequent verification that the actual implementation satisfies independence requirements and hence fulfills those Independence Principles. The goal of the CMA is to identify areas where a lack of independence may occur for the Independence Principles of interest. It is not to obtain perfect and/or absolute/theoretical independence, because that is considered unrealistic from an engineering viewpoint, but to take particular care that needed independence is not defeated. The CMA identifies sources of failures and errors which may result in a lack of independence.

PASA/PSSA generates Independence Principles which are inputs to the CMA to be examined. As a result of the CMA, the PASA/PSSA then generates independence requirements that are more specific.

CMA is part of the common cause methods, which includes Particular Risk Analysis (PRA) and Zonal Safety Analysis (ZSA). CMA is performed to consider potential breaches of independence other than those that are considered separately in the PRA or ZSA. PRA and ZSA are not part of the CMA, but provide complementary common cause failure analysis results. An aircraft-level CMA should consider potential common causes not covered in the PRA or ZSA.

M.2 SCOPE

This appendix provides guidelines for performing CMA activities. The process described may be used at aircraft, system, equipment, function or item-levels and takes into account the function, architecture, development/design, implementation, manufacturing, maintenance, and operation.

M.3 COMMON MODE ANALYSIS FIELD OF APPLICATION

CMA may be performed at different times during the safety assessment process. This qualitative assessment supports examination of the key features of the intended implementation, where independence has been determined to be necessary which are hereafter referred to as Independence Principles. The nature of the evaluation is determined by when in the development cycle (i.e., development or verification) the CMA is being performed.

For each Independence Principle identified, it needs to be determined whether the principle is subject to common cause failure, common cause error, or both.

SAENORM.COM : Click to view the full PDF of arp4761a

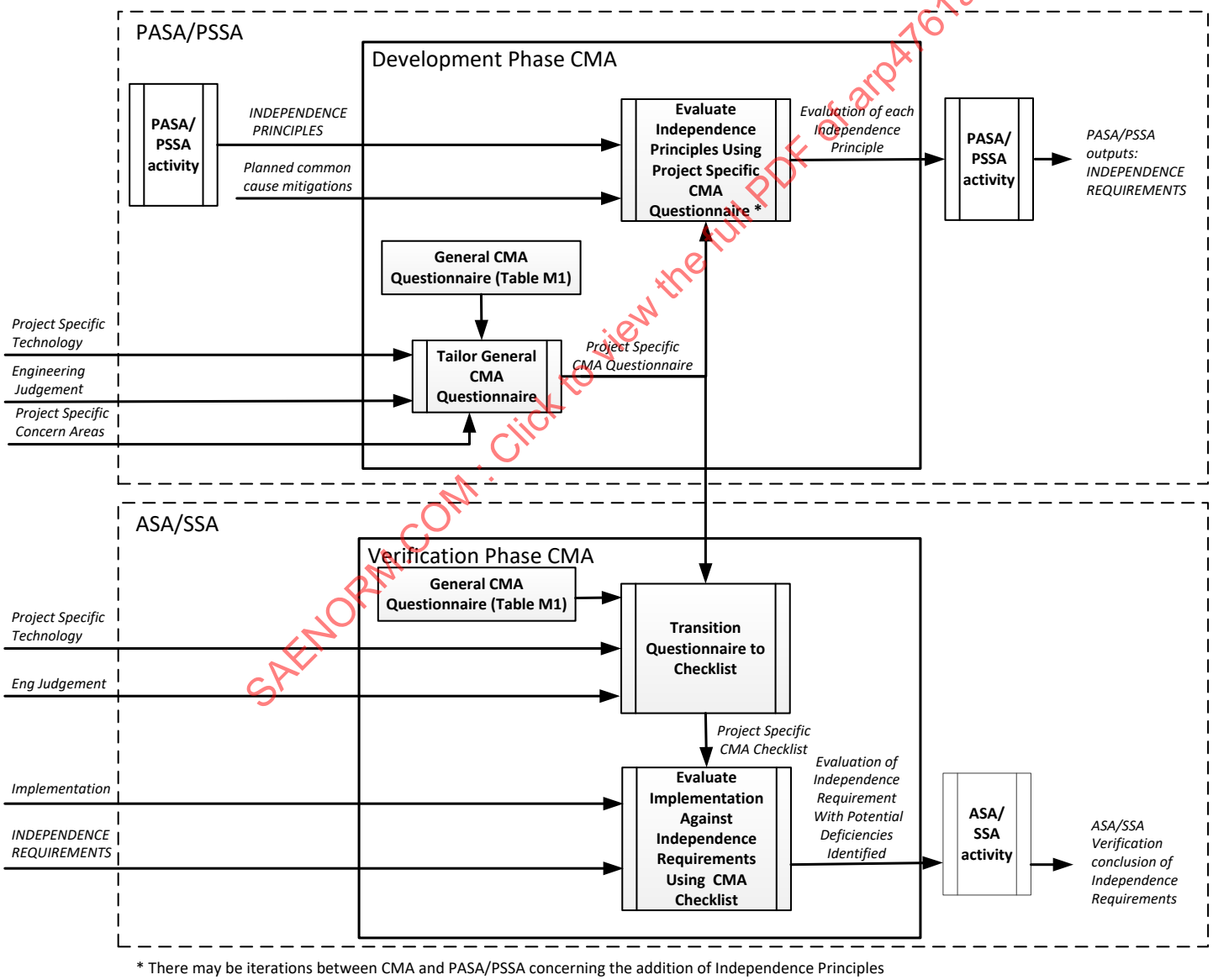
M.3.1 describes how CMA activities may be tailored to suit the needs of particular projects. A generic questionnaire, presented in Table M1, summarizes a wide range of potential common cause failure types, error types, event types, and installation considerations. Table M1 is used to guide the analyst in the generation of a project-specific set of CMA questions which may then be applied to the system or equipment being analyzed.

M.3.2 describes the aircraft-level CMA activity. It describes how the CMA activities support the PASA in ensuring that the Independence Principles may be satisfied by the proposed design and how the ASA CMA activities verify that the Independence Principles have been maintained or have not been compromised by the implementation.

M.3.3 describes the system-level CMA activity. Similar to the aircraft-level CMA, this section describes the CMA activities supporting the PSSA and SSA.

The CMA activity supports development assurance level assignment as covered in Appendix P.

Figure M1 presents the boundaries for the CMA activities being described within this appendix.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure M1 - CMA activities and boundaries

M.3.1 Tailoring CMA Activities to the Specific Project

It is important to establish the scope of the concern areas that will be considered during the Development Phase and Verification Phase CMAs. There will be unique elements to every project. As the aircraft architecture develops and the safety activities progress, new Independence Principles may be identified, resulting in additional CMA activities. These unique elements will need to be taken into account when establishing the scope of CMA activities.

One method for planning CMA activities is to use the CMA questionnaire (or set of questionnaires) as a task identification tool. Table M1 illustrates general common cause types and potential common cause sources. For each project, the general set of potential common cause types are reviewed for applicability to the present project development activities and tailored to better represent the scope of work and issues for that project. As the architecture develops or new Independence Principles are identified, the elements within the CMA questionnaire may need to be refined or augmented to ensure that all relevant aspects of independence are addressed by the CMA.

Tailored CMA questionnaires are derived based on the example data presented in Table M1 and previous experience. The level of detail of these questionnaires depends upon the level of complexity or novelty of the technology or system under study and is adapted to the level of analysis.

Table M1 - CMA questionnaire examples

Common Cause Sub-Type	Could Independence be Affected by a Common Failure of:	Failure Mode or Error Source Examples
Common Resource - Electrical Power		
Electrical power generation	Power source/supply malfunction?	- Failure due to loss of single electrical power source/supply. - Failure due to insufficient electrical power source/supply capability to support load. - Failure due to common response to over/under voltage output.
Electrical power distribution	Common functions used in power distribution system? Common equipment used in power distribution system?	- Loss of electrical power due to malfunctions of switches, relays, circuit breakers. - Inadequate grounding/earth point design (loss of a common ground shared between two otherwise independent functions).
	Power distribution cabling?	- Insufficient cable current carry capability resulting in excessive voltage drop. - Failure due to loss of single power source/supply cabling.
Common Resource - Hydraulic Power		
Hydraulic power generation	Hydraulic pump malfunction?	- Failure due to loss of single hydraulic power source/supply. - Failure due to insufficient hydraulic power source/supply capability to support load. - Failure due to common response to over/under pressure output.
Hydraulic Supply Distribution	Common functions used in the hydraulic distribution? Common components used in the hydraulic distribution?	- Failure due to valves, pressure regulators, manifolds.
	Hydraulic distribution piping?	- Insufficient fluid flow resulting in pressure drop. - Insufficient pressure or volume capacity of the hydraulic lines.
Common Resource - Pneumatic		
Pneumatic pressure generation Pneumatic vacuum generation	Common functions used in creating pressure? Common functions used in creating vacuum?	- Failure due to loss of single pneumatic source/supply. - Failure due to insufficient pneumatic source/supply capability to support load. - Failure due to common response to over/under output.
Pneumatic piping	Common equipment used in pneumatic implementation? Common distribution piping/tubing?	- Insufficient flow resulting in pressure drop causing common failure. - Insufficient pressure and volume capacities of the pneumatic lines.
Common Resource - Other		
Networks	Receipt or transmission of data on common network?	- Inadequate network infrastructure, protocols. - Inadequacy of network protections. - Lack of separation of networks by criticality of data.

SAENORM.COM : Click to view the full PDF of arp4761a

Common Cause Sub-Type	Could Independence be Affected by a Common Failure of:	Failure Mode or Error Source Examples
Interfaces (e.g., connectors, routes)	Separation/segregation of signals within interfaces?	- Lack of signal separation/segregation within an interface causes failure of otherwise independent signals. - Failure of interface due to inadequate environmental ratings.
	Separation/segregation of signals between interfaces?	- Lack of signal separation between interfaces results in common failure. - Inadequate separation maintained through signal path (e.g., cables, flex cable, motherboards) results in failure. - Lack of signal separation of two independent functions through same interface supporting the same failure condition (e.g., loss of signal resulting in loss of brake function and loss of signal causing loss of ground spoiler where both used for stop on the runway failure condition). - Failure of interface due to inadequate environmental ratings.
Processing	Common processing elements?	- Failure of common receive/transmit devices. - Failure of common data packaging software routines. - Failure of common computing devices. - Use of common software, e.g., software drivers, CSCIs (when item development independence was assumed).
Data	Incorrect or corrupted data?	- Missing data. - Erroneous data. - Incorrect upload/download of data.
Data Storage	Common data storage devices?	- Inadequacy of data protection from external interference/ corruption. - Inadequate volume/speed of data transfer from data storage to other devices. - Insufficient storage capacity of RAM, mass data stores, motherboard data transfer/volume capacity.
Databases/Libraries	Loss of common database or library? Corruption of common database or library?	- Failure due to common response to loss of database/library information. - Failure due to common response to erroneous database/library information.
Sensors	Functions sharing common sensors or common sources?	- Failure of common sensor used for control path and a monitor path that are intended to be independent. - Failure of common sensor used to provide data to multiple functions (systems).
Additional common resources identified by the PASA	Any additional common resources identified by the PASA	- Air-ground signals. - Inertial data. - Air data. - Navigation data. - Electronics cooling.
Development/Design Process		
Specification	Common specifications? Common requirements error?	- Erroneous specification due to human error, omission, or commission (e.g., specification temperature is set at 70 °C when it should be 80 °C). - Standard mathematical functions or lookup tables (e.g., sine lookup). - Erroneous specification interpretation. - Erroneous requirement interpretation errors, i.e., requirement is subject to ambiguity (e.g., cultural or company differences).
Software Development/Design	Common software specification? Common software error? Common software function?	- Erroneous software specification due to human error, omission or commission. - Software error due to implementation tools (e.g., compilers, linker, relocate, loader). - Errors in common software library functions. - Errors in software function (e.g., aircraft flight dynamics model, Kalman filter, flight control equations).
Hardware Development/Design	Common hardware specification? Common hardware error? Common hardware function? Hardware tool error?	- Erroneous hardware specification due to human error, omission or commission. - Erroneous component usage in circuit design. - Erroneous hardware function (e.g., aircraft flight dynamics model, Kalman filter, flight control equations, power supply). - Error in VHDL compiler or synthesis tool.

SAENORM.COM : Click to view the full PDF of arp4761a

Common Cause Sub-Type	Could Independence be Affected by a Common Failure of:	Failure Mode or Error Source Examples
Firmware Development/Design	Common firmware specification? Common firmware error? Common firmware function?	- Erroneous firmware specification due to human error, omission, or commission. - Firmware error due to implementation tools (e.g., compilers, loader). - Errors in common firmware library functions. - Errors in common firmware function (e.g., algorithm).
Tools	Support tools contain or generate errors?	- Error in Computer Aided Design (CAD) tool. - Error in modelling tool (Model Based Systems Engineering Tool - MBSE). - Error in requirements management tool.
Processes	Common development process error (omission or commission)?	- Inadequate functional and/or development independence. - Designer failure to predict an event. - Designer failure to specify adequate environmental conditions ranges.
Implementation		
Implementation Issues	New or sensitive technology? Common equipment? Common hardware implementation error? Component application?	- Erroneous application of new or sensitive technology. - Failure due to common component operation (e.g., processor incorrectly handles integer number arithmetic operations (always adds one to the result)). - Failure due to common implementation features (e.g., power supply voltages, ground paths, isolation mechanisms, incorrect A/D or D/A conversion, printed wiring assembly). - Equipment used outside of data sheet operating ranges. - Failure due to component wear out (e.g., contamination of multiple braking surfaces due to contamination).
Installation Design		
Equipment Bays	Local failure or event? Interaction of equipment installed in same location?	- Insufficient structural strength to support load of installed equipment. - Inadequate wire bundle diameter not appropriate to allow escape of heat. - Failure of common load paths. - Uncontained failure of equipment having intrinsic hazard. - See Zonal Safety Assessment.
Environmental Conditioning	Malfunction of environmental conditioning? Malfunction of heating?	- Loss of cooling air. - Erroneous cooling (e.g., air volume/temperature less than designed). - Equipment bay environmental conditioning system cooling capacity not adequate for the heat load of installed equipment. - Loss of heating, erroneous heating.
Equipment installed incorrectly	Equipment being cross-installed? Over-torquing?	- Lack of keying results in two functions/connector pins both being installed in the incorrect position.
Physical Partitioning	A physical barrier?	- Arcing. - Fire. - Physical damage between wires or groups of wires. - Metal whiskers. - Electrical propagation. - Loose hardware (e.g., wire cuttings, loose screws).
Environment		
Mechanical and Thermal	Temperature? Grit? Impact? Vibration? Pressure? Humidity? Moisture? Stress? Flammable vapor?	- Fire, lightning, welding, cooling system faults, electrical short circuits. - Airborne dust, metal fragments generated by moving parts with inadequate tolerances. - Pipe whip, water hammer, structural failure, shock. - Machinery in motion. - Out of tolerance system changes (pump overspeed, flow, blockage). - Misting pipe break, steam pipe. - Condensation, pipe rupture, rainwater. - Thermal stress at welds of dissimilar metals, thermal stresses. - Auto ignition temperature.

SAENORM.COM : Click to view the full PDF of arp4761a

Common Cause Sub-Type	Could Independence be Affected by a Common Failure of:	Failure Mode or Error Source Examples
Electromagnetic	Electromagnetic interference, electromagnetic compatibility? Conducting Medium? Out of tolerance?	- Inadequacy of EM testing, bonding, shielding, rotating electrical machinery. - Moisture resistance. - Power surge voltage, short circuit, power surge current.
Chemical	Corrosion (acid)? Corrosion (oxidation)? Other Chemical Reactions?	- Leak of acid used in maintenance for removing rust and cleaning. - Moisture around metals. - Galvanic corrosion, complex interactions of fuel cladding, water, oxide fuel.
Miscellaneous	Biological?	- Poisonous gasses, animate (i.e., living organisms) causes.
Manufacturing		
Manufacturer	Common manufacturer?	- Error due to inadequately trained manufacturing personnel. - Error due to manufacturing procedure interpretation. - Incorrect procedure used by manufacturing personnel.
Procedures	Same manufacturing procedure use?	- Error in procedure (omission or commission).
Process	Same manufacturing process use?	- Incorrect manufacturing process. - Inadequate manufacturing control or inspection, or testing.
Tools	Common manufacturing tools?	- Tools used in manufacturing of equipment that is intended to be independent.
Operation		
Staff	Common operations staff?	- Operator error due to inadequately trained or over-stressed personnel. - Operator error due to incorrect or inadequate procedure interpretation. - Omission of procedure action.
Procedures	Common operation procedure?	- Faulty operating procedures. - Misdiagnosis (following wrong procedure). - Missing or incomplete procedure information.
Maintenance		
Staff	Common maintenance staff? Common installer (fitter) staff?	- Maintenance or installation error due to inadequately trained or over stressed personnel. - Maintenance or installation error due to incorrect or inadequate procedure interpretation. - Maintenance or installation error due to use of incorrect procedure. - Failure to follow repair or installation procedure.
Procedures	Common maintenance or installation procedure?	- Erroneous or defective repair or installation procedure. - Missing repair or installation procedure. - Inadequate calibration/tools adjustments. - Failure to follow calibration procedures. - Lack of calibration procedure.
Location	Interaction between elements during Installation or maintenance?	- Local failure or event (see Zonal Safety Analysis).

SAENORM.COM : Click to view the full PDF of arp4761a

M.3.2 CMA Performed for Aircraft Level

This section describes the activities of a CMA supporting PASA and ASA. It is applicable to the Development Phase where the focus of the CMA is to evaluate the planned development and planned implementation with respect to the allocated Independence Principles (the relationship between Independence Principles and independence requirements is discussed in Section M.1). It is also applicable to the verification phase where the focus of the CMA is to evaluate the implementation with respect to the allocated Independence Principles.

The usage of CMA within the assignment of development assurance levels with architecture considerations is described in Appendix P.

M.3.2.1 Development Phase CMA as Part of a PASA

Development Phase CMA activities may be performed to support independence assessment as part of the PASA process. This section discusses the inputs, CMA questionnaire development and application, and PASA CMA result output.

M.3.2.1.1 CMA as Part of a PASA - Inputs

The inputs needed to perform the Development Phase PASA CMA include:

a. CMA questionnaire examples (Table M1).

b. Independence Principles (and associated rationale) identified by the PASA, including any project level Independence Principles coming from other sources or experience.

c. Characteristics intended to eliminate or reduce sources of common causes. (e.g., partitioning, redundancy, intended diversity, segregation, isolation or barriers, error tolerance).

The analyst needs to be familiar with and understand the proposed aircraft architecture characteristics with regard to development, implementation, operation and installation. These characteristics may be included in:

a. Project planning and development information.

b. Function specifications (requirements documentation).

c. Design architecture descriptions.

d. Installation considerations.

e. Maintenance and test considerations.

f. Operational information.

Also, the analyst may use the following aircraft-level information from the PASA:

a. Interdependence Analysis results (Table B1 in Section B.3) which identifies potential common causes affecting two or more otherwise independent systems

b. List of aircraft-level functions that are identified as needing aircraft-level functional independence. These may be needed to support Function Development Assurance Level (FDAL) assignment (B.4.1).

c. Multifunction and Multisystem (MF&MS) Analysis results from B.4.2, that identify the following:

    1. How system functional failures combine to result in the considered aircraft failure condition.

    2. Whether functional Independence Principles and physical segregation or separation requirements are adequately identified for systems whose failures combine to produce an aircraft-level failure condition.

d. Common resource considerations results (list of common resources that could potentially violate assumed independence of systems, from B.4.3).

e. PASA documentation to allow traceability of Independence Principles

M.3.2.1.2 CMA as Part of a PASA - Tailor the Generic Questionnaire

There are a large number of recurring concerns regarding common cause failures throughout a broad spectrum of designs (e.g., electrical supply, data-bus, common processor modules). Such concerns, derived from the generic CMA questionnaire provided in Table M1, may be addressed across all development projects and/or tailored to suit the particular project under consideration. For example, there is no need to consider areas relating to software when it is clearly not appropriate, such as mechanical-only system.

SAENORM.COM : Click to view the full PDF of arp4761a

Project-specific CMA questionnaires are derived based on the generic CMA questionnaire given in Table M1 and previous experience, such as common knowledge or experience in similar aircraft (e.g., lessons learned). The level of detail of these questionnaires depends upon the level of complexity or novelty of the technology or system under study. The questionnaire is adapted to the level of analysis (aircraft or system or subsystem). It should be emphasized that while Table M1 provides an initial starting point, it is not necessarily exhaustive. The Analyst should therefore consider other potential common cause sources that may be able to defeat assumed independence in the particular project under consideration since these are not already included in the example CMA evaluation questions of Table M1. Particular attention should be paid to new technologies, processes or methodologies.

M.3.2.1.3 CMA as Part of a PASA - Process

Once the project-specific CMA questionnaire is complete, each Independence Principle is evaluated in an appropriate format, against the common cause sources to create a descriptive narrative, which identifies concerns and mitigations. Results of the CMA, such as the example information shown in Table M2, are used by the PASA process to develop the necessary independence requirements.

Table M2 - Example CMA evaluation table

Independence Principle Under Analysis		
Common Failure or Error Source Concern	**Description of Effect on Principle**	**Description of Mitigating Factors or Lack of Independence**
Question from tailored questionnaire list.	Narrative description of the effect of the common failure source on the Independence Principle under evaluation.	Narrative description of the factors planned or implemented to mitigate the common failure source or the description of any lack of independence identified for the principle.
- - -	- - -	- - -
Continue question/evaluations until tailored questionnaire list is complete for the Independence Principle under evaluation.		

SAENORM.COM : Click to view the full PDF of arp4761a

For each CMA Independence Principle identified, the following CMA steps are performed:

a. Apply the questionnaire to determine any lack of independence for the principle due to potential common cause failures or error sources.

b. Analyze each potential common cause source; identify resulting failure effects of the common cause source and describe the planned mitigations to substantiate that the independence criteria will be met.

c. In case of finding a lack of independence for the principle, the finding is captured and addressed by the PASA process.

Potential independence deficiencies are identified using CMA. The PASA process acts on these deficiencies by identifying additional mitigation strategies or if necessary, passing corrective action (creation/correction of Independence Principles) needs to the development process. It is the task of the CMA, during the PASA phase, to help define the need for mitigation strategies.

Independence requirements are developed as part of the PASA process using the output of the CMA.

M.3.2.1.3.1 CMA as Part of a PASA - FDAL Assignment

The process in terms of FDAL assignment examination is similar to that discussed in M.3.2.1.3. The difference is that for FDAL assignment examination, the activities during the PASA phase focus on identification of potential error sources (rather than failures) within the development/design process that may defeat the intended independence of functions. The CMA emphasis is on identification of adequate functional independence within the development process to satisfy the independence attribute characteristics of ARP4754B/ED-79B. FDAL assignment is described in Appendix P.

M.3.2.1.4 CMA as Part of a PASA - Outputs

The outputs of a Development Phase CMA supporting the PASA include the following:

a. Project-specific CMA questionnaire.

b. Feedback to the PASA process covering:

   1. Evaluation of each Independence Principle.

   2. Any potential independence deficiencies identified.

   3. Any assumptions made in accomplishing the CMA.

c. Reference to information, drawings, and support material used in the analysis.

M.3.2.2 Verification Phase CMA as Part of an ASA

Verification Phase CMA activities may be performed to support assessment of independence as part of the ASA process.

M.3.2.2.1 CMA as Part of an ASA - Inputs

The inputs needed to perform the Verification Phase CMA as part of the ASA process:

a. The project-specific CMA questionnaire developed during the Development Phase PASA CMA activities and any further relevant developments that may have emerged during the implementation process.

b. All Independence Principles (including any that may have emerged during the implementation process).

c. Independence requirements identified during the PASA process.

d. Design implementation information.

M.3.2.2.2 CMA as Part of an ASA - Gather Design Implementation Information

In the verification phase, the focus of CMA is to ensure that the appropriate Independence Principles and requirements (and hence objectives and characteristics) have been accomplished in the implementation such that the effects of common cause errors and common cause failures have been adequately mitigated. The analyst(s) needs to know and understand the subject system characteristics with regard to system development, implementation, operation, and installation. These system characteristics may include:

a. Design architecture.

b. Installation data (may be related to ZSA which considers a particular zone).

c. Equipment and component characteristics.

d. Software design characteristics (e.g., partitioning).

e. Maintenance and test tasks.

f. Systems, equipment, and item specifications (requirements).

g. Equipment implementation data.

h. Operational information.

SAENORM.COM : Click to view the full PDF of arp4761a

Also, the analyst reuses the following aircraft-level information:

a. Interdependence Analysis results.

b. Function list along with any independence claims to support the FDAL assignment.

c. Multifunction and Multisystem analysis results that identifies the following:

    1. How system functional failures combine to lead to the considered aircraft failure condition.

    2. What availability and integrity requirements/ probability allocations to systems are necessary in order to meet safety objectives associated to the aircraft-level failure condition severities, expressed numerically or qualitatively (e.g., 1.0E-07 or Remote)

    3. Whether functional Independence Principles and physical segregation/separation requirements are adequately identified for systems whose failures combine to produce an aircraft-level failure condition.

d. Common resource considerations results (list of common resources that can violate independence of systems).

ASA documentation to allow traceability of independence requirements and attributes at aircraft-level should also be captured.

Additionally, the analyst interfaces with the design team to become aware of mitigation characteristics utilized to eliminate or reduce sources of common causes. Examples of these mitigations may include:

a. Diversity.

b. Redundancy.

c. Barriers.

d. Testing.

e. Preventive maintenance programs.

f. Design control and design quality level (FDAL application).

g. Independent review of procedures, processes and specifications.

h. Training of personnel.

i. Quality control.

SAENORM.COM : Click to view the full PDF of arp4761a

M.3.2.2.3 CMA as Part of an ASA - Examination of the Implementation

The Verification Phase ASA CMA activities are based on analyzing the aspects of the implementation that may defeat the intended independence of functions as detailed in specific Independence Principles and allocated independence requirements. The project-specific CMA questionnaire developed during the Development Phase PASA CMA activities is reviewed and updated as necessary, considering the general CMA concerns of Table M1 and any new concerns that may have arisen during the development. At this point the questionnaire becomes a “final” ASA checklist which is then applied to the Independence Principles of interest.

For each CMA Independence Principle identified, the following CMA steps are performed:

a. Apply the checklist to determine the potential sources of common cause failures/errors associated with each source.

b. Analyze each potential source and resulting common cause failures/errors to substantiate whether the independence requirements have been satisfied.

c. In case of finding a lack of independence for the principle, the finding is captured and addressed via the ASA process.

M.3.2.2.4 CMA as Part of the ASA - Outputs

The results of the CMA supporting the ASA process may be captured similar to the example CMA evaluation table in Table M2. The output of a Verification Phase CMA include feedback to the ASA process covering:

a. List of Independence Principles and independence requirements analyzed.

b. Rationale supporting independence of each Independence Principle for each relevant checklist concern area.

c. Problems/concerns identified during the analysis, as applicable.

d. Reference to information, drawings, and support material used in the analysis.

e. Conclusion/result of the CMA supporting the ASA.

M.3.3 CMA Performed for System Level

This section describes the activities of a CMA supporting PSSA and SSA. It is applicable to the Development Phase where the focus of the CMA is to evaluate the planned development and planned implementation with respect to the allocated Independence Principles (the relationship between Independence Principles and independence requirements is discussed in Section M.1). It is also applicable to the verification phase where the focus of the CMA is to evaluate the implementation with respect to the allocated Independence Principles.

The usage of CMA within the assignment of development assurance levels with architecture considerations is described in Appendix P.

M.3.3.1 Development Phase CMA as Part of a PSSA

Development Phase CMA activities may be performed to support independence assessment as part of the PSSA process. This section discusses the inputs, CMA questionnaire development and application and PSSA CMA result output.

M.3.3.1.1 CMA as Part of a PSSA - Inputs

The inputs needed to perform the Development Phase PSSA CMA include:

a. CMA questionnaire examples (Table M1).

b. Independence Principles (and associated rationale) identified by the PSSA, including any project level Independence Principles coming from the other sources or experience.

c. Characteristics intended to eliminate or reduce sources of common causes. Examples of these mitigations may include planned diversity, planned segregation, isolation, or barriers. Some of these mitigations will already be known or planned, but it is the task of the CMA, during the PSSA phase, to help define the need for other mitigations.

The analyst needs to be familiar with and understand the proposed system architecture characteristics with regard to development implementation and operation. In addition, specific architecture requirements including constraints that were needed at the higher level to support the PASA or high-level PSSAs should be understood.

SAENORM.COM : Click to view the full PDF of arp4761a

These proposed characteristics of the system may be included in:

a. Project planning and development information.

b. System, equipment and/or associated item specifications (requirements documentation).

c. Design architecture descriptions.

d. Item design descriptions.

Also, the analyst may use the following system-level information from the PSSA:

a. Common cause sources to be considered during the PSSA process.

b. Requirements associated with physical failure Independence Principles identified in the PSSA. This includes identified separation or segregation requirements.

M.3.3.1.2 CMA as Part of a PSSA - Tailor the Generic Questionnaire

There are a large number of recurring concerns regarding common cause failures throughout a broad spectrum of designs (e.g., electrical supply, data-bus, common processor modules). Such concerns, derived from the generic CMA questionnaire provided in Table M1, may be addressed across all development projects and/or tailored to suit the particular project under consideration. For example, there is no need to consider areas relating to software when it is clearly not appropriate; such as mechanical-only system.

Project-specific CMA questionnaires are derived based on the generic CMA questionnaire given in Table M1 and previous experience, such as common knowledge or experience in similar aircraft (e.g., lessons learned). The level of detail of these questionnaires depends upon the level of complexity or novelty of the technology or system under study. The questionnaire is adapted to the level of analysis (aircraft or system or subsystem). It should be emphasized that while Table M1 provides an initial starting point, it is not necessarily exhaustive. The analyst should therefore consider other potential common cause sources that may be able to defeat assumed independence in the particular project under consideration since these are not already included in the example evaluation questions of Table M1. Particular attention should be paid to new technologies, processes or methodologies.

M.3.3.1.3 CMA as Part of a PSSA - Process

Once the project-specific CMA questionnaire is complete, each Independence Principle is evaluated in an appropriate format, against the common cause sources to create a descriptive narrative, which identifies concerns and mitigations. Results of the CMA such as the example information shown in Table M2 are used by the PSSA process to develop the necessary independence requirements.

For each CMA Independence Principle identified, the following CMA steps are performed:

a. Apply the questionnaire to determine any lack of independence for the principle due to potential common cause failures or error sources.

b. Analyze each potential common cause source; identify resulting failure effects of the common cause source and describe the planned mitigations to substantiate that the independence criteria will be met.

c. In case of finding a lack of independence for the principle, the finding is captured and addressed via the PSSA process.

Potential independence deficiencies are identified using CMA. The PSSA process acts on these deficiencies by identifying additional mitigation strategies or passing corrective action (creation/correction of Independence Principles) needs to the development process.

Independence requirements are developed as part of the PSSA process using the output of the CMA.

SAENORM.COM : Click to view the full PDF of arp4761a

M.3.3.1.3.1 CMA as part of a PSSA - FDAL or IDAL Assignment

The process in terms of FDAL or IDAL assignment examination is very similar to that discussed in M.3.2.1.3. The difference is that for FDAL or IDAL assignment examination, the activities focus on identification of potential error sources (rather than failures) within the development/ design process that may defeat the intended independence of functions and items.

Note that when performing CMA as part of development assurance level assignment, the emphasis is on examination that there is adequate functional independence and/or adequate item development independence, as applicable within the development process, to satisfy the development assurance level assignment (see Appendix P).

M.3.3.1.4 CMA as Part of a PSSA - Outputs

The outputs of a Development Phase CMA supporting the PSSA include the following:

a. Project-specific CMA questionnaire.

b. Feedback to the PSSA process covering:

    1. Evaluation of each Independence Principle.

    2. Any potential independence deficiencies identified.

    3. Any assumptions made in accomplishing the CMA.

    4. Reference to information, drawings, and support material used in the analysis.

M.3.3.2 Verification Phase CMA as Part of an SSA

Verification Phase CMA activities may be performed to support assessment of independence as part of the SSA process.

M.3.3.2.1 CMA as Part of an SSA - Inputs

The inputs needed to perform the Verification Phase CMA as part of the SSA process:

a. The project-specific CMA questionnaire developed during the Development Phase PSSA CMA activities and any further relevant developments that may have emerged during the implementation process.

b. All Independence Principles (including any that may have emerged during the implementation process).

c. Independence requirements identified during the PSSA process.

d. Design implementation information.

M.3.3.2.2 CMA as Part of an SSA - Gather Design Implementation Information

In the verification phase, the focus of CMA is to ensure that the appropriate Independence Principles and requirements (and hence objectives and characteristics) have been accomplished in the implementation such that the effects of common cause errors and common cause failures have been adequately mitigated. The analyst needs to know and understand the subject system characteristics with regard to system development, implementation, operation and installation. These system characteristics may include:

a. Design architecture.

b. Installation data (may be related to ZSA which considers a particular zone).

c. Equipment and component characteristics.

d. Software design characteristics (e.g., partitioning).

SAENORM.COM : Click to view the full PDF of arp4761a

e. Maintenance and test tasks.

f. Systems, equipment and item specifications (requirements).

g. Equipment implementation data.

Also, the analyst may need to know (or capture assumptions about) the following aircraft-level information:

a. Interdependence analysis results.

b. Function list along with any independence claims to support the FDAL and IDAL assignment.

c. Multifunction and Multisystem analysis results that identifies the following:

1. How system functional failures combine to lead to the considered aircraft failure condition.

2. What availability and integrity requirements/probability allocations to systems are necessary in order to meet safety objectives associated to the aircraft-level failure condition severities expressed numerically (e.g., 1.0E-07) or qualitatively (e.g., Remote).

3. Whether functional Independence Principles and physical segregation/separation requirements are adequately identified for systems whose failures combine to produce an aircraft-level failure condition.

d. Common resource considerations results (List of common resources that can violate independence of systems).

Additionally, the analyst interfaces with the design team to become aware of mitigation characteristics utilized to eliminate or reduce sources of common causes. Examples of these mitigations may include:

a. Diversity.

b. Redundancy.

c. Barriers.

d. Testing.

e. Preventive maintenance programs.

f. Design control and design quality level (FDAL application).

g. Independent review of procedures, processes, and specifications.

h. Training of personnel.

i. Quality control.

M.3.3.2.3 CMA as Part of an SSA - Examination of the Implementation

The verification phase system-level CMA activities are based on analyzing the aspects of the implementation that may defeat the intended independence of functions as detailed in specific Independence Principles and allocated independence requirements. The project-specific CMA questionnaire developed during the Development Phase PSSA CMA activities is reviewed and updated as necessary, considering the general CMA concerns of Table M1 and any new concerns that may have arisen during the development. At this point, the questionnaire becomes a “final” SSA checklist which is then applied to the Independence Principles of interest.

SAENORM.COM : Click to view the full PDF of arp4761a

For each Independence Principle identified, the following CMA steps are performed:

a. Apply the checklist to determine the potential sources of common cause failures/errors associated with each source.

b. Analyze each potential source and resulting common cause failures/errors to substantiate whether the independence requirements (e.g., FDAL/IDAL assignments, installations) have been satisfied.

c. In case of finding a lack of independence for the principle, the finding is captured and addressed by the SSA process.

M.3.3.2.4 CMA as Part of an SSA - Outputs

The results of the CMA supporting the SSA process may be captured similar to the example CMA evaluation table in Table M2. The output of a Verification Phase CMA include feedback to the SSA process covering:

a. List of Independence Principles and independence requirements analyzed.

b. Rationale supporting independence of each Independence Principle for each relevant checklist concern area.

c. Problems/concerns identified during the analysis as applicable.

d. Reference to information, drawings, and support material used in the analysis.

e. Conclusion/result of CMA supporting the SSA.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX N - MODEL-BASED SAFETY ANALYSIS (MBSA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

N.1 INTRODUCTION 292
N.1.1 Model Based Safety Analysis Methodology Overview 292
N.1.2 Role of MBSA in Safety Assessment Process - MBSA Application Context 293
N.1.3 Advantages of MBSA 294
N.1.4 Limitations of MBSA 295

N.2 ELEMENTS OF MBSA METHODOLOGY 295
N.2.1 MBSA Model Elements 295
N.2.2 MBSA Inputs and Outputs 298

N.3 MBSA PROCESS STEPS 302
N.3.1 Gather System Data 302
N.3.2 Define the Goal and the Granularity of the Analysis 302
N.3.3 Define the Failure Conditions to be Studied 303
N.3.4 Build the Failure Propagation Model 303
N.3.5 Build the Failure Condition Logic 304
N.3.6 Verification of the Failure Propagation Model and Failure Condition Logic 304
N.3.7 Failure Condition Evaluation and Analysis 304

N.4 MBSA OUTPUT GENERATION METHODS 304
N.4.1 Algorithm 1: Deductive MBSA Approach (Back-Fault-Propagation) 304
N.4.2 Algorithm 2: Inductive MBSA Approach (Forward-Fault-Propagation) 305

N.5 DOCUMENTATION EXPECTATIONS 305

N.6 MBSA EXAMPLES 305
N.6.1 Simple MBSA Example 305
N.6.2 More Complex MBSA Example 312

N.7 POTENTIAL MBSA SERVICES BASED ON RELATIONSHIPS COMPUTATIONS AND DISPLAY 318
N.7.1 Display of Function and Architecture Dependencies 318
N.7.2 Links Between Functional Safety Requirements and Faults/Failures and Change Impact Analysis 319
N.7.3 Fault Propagation Net Computation and FMES Derivation 319

Figure N1 Classic safety analysis approach 292
Figure N2 MBSA approach 293
Figure N3 MBSA model equipment/functional block elements 296
Figure N4 MBSA equipment/functional block element using state charts example 297
Figure N5 Elements, inputs, and outputs of MBSA 301
Figure N6 MBSA example, circuit 306
Figure N7 MBSA example, FPM 306
Figure N8 Battery equipment/functional block 306
Figure N9 Electrical distribution equipment/functional block 307
Figure N10 Dual contact switch equipment/functional block 307
Figure N11 Electrical <<OR>> equipment/functional block 308
Figure N12 Lamp equipment/functional block 308
Figure N13 Top failure condition example 311
Figure N14 Next level of failure condition example 311
Figure N15 MBSA complex example, control system 312

SAENORM.COM : Click to view the full PDF of arp4761a

Figure N16 Engine equipment/functional block 313
Figure N17 Power supply equipment/functional block 313
Figure N18 Computer equipment/functional block 314
Figure N19 Voter equipment/functional block 314
Figure N20 Switching equipment/functional block 315
Figure N21 Top failure condition FC2 deductive Boolean function 317
Figure N22 Next level of failure condition example 317
Figure N23 FC1 cut set example 318
Figure N24 FC2 cut set example 318
Figure N25 Focused functions/architecture dependency example 319
Figure N26 Focused fault propagation graph example 320

Table N1 Sample of cut set traces leading to a Failure Condition (Lamp:Out = “off”) 310
Table N2 Sample of cut set traces leading to two failure conditions (Switch.Loss = True, Switch.MisLead = False) 316
Table N3 Sample of cut set traces leading to two failure conditions (Switch.Loss = False, Switch.MisLead = True) 316

SAENORM.COM : Click to view the full PDF of arp4761a

N.1 INTRODUCTION

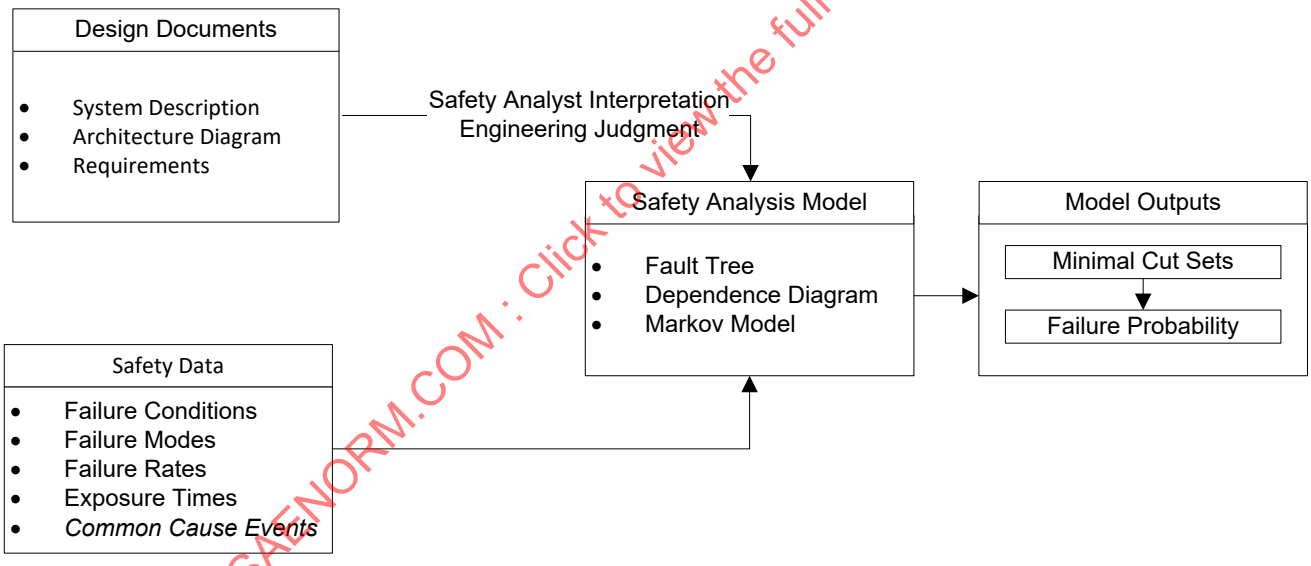
This appendix provides an overview of the concepts and processes associated with performing a safety analysis using Failure Propagation Models (FPMs). Within this appendix this analysis concept is referred to as Model-Based Safety Analysis (MBSA)

NOTE: MBSA is a generic term for a family of techniques and methods based on an FPM. MBSA described in this appendix may be used to replace the Fault Tree Analysis (FTA), Markov Analysis (MA), or Dependence Diagram (DD) analyses, and may also help inform the Common Mode Analysis (CMA), Particular Risk Analysis (PRA), Zonal Safety Analysis (ZSA), and Cascading Effects Analysis (CEA). Other MBSA may be developed for performing other aspects of an overall safety assessment. The methods described in this MBSA appendix are not dependent on Model-Based System Engineering (MBSE) development processes and are written generally for use with any structured development processes, whether traditional text-based requirements or MBSE processes. There exist a variety of modeling languages and methods. This appendix is deliberately technology neutral, and does not provide technology-specific guidelines

N.1.1 Model Based Safety Analysis Methodology Overview

Performing the safety assessment of a design consists of understanding the system content and behavior to provide safety analysis results that are compared to safety objectives/requirements.

In order to understand system behavior, the safety analyst interprets design data and clarifies the design information in discussions with the designers to develop an FPM.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure N1 - Classic safety analysis approach

In the classic safety assessment approach (Figure N1), the safety analyst uses the acquired understanding to manually construct fault trees or other safety analysis artifacts (e.g., MA, DD) to calculate minimal cut sets and failure probabilities. The MBSA methodology (Figure N2) achieves results (minimal cut sets, failure sequences, and failure probabilities) that are equivalent to those obtained from the classical (e.g., FTA) safety analysis methods.

In the MBSA approach, the safety process captures, using a modeling language, the architecture, failure mode models, safety-relevant functional behavior (e.g., reconfigurations, monitoring), failure condition (FC) description, and possibly additional data depending on the analysis objective. Such a model, called the “failure propagation model” represents the system architecture and its dysfunctional behavior. The FPM is then analyzed using a suitable computational tool set to generate outputs such as failure sequences, minimal cut sets, or other results. These outputs may then be compared with the system safety requirements as for the classical safety analysis methods.

The model interpretations or clarifications must be rolled back into the development for consistency and maintained when the model is used for the safety analysis of the system.

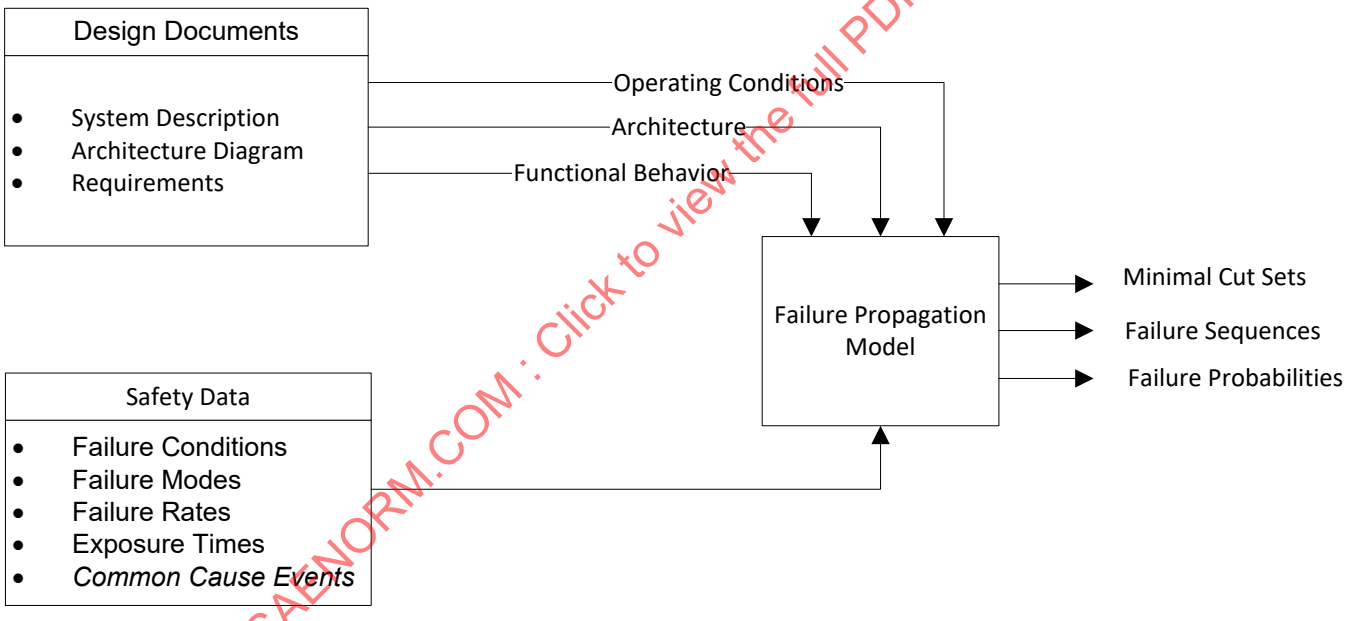
The overall goals of MBSA, similar to other methods, are to:

a. Support safety analysis of a function and/or architecture by creating representative failure models of the system.

b. Help address the complexity of functions and systems.

c. Establish a common communication mechanism between designer and safety analyst.

The MBSA methodology may vary due to the type and capability of the system modeling languages, the extent to which nominal behavior is captured and the range of output results. These variants allow the methodology to be adapted to different scopes of analysis and varying complexity/detail of the systems being modeled.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure N2 - MBSA approach

N.1.2 Role of MBSA in Safety Assessment Process - MBSA Application Context

The role of MBSA in the overall safety assessment process is to support the Preliminary Aircraft Safety Assessment (PASA), Preliminary System Safety Assessment (PSSA), System Safety Assessment (SSA), and Aircraft Safety Assessment (ASA) processes. The primary use of MBSA is to generate Functional Failure Sets (FFS) and/or minimal cut sets for a specific failure condition. MBSA use will normally occur early in a program during the preliminary stage of system design, and then again in later phases of a program when implementation details are available. The MBSA approach used during the complete development cycle is iterative, hierarchical, and progressive in detail.

The following information is required to construct the FPM (see N.2.2 for minimum inputs associated with each analysis).

a. Architecture definitions.

b. Links between the equipment/functional blocks.

c. Flows (signal path) inside the links.

d. Events (e.g., failures or reconfiguration mechanisms) that lead to output flow changes.

MBSA results may be applied to:

a. Influence timely architecture/design decisions via PASA and PSSA.

b. Verify safety objectives via SSA, ASA, and other safety processes.

c. Support the data rollback with the system design (architecture, requirements, etc.) in order to keep MBSA model synchronized with the system definition.

MBSA can also be used to support the common cause methods (CMA, PRA, and ZSA). MBSA provides FFS and/or MCS, which then may be used to identify common cause potentials for events and independence assumptions. MBSA supports visualizing the effects of multiple common cause events through simulation and can help the designer and safety analyst assess the effects via fault injection.

N.1.3 Advantages of MBSA

Some advantages afforded through use of MBSA techniques include:

a. The FPM enhances communication/coordination/synchronization between the system design process and the safety assessment process:

    1. The FPM facilitates understanding of system behaviors by having the FPM accurately represent the actual system architecture and system operations.

    2. The FPM supports simulation of combined functional and failure behavior.

b. The FPM facilitates the ability to manage design changes to the subsequently developed safety analyses and analysis results.

c. Analyses can be repeated if a model changes or if additional failure conditions are identified.

d. Multiple failure conditions can be analyzed consistently and efficiently using the same FPM.

e. More complex systems (together with their reconfiguration modes) can be analyzed as a result of the MBSA tool's ability to exhaustively identify all combinations of failures that result in the failure conditions from the FPM.

f. The FPM supports reconfiguration modeling.

NOTE: The usage of a formal language and the simulation of the behavior (functional and dysfunctional) of the system lead to request more information to the designer. See the example appendix where some questions are raised.

SAENORM.COM : Click to view the full PDF of arp4761a

N.1.4 Limitations of MBSA

Some limitations associated with the use of MBSA techniques include:

a. When starting with a failure condition, the required level of completeness (as expected from FTA), granularity, and abstraction for model development may not be obvious. This “uncertainty” in required model-detail can complicate the model development process.

b. The additional task for confirming the correctness of a model should be assured using techniques such as simulation, formal analysis, and syntax/semantic checks.

c. MBSA relies on the analytical models being constructed to the appropriate level of abstraction. The system may need to be modeled at different levels of abstraction to support different levels of analysis. The consistency of models at different levels needs to be assured.

d. It could be difficult to represent complicated failure condition observers in an FPM.

e. There are potential scalability issues if a model is not developed to the right level of abstraction. This could affect the verification of the model.

N.2 ELEMENTS OF MBSA METHODOLOGY

The MBSA method allows for the analysis of a complex system by associating a system’s safety concerns with the system’s functionality, as shown in Figures N2 and N3. MBSA provides increasing benefits as a program progresses from early stages to later stages of development. During early stages of a program where the granularity of data is at a high-level or the architecture data is limited, MBSA outputs may be suitable for PASA and PSSA. During later stages of a program where more systems data are available, MBSA outputs may be suitable for ASA, SSA, and possibly common causes.

The main elements of the MBSA method that enable the analyst to execute the analysis are described in the following sub-sections. Note that the configuration of the MBSA models need to be managed and correlated to the system configuration analyzed so that their applicability is appropriate and the models are not misused for analyzing systems with different configurations

N.2.1 MBSA Model Elements

The MBSA method differs from the other safety analysis methods by how the analyst models the system. The safety analyst first uses the function list, considered in the Aircraft Functional Hazard Assessment (AFHA)/PASA/System Functional Hazard Assessment (SFHA), as a guide to influence the boundaries of the FPM under construction. Once the FPM boundaries are defined, a preliminary list of failures modes (generic common failure modes derived from experience or engineering assumptions) or an actual list of failure modes—based on the Failure Mode and Effect Analysis (FMEA) or the Failure Mode and Effect Summary (FMES) input—is used to define the equipment/functional blocks, and the system architecture is used to interconnect the blocks to form a complete FPM. The equipment/functional block modules consist of events, states, inputs/outputs (I/O), and transfer functions. Figure N3 shows the MBSA model equipment/functional block elements.

N.2.1.1 Failure Propagation Model (FPM)

The FPM represents the system architecture and its dysfunctional behavior. The key driver of the FPM definition is the analysis type (e.g., PASA, PSSA, ASA, SSA) being supported. The model should represent the system nominal design (from a safety point of view) and failure behavior, maturity of the design, and assumptions on failure independence. The granularity, i.e., the level of the elementary events, of the model is mainly driven by the analysis type. Depending on the analysis type, the safety analyst defines the boundaries of the FPM and determines to what extent the MBSA Inputs are used to define the FPM.

SAENORM.COM : Click to view the full PDF of arp4761a

The FPM describes:

a. The relationship between the inputs and outputs of the elements in a nominal situation.

b. The failure events with their occurrence conditions (based on input data and failure mode) and their effects on outputs.

c. The links between elements according to the system architecture.

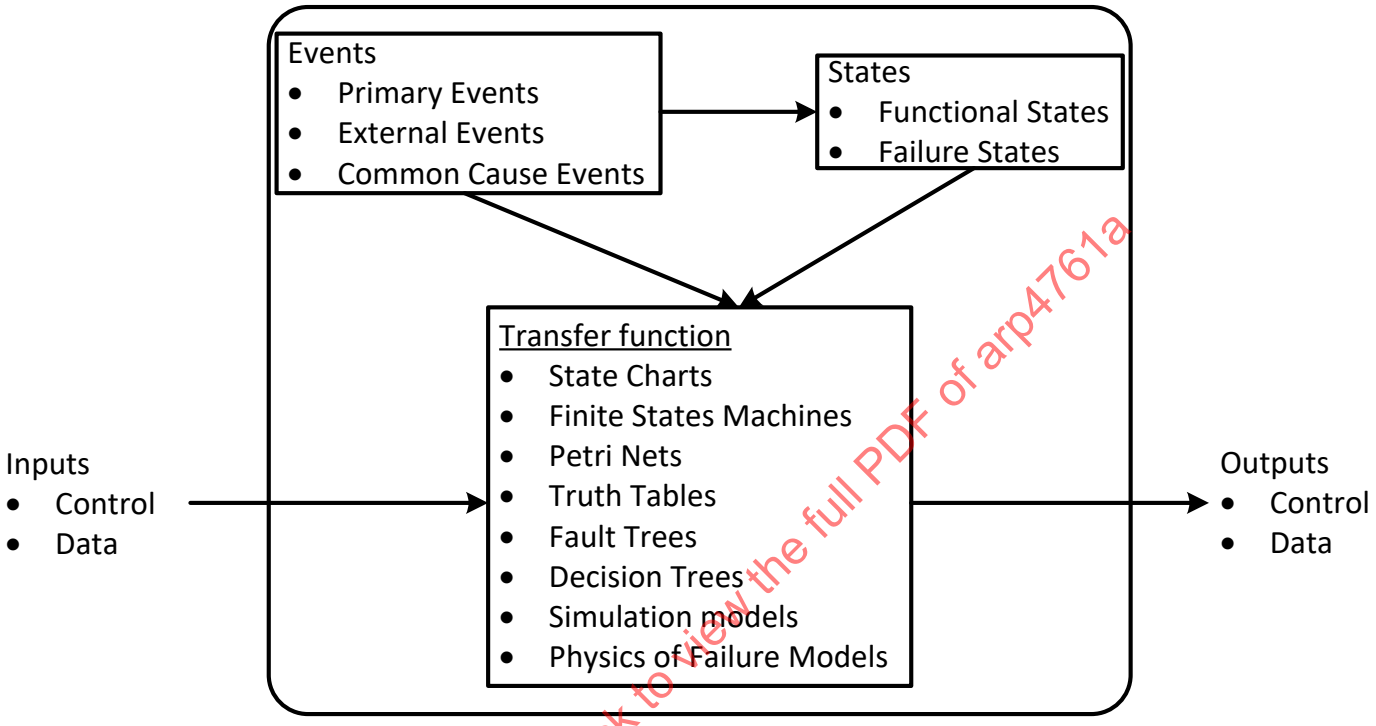


Figure N3 - MBSA model equipment/functional block elements

N.2.1.2 FPM Equipment/Functional Block

An FPM equipment/functional block model is composed of inputs/outputs, events, states, and transfer functions. Each of these model elements are described in N.2.1.2.1 through N.2.1.2.2.

Figure N4 provides an example of an MBSA equipment/functional block element. In this model example, HYD_IN (hydraulic pressure input) and SV_CDE (shutoff valve condition) are the model inputs with HYD_OUT (hydraulic pressure out) as the model output.

N.2.1.2.1 Block Input/Output (I/O)

The block I/O is the input and output data being manipulated within the equipment/functional block.

SAENORM.COM : Click to view the full PDF of arp4761a

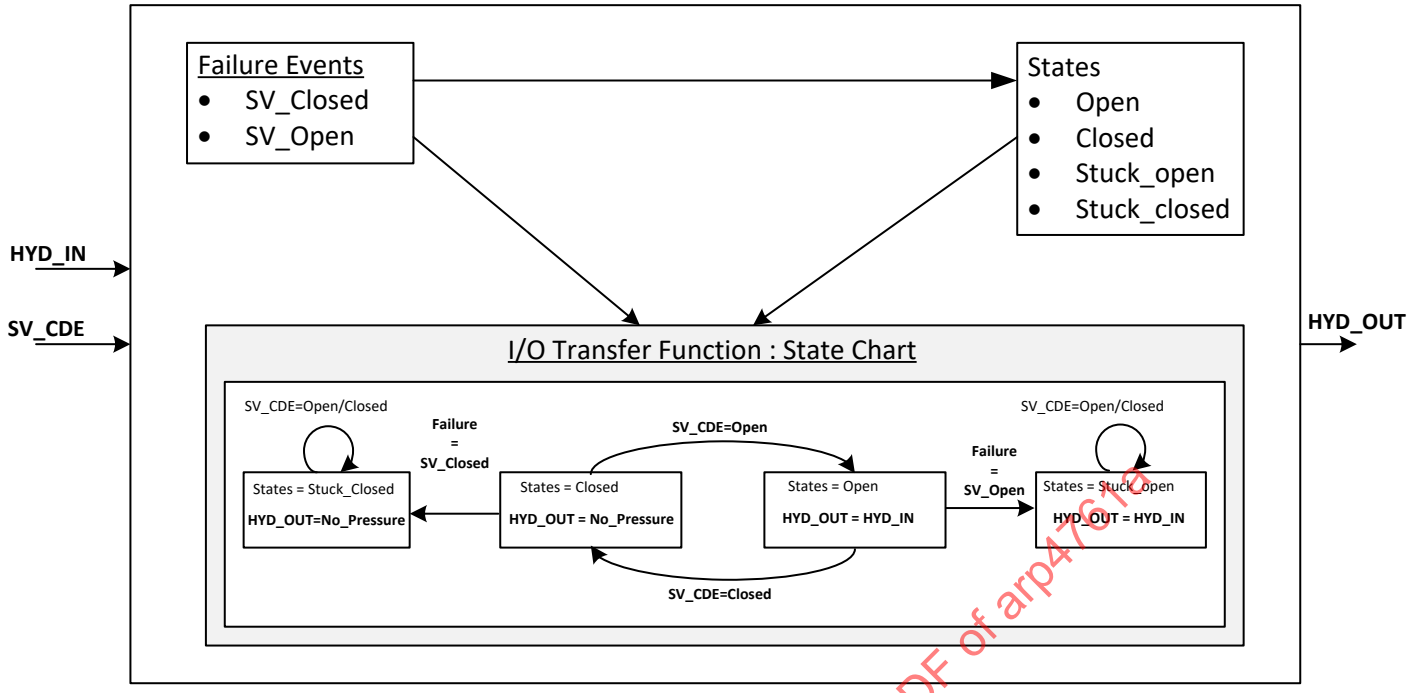


Figure N4 - MBSA equipment/functional block element using state charts example

N.2.1.2.2 Equipment/Functional Block Events, States, and Transfer Functions

a. Equipment/functional block events:

The equipment/functional block events can be based on a preliminary list of failures modes (e.g., common failure modes derived from experience or engineering assumptions) in early stages of the development process and/or directly defined by actual list of failure modes (FMEA or FMES input). As mentioned previously, the construction of an FPM is dependent on the analysis type. The granularity of the FPM event definition is one of the areas where the impact is noted since the level is directly determined by the analysis type. Equipment/functional block events can be:

1. Primary events that result from logic outcomes within the FPM model being defined such as normal designed system states.

2. External events originating from outside the defined boundaries of the FPM model being defined.

3. Common cause events or by system logic flows for the FPM equipment/functional blocks being defined in the FPM.

b. Equipment/functional block states:

The equipment/functional block states are also directly impacted by the analysis type similar to the equipment/functional block events. The equipment/functional block state transitions are triggered by events. The equipment/functional block states are categorized as:

1. Functional states: Based on the function definitions of the system.

2. Failure states: Based on the FMEA conditions and function failures defined in the system design document.

c. Equipment/functional block transfer functions:

The equipment/functional block transfer function determines the output based on the inputs and the equipment/functional block states.

SAENORM.COM : Click to view the full PDF of arp4761a

N.2.1.3 Failure Condition Observer

The failure condition observer is a key feature within the model that indicates when the FPM satisfies the defined failure condition logic. The failure condition observer formalizes the definition of the selected failure conditions (from the AFHA or SFHA, whichever is appropriate) and translates them into a formula based on system states, inputs and logic of relevant equipment/functional blocks.

N.2.2 MBSA Inputs and Outputs

MBSA uses similar inputs to other safety analysis methods (e.g., FTA, DD, and MA) but may also start from the system design model. The outputs of the MBSA method are similar to those produced by the other analysis methods outlined in this guideline. MBSA progresses from early stages to later stages of development. Depending on the phase of the program, the different analyses supported by MBSA (e.g., PASA, PSSA, ASA, SSA), have different required inputs. The inputs may be included in the same or different tool used by the FPM. The inputs, outputs, and details of how they are used in the MBSA process are illustrated in Figure N5.

N.2.1 describes “core” information for MBSA—data required to build the FPM and generate MCS. “Extension” information for MBSA are data to be added to the core information in order to perform a safety analysis. These safety analyses and associated required data include, but are not limited to:

a. PASA: AFHA/SFHA failure conditions, Independence Principles.

b. PSSA/SSA: failure rates and exposure time.

c. PRA: common cause events.

d. ZSA: zonal attributes.

e. Function Development Assurance Level (FDAL) and Item Development Assurance Level (IDAL) assignment validation supports: FDAL and IDAL attributes.

Inputs and outputs for the various analyses are described in the corresponding section.

N.2.2.1 PASA

The PASA process is a systematic safety analysis of a proposed aircraft architecture. The PASA determines whether the safety objectives associated with each individual aircraft-level failure condition can be satisfied and any necessary associated system safety requirements are derived. The PASA also demonstrates that, for the proposed aircraft architecture, the relationships between functions/systems are acceptable.

PASA has many inputs such as the failure conditions (FCs) from AFHA, SFHA, aircraft functions and architecture, operational conditions, and requirements. The PASA process depends on the Multifunction and Multisystem (MF&MS) analysis and supporting analyses such as Combined Functional Failure Effects (CoFFE) analysis, CEA, and common causes.

The MBSA minimal data inputs to support PASA generally include the following inputs:

a. Functional Flow Block Diagram (FFBD)—the aircraft’s functional logic flow. This is constructed from knowledge of the aircraft architecture and operational assumptions.

b. AFHA/SFHA failure conditions (aircraft or system—depends at which point of the safety analysis process the method is being applied).

c. Functional failure modes—typical functional failure modes derived from experience or engineering assumptions.

SAENORM.COM : Click to view the full PDF of arp4761a

MBSA outputs for PASA may include:

a. Minimal cut sets.

b. Failure probability.

c. Failure sequences.

d. Importance metrics: importance metrics are the sensitivity of the failure condition probability to specific events and failure modes in the MBSA. There are many such metrics such as Birnbaum and Fussell-Vesely; they can be obtained by post-processing the cut sets using a numerical probability analysis computation.

Note that MCS and failure sequences which result in the failure condition under analysis (from AFHA) are primary outputs of MBSA. MCS for functional failures such as in multifunction analysis are also called FFS and are useful for FDAL assignments and deriving Independence Principles. MBSA simulation capability can also be used to support CoFFE, CEA, CMA, ZSA, and PRA.

N.2.2.2 PSSA

The MBSA minimal data inputs to support PSSA include:

a. System FFBD—the system's functional logic flow.

b. System FHA failure conditions.

c. Failure modes—typical functional failure modes derived from experience, engineering assumptions, or FMEA/FMES.

d. Failure rates, exposure times, "at risk" times, latent intervals, failure rate budgets during the early stage of the development process.

MBSA outputs for PSSA may include:

Minimal cut sets and failure sequences as described for PASA.

b. Failure probabilities: Calculated probabilities of the MCS, failure sequences, and the failure conditions. This output is generated by a numerical probability analysis engine as a post-processor of the MBSA outputs.

c. Importance metrics: Importance metrics are the sensitivity of the failure condition probability to specific events and failure modes in the MBSA. There are many such metrics such as Birnbaum and Fussell-Vesely; they can be obtained by post-processing the cut sets using a numerical probability analysis computation.

N.2.2.3 ASA, SSA, and Other Analyses

The MBSA inputs to support ASA and SSA may include:

a. Aircraft/system FFBD used for verification.

b. FHA failure conditions used for verification.

c. System design documents—list of architectural features (e.g., hardware, software, interconnections, monitors, indications).

d. Failure modes—specific failure modes directly from FMEA/FMES.

e. Failure rates, exposure times, "at risk" times, latent intervals from FMEA.

SAENORM.COM : Click to view the full PDF of arp4761a

MBSA outputs to support ASA, SSA, and other analyses may include:

a. MCS and failure sequences as described previously.

b. Failure probabilities: Calculated probabilities of the minimal cut sets, failure sequences, and the failure conditions are outputs from MBSA. This output is generated by a numerical probability analysis computation as a post-processor of the MBSA outputs.

c. Importance metrics: Importance metrics are the sensitivity of the failure condition probability to specific events and failure modes in the MBSA. There are many such metrics such as Birnbaum and Fussell-Vesely; they can be obtained by post-processing the cut sets using a numerical probability analysis computation.

N.2.2.4 PRA, ZSA, or FDAL/IDAL Assignment Validation

The inputs to MBSA for PRA, ZSA, and FDAL/IDAL assignment are the inputs required to build the aircraft/system FPM with the appropriate data. The specific data associated with each analysis is identified below:

a. PRA: common cause events.

b. ZSA: zonal attribute of each aircraft/system/equipment.

c. FDAL assignment validation: FDAL attribute.

d. IDAL assignment validation: IDAL attribute.

MBSA outputs for these analyses may include:

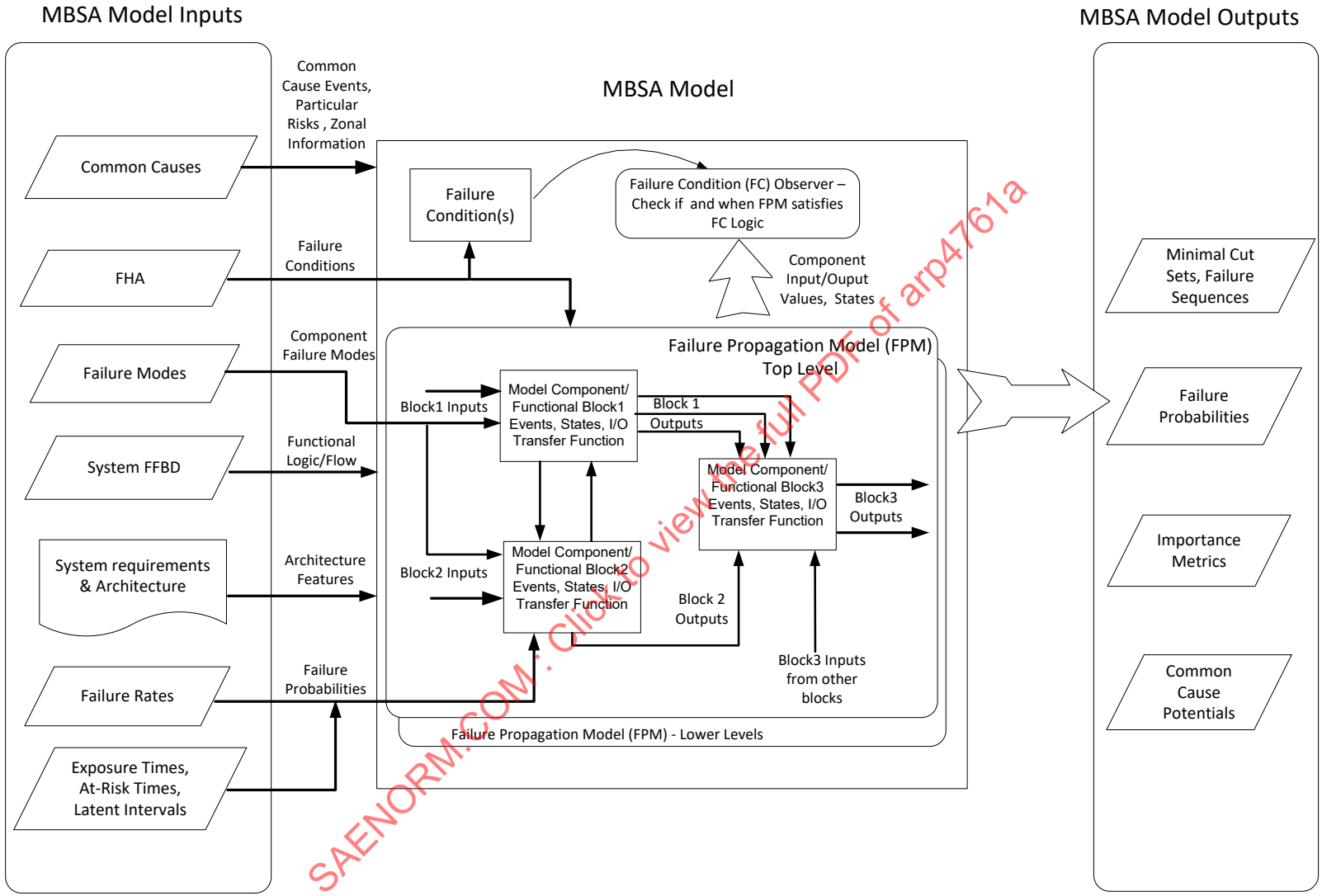
a. MCS and failure sequences as described previously, including common cause events.

b. MCS and failure sequences as described previously composed of zonal, FDAL, and IDAL attributes. The MCS and failure sequences can be obtained by post-processing the cut sets using substitution of the failure events with the corresponding attribute.

c. Common cause potentials. Common cause potentials can be output from MBSA by analyzing the MCS similar to what is accomplished for traditional manual FTA as shown in Appendix G.

Note that a model for FDAL assignment covers high-level functionality while a model used for IDAL, ZSA, or PRA includes items.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure N5 - Elements, inputs, and outputs of MBSA

Note that, depending on the function performed by the blocks, the block's output number may differ. In this schematic, one line may include several flows (this capability is tool dependent).

N.3 MBSA PROCESS STEPS

The following outlines the steps of the MBSA process.

N.3.1 Gather System Data

To initiate the process the analyst gathers the most complete system data available at the stage of the program. As described in the previous sections, the data needed for PASA, PSSA, ASA, SSA, or other analyses includes:

a. System architecture description (from design description documentation or design requirement documentation), including relations between equipment.

b. Equipment/functional block behavior from system hierarchy and block diagrams.

c. Inputs/outputs of the equipment/functional blocks and the equipment connectivity, as would be available in a functional flow block diagram or interface definition.

d. Equipment/functional block failure or malfunction behavior based on preliminary FMEA/FMES.

e. Common cause events to be studied; e.g., particular risks and external events.

f. Zonal information as necessary to model zonal safety aspects related to system zonal implementation.

N.3.2 Define the Goal and the Granularity of the Analysis

The analysis application (PASA, PSSA, ASA, SSA) is the key driver of the FPM definition. The granularity, level and type of the equipment/functional block and I/O, of the FPM is mainly driven by the analysis application. See N.2.2 for MBSA inputs/outputs for each analysis type.

For example, for a PASA, the FPM may have:

a. Initially a few levels of hierarchy, which increase as the design matures

b. Equipment/functional blocks representing:

    1. Initially system functions with possibly:

        i. No hardware or software implementation details.

        ii. Input/output representing functional flow.

        iii. Failure modes representing functional failures.

    2. Hardware and software items, when the individual system designs are refined, with:

        i. I/O representing safety relevant data and messages from an interface definition.

        ii. Common points allowing risks such as electrical wiring interconnect systems (EWIS) to be studied.

SAENORM.COM : Click to view the full PDF of arp4761a

For example, for a PSSA, the FPM may have:

a. One or two levels in hierarchy.

b. Equipment/functional blocks representing system functions with possibly:

    1. No hardware or software item implementation details.

    2. I/O representing functional flow.

    3. Failure modes representing functional failures.

As the design matures, the FPM to perform an SSA may have:

a. Many levels of hierarchy.

b. Equipment/functional blocks representing hardware and software items with:

    1. I/O representing data and messages from an interface definition.

    2. Zonal information representing zonal risks to be studied.

Safety benefits beyond the basic MBSA analyses include PRA, CMA, and ZSA. However, MBSA support for these analyses requires a high-level of detail in aircraft and system definition.

Depending on the analysis type, the analyst defines the boundaries of the FPM as described in N.2.1.

N.3.3 Define the Failure Conditions to be Studied

The failure conditions to be studied can be directly obtained from an AFHA/SFHA or the MBSA objectives can be tied to an input (undeveloped) event of another model/system. The failure condition may have an impact on the FPM definition and granularity, the decomposition level and the failure condition observer logic to be implemented.

As an example, for a PASA analysis the failure conditions may be initially from the aircraft FHA and then, as the design matures, from the different SFHA. For a PSSA or SSA, the failure conditions will be obtained from the System FHA.

N.3.4 Build the Failure Propagation Model

Using collected data, the analyst creates a system functional and “malfunctional” behavior model by:

a. Creating equipment/functional blocks determined by the required FPM granularity given the level of analysis. The equipment/functional blocks may be at the function or component level based on the required granularity. Creating the equipment/functional blocks models requires using an MBSA tool (graphical or textual) which allows the creation of blocks similar to those available in an engineering CAD system. Some MBSA tools may even support importing design schematics into the function blocks. MBSA tools may also allow for the reuse of previously verified equipment/functional blocks. In this case, the creation process for the equipment/functional blocks is skipped.

    As shown in Figure N3, the equipment/functional blocks need additional information such as I/O, events, states, and transfer functions. MBSA methods may support different modeling scenarios based on the transfer function supported by the method. Events and states are created based on nominal functional behavior and failure modes from FMEA/FMES for the different system components. The equipment/functional block creation is completed only after transfer function definition.

b. The analyst then links the equipment/functional block inputs and outputs together to compose the FPM as shown in Figure N3 according to the system architecture. Depending on the abstraction and granularity level, the FPM may not exactly resemble the design schematics. At lower levels in the design process, the FPM will be closer to a design schematic.

SAENORM.COM : Click to view the full PDF of arp4761a

N.3.5 Build the Failure Condition Logic

To analyze a specific hazard from the FHA, the analyst uses the data from the FPM to determine the unique formula to be called the failure condition logic.

The failure condition logic may be a specific failure state of a system output (e.g., erroneous output on display) or may be a specific combination of failure states on multiple system outputs (e.g., loss of outputs on both displays).

N.3.6 Verification of the Failure Propagation Model and Failure Condition Logic

The FPM and the failure condition logic should be verified to assure that the model is representative of the real system architecture behavior. This can be done using a specific set of verification tests that can be reused for each model modification to assure non-regression in the model.

As an example:

a. Verification of each failure mode of a component (from FMEA/FMES process) is used and its impact reflect the system behavior.

b. Verification of the behavior of the FPM can be done by simulation (fault injection) and comparing the model effect with the system effect.

N.3.7 Failure Condition Evaluation and Analysis

The failure condition evaluation and analysis will be based on the outputs generated from the MBSA. These outputs are the minimal cut sets, failure sequences and other results as summarized in Figure N3. These results will be obtained based on the output generation methods (deductive method or inductive method) described in Section N.4, as supported by the MBSA tool. Not all methods described in Section N.4 may be available in all tools. The MBSA tool may make it easier to activate the deductive method or the inductive method such as simulation traces via user interfaces. Simulation results are shown graphically to visualize fault propagations and to verify whether such a failure path is logically possible.

Once minimal cut sets are obtained, the evaluation can be quantitative (i.e., aimed at verifying compliance with quantitative safety objectives) and/or qualitative (e.g., no single failure criteria or common cause/modes identification). The outputs of the MBSA process may be used to support the FDAL/IDAL assignment process, as defined in Appendix P.

N.4 MBSA OUTPUT GENERATION METHODS

There are two main types of algorithms for generating MBSA output: the deductive approach and the inductive approach. Since these approaches may not be as familiar to the safety analyst as classical methods, they are described in more detail in N.4.1 and N.4.2.

N.4.1 Algorithm 1: Deductive MBSA Approach (Back-Fault-Propagation)

This method consists of an exploration of the state space of the model, starting from a representation of the failure condition (the failure condition observer) and proceeding backward along logical paths that lead to the condition. The failure condition observer and the transfer function logic are encoded as logical formulae and may be symbolically manipulated.

The state space exploration starts from a logical formula representing the failure condition observer, and proceeds to identify the downstream components contributing to the observed event. Using the transfer function logic, logical conditions on the outputs of one component are mapped to conditions on the inputs and on the internal state of the component, including local faults. The process is repeated for each input value of the component that has been identified and stops when all downstream components have been processed.

The derivation and the formula manipulation can be implemented using different technologies, such as constraint solving and model checking. Model checking techniques are fully automated and work by performing an exhaustive exploration of the state space of the model.

SAENORM.COM : Click to view the full PDF of arp4761a

N.4.2 Algorithm 2: Inductive MBSA Approach (Forward-Fault-Propagation)

This method consists of an exploration of the state space of the model, starting from the set of basic faults, and combinations thereof, and analyzing their impact on the failure condition observer. This method uses forward fault propagation to carry out the derivation. Similar to the deductive approach, the failure condition observer and the transfer function logic are encoded as logical formulae and may be symbolically manipulated.

The forward-fault-propagation method is used to generate cut sets. The state space exploration starts from the set of admissible initial states of the model and the set of basic faults; it analyzes the reachable states of the system. A reachable state satisfying the failure condition observer corresponds to a cut set comprising all of the basic faults that are active along the trace linking an initial state with the state satisfying the failure condition observer.

The derivation and the formula manipulation can be implemented using different technologies. In addition to the technologies used for the deductive approach, simulation techniques can be used. Simulation techniques typically analyze one trace at a time. Different traces to be analyzed are chosen, as representatives of different failure combinations, and the analysis is repeated for each trace. In general, the order of occurrence of each fault in a fault combination may be relevant. For this reason, simulation techniques may be inefficient, when the set of faults, and consequently the set of traces to be analyzed, is very large. Simulation techniques are inherently incomplete (the analysis may miss cut sets) when the set of traces to be analyzed is very large. For efficiency reasons, it is possible to limit the analysis to cut sets of a maximum order (i.e., applying cardinality). The set of cut sets extracted during the analysis may be minimized to derive the set of minimal cut sets. Similar to the deductive approach, model checking techniques can be used to perform an exhaustive exploration of the state space of the model.

Quantitative evaluation of the generated minimal cut sets, for both the deductive and the inductive approach, can be performed using standard Boolean evaluation engines, or by using the standard sum-of-product rules of probabilities. Efficient evaluation engines exist which use binary decision diagrams to manipulate logical formulae representing probabilities.

N.5 DOCUMENTATION EXPECTATIONS

When one uses MBSA, the safety documentation (e.g., PASA, PSSA, ASA, SSA) should include:

a. A list of the tool(s) used, instructions for use, and all the necessary additional information to reproduce the results.

b. The configuration of the MBSA (including models and tools) baseline used to generate the results.

c. Relevant data and checklists supporting the “model to results.”

d. The list of all the failure modes captured in the model with all their characteristics (e.g., failure behavior, parameters, latency period).

e. Results of the MBSA including minimal cut sets, failure sequences, probabilities.

f. Summary of the model validation results and acknowledged limitations of the model (to guide usage as intended and avoid future misuse) with reference to any further data needed for the model validation.

N.6 MBSA EXAMPLES

Two examples are provided. A simple example and a more complex example. Objectives of these examples are not to perform a complete safety analysis using a model including all component failure modes but to explain how to create a comprehensive model, and to understand the methodology.

N.6.1 Simple MBSA Example

The MBSA example, shown in Figure N6, models a system for turning on a lamp when a dual contact switch is closed. The intent is to show the FPM, the elements involved in building the model and the analysis. The battery (1) provides power to two redundant stages of a switch (3) that commute the power for the monitoring lamp (5).

SAENORM.COM : Click to view the full PDF of arp4761a

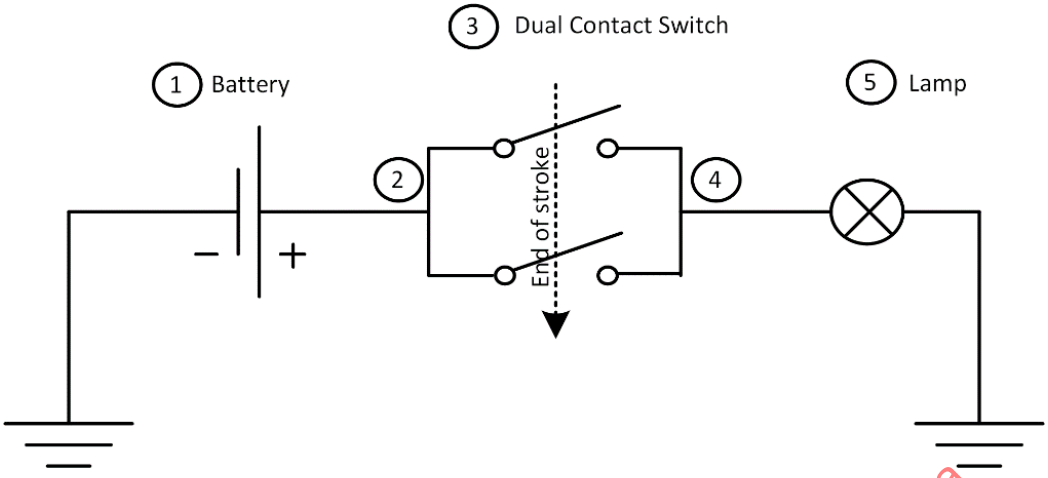


Figure N6 - MBSA example, circuit

The MBSA FPM for this system is shown in Figure N7. The MBSA simple model does not consider wiring open and short circuit failures.

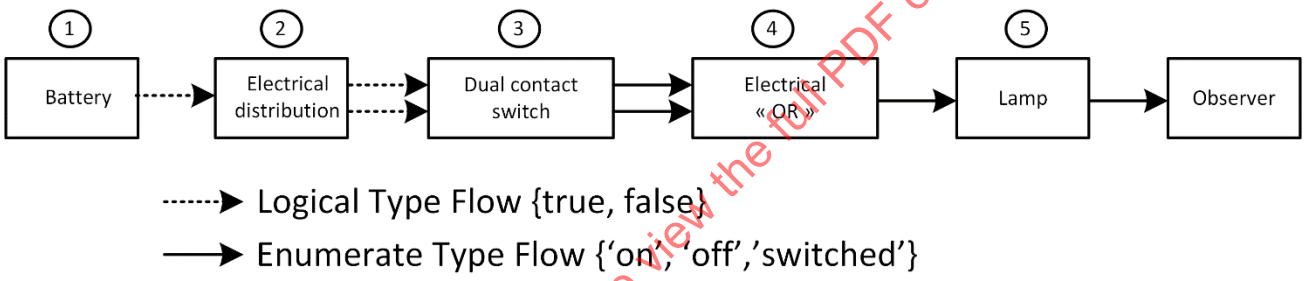


Figure N7 - MBSA example, FPM

Equipment/functional blocks for the example FPM are as shown in the Figures N8 through N12.

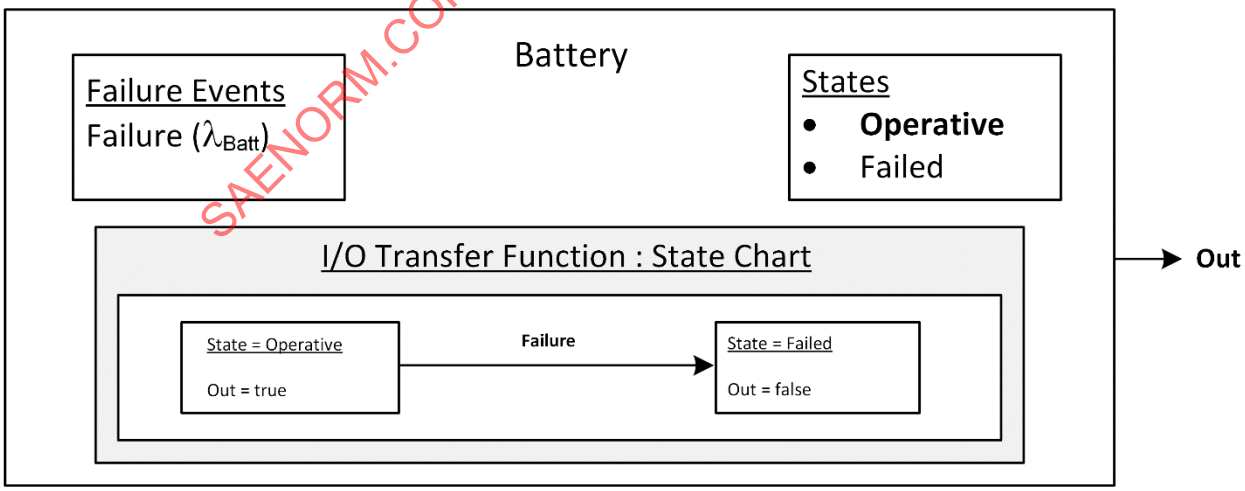


Figure N8 - Battery equipment/functional block

SAENORM.COM : Click to view the full PDF of arp4761a

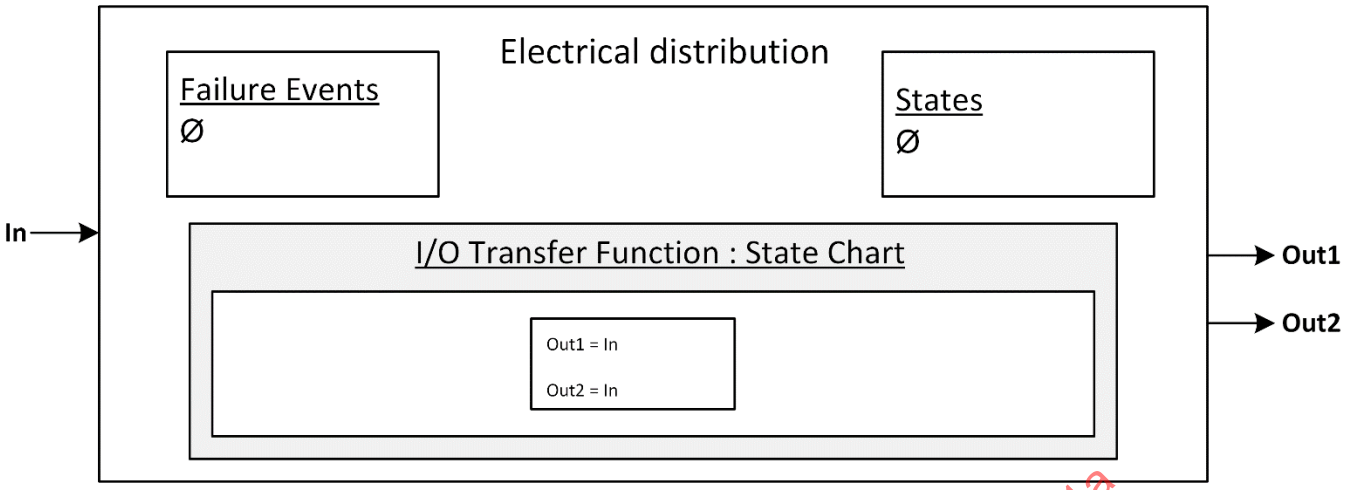
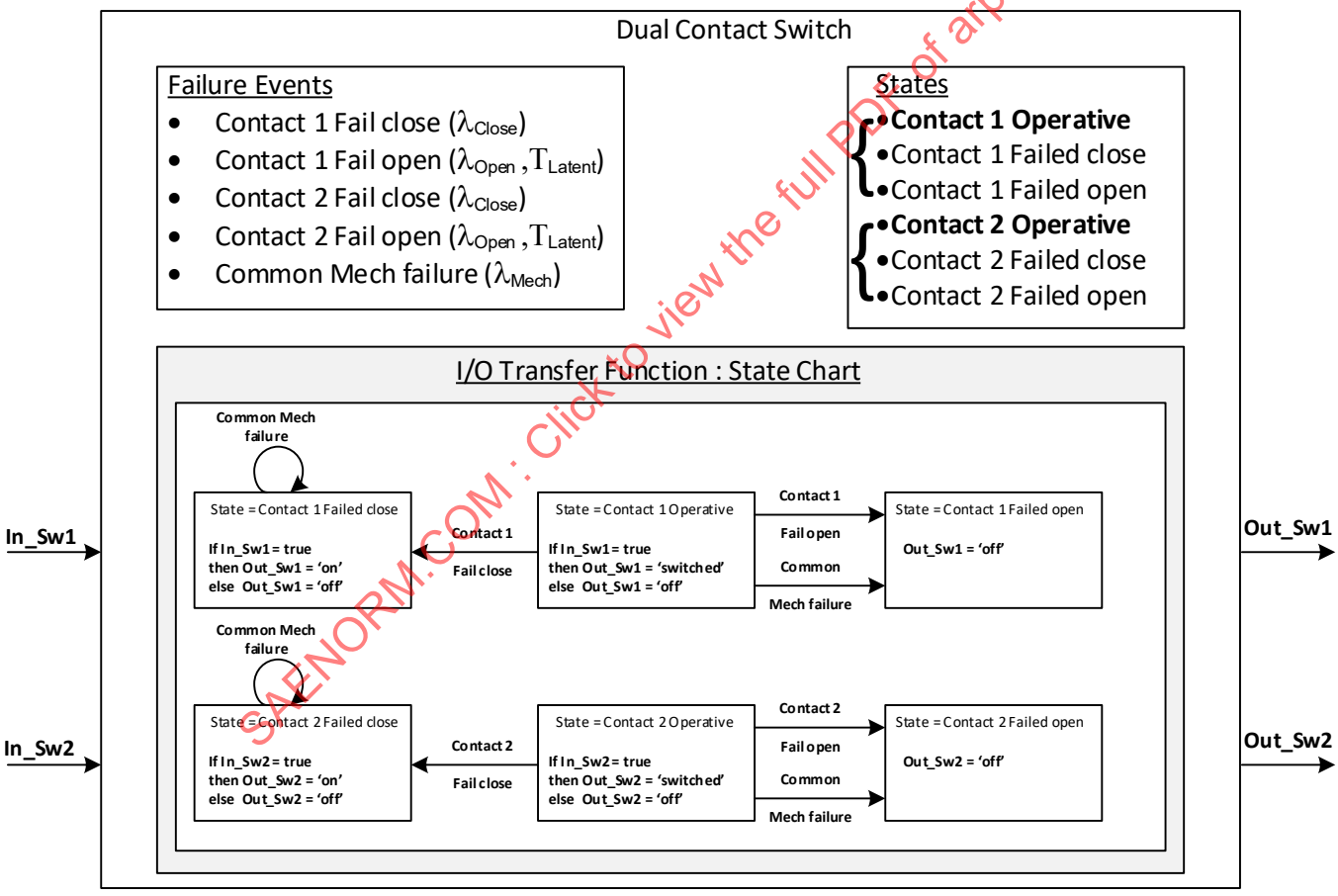


Figure N9 - Electrical distribution equipment/functional block



SAENORM.COM : Click to view the full PDF of arp4761a

Figure N10 - Dual contact switch equipment/functional block

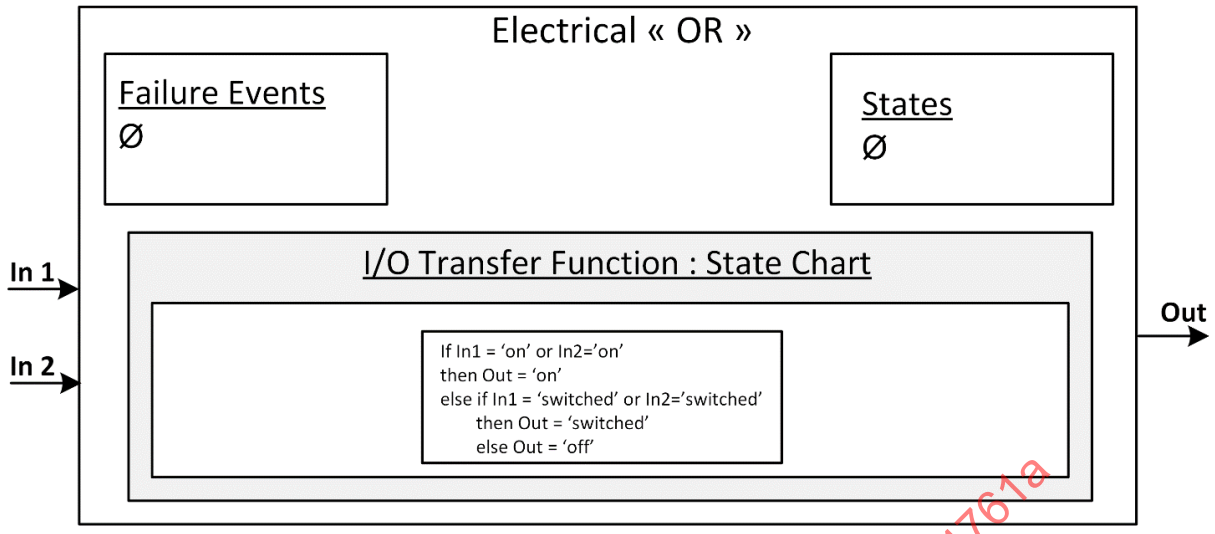


Figure N11 - Electrical <<OR>> equipment/functional block

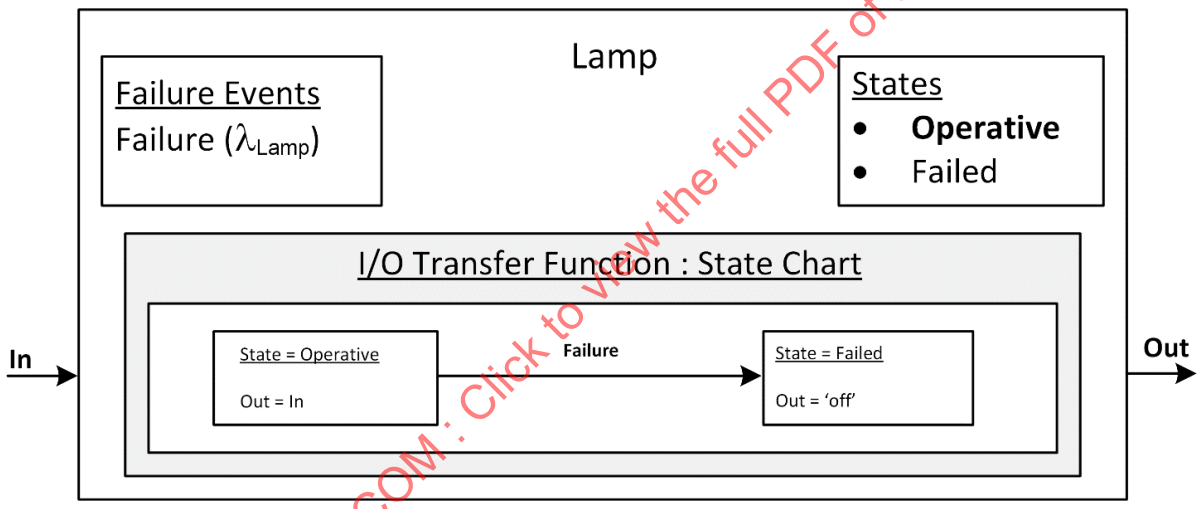


Figure N12 - Lamp equipment/functional block

SAENORM.COM : Click to view the full PDF of arp4761a

N.6.1.1 Failure Condition Logic

For purposes of this example, the failure condition to be analyzed is Lamp:Out = 'off'.

N.6.1.2 Output Generation

Section N.4 discusses two output generation methods: the deductive approach and the inductive approach. The following discussion highlights these two approaches to cut set and failure sequence generation for this example.

First, consider the inductive MBSA approach by means of simulation traces to explore the failure sequences and cut sets. From a safety perspective, the simulation will be performed by first injecting one failure event for each trace, then by injecting two failure events for each trace and so on. The injection process will use the transfer function logic involving the failure event to determine the state changes and the resulting output effects for the equipment/functional blocks containing the transfer function. Changes in outputs will be tracked as input changes to downstream components and component state changes per the FPM. After propagating the injected failure event in the FPM, the failure condition logic will be checked for each trace to see if it is true. If it is true, then that trace will be recorded as a cut set. In case of multiple events, the combination of multiple events under consideration can be injected in different sequence to detect the failure sequences. If all such sequences for the set of multiple events lead to the failure condition becoming true, then the multiple event combination is sequence-independent and will be recorded as a cut set. Table N1 shows a sample of such traces. The highlighted rows are cut sets as they make the failure condition logic true.

The systematic simulation for a large system with many equipment/functional blocks can lead to a large number of traces to explore; to answer this challenge, MBSA tools are equipped to generate cut sets. Note that the simulation traces in the table are typically highlighted by graphical methods on the FPM to facilitate visualization of fault propagation by the analyst to verify the system behavior.

SAENORM.COM : Click to view the full PDF of arp4761a

Table N1 - Sample of cut set traces leading to a Failure Condition (Lamp:Out = 'off')

		Battery	ElectricalDistribution			Dual Contact Switch				Electrical <<OR>>			Lamp	
Simulation Trace	Failure Events Injected	Out	In	Out1	Out2	In_Sw1	In_Sw2	Out_Sw1	Out_Sw2	In1	In2	Out	In	Out
1	Battery-Failure	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Off	Off	Off	Off	Off	Off	Off
2	Lamp-Failure	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	switched	switched	switched	switched	switched	switched	Off
3	Dual Contact Switch - Common Mode Failure	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	Off	Off	Off	Off	Off	Off	Off
4	Dual Contact Switch - Contact 1 Fail Open	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	Off	switched	Off	switched	switched	switched	switched
5	Dual Contact Switch - Contact 1 Fail Open Dual Contact Switch - Contact 2 Fail Open	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	Off	Off	Off	Off	Off	Off	Off
6	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Note that this table records the effects on each component when failure events are injected.

When double failure events are injected, two lines are used (see Simulation Trace 5).

When a combination of failure events injected (Column 2) leads to the failure condition (Lamp.Out = 'off'), the simulation trace is colored in grey.

SAENORM.COM : Click to view the full PDF of arp4761a

The deductive MBSA approach will start with the failure condition and back-trace the input and outputs and failure events that are compatible with such inputs and outputs. This will be done by recursive Boolean function evaluation. Thus, the Lamp:Out='off' top failure condition is broken down into intermediate Boolean events as shown in Figure N13. The graphic is meant to show the Boolean expression and not the fault tree methodology described in Appendix G.

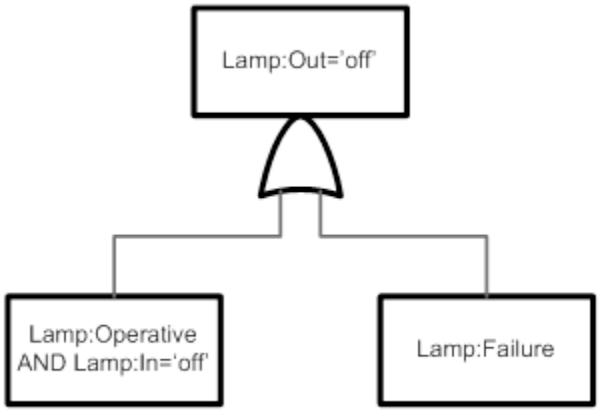
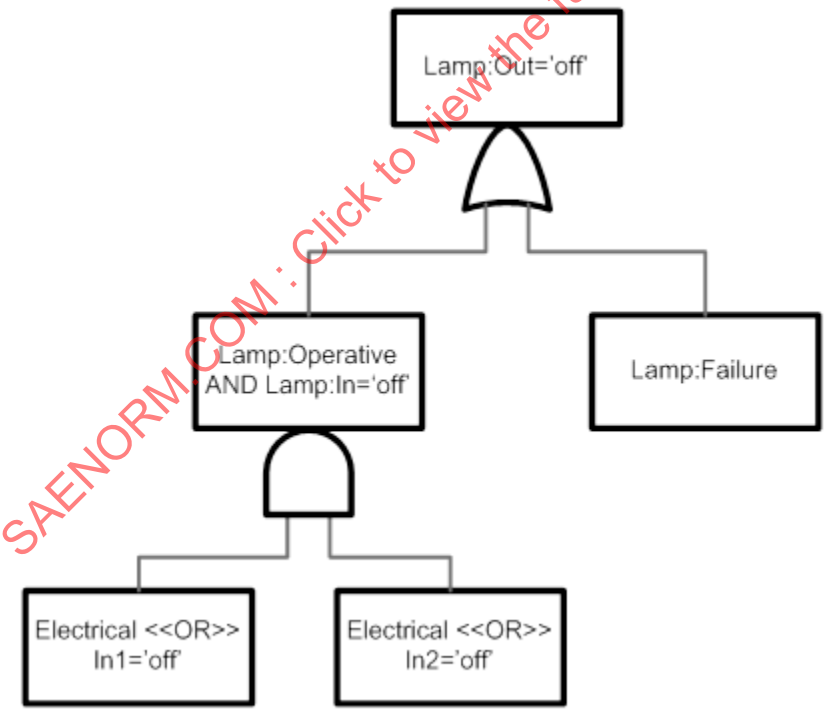


Figure N13 - Top failure condition example

Then back propagation from Lamp:In='off' condition to electrical <<OR>> block output helps build the next level of the Boolean logic as shown in Figure N14.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure N14 - Next level of failure condition example

This process is continued until the need for back propagation is exhausted (e.g., end in a terminal block with no inputs such as “battery”). Such a Boolean representation can be processed for cut sets by many tools. It is clear that Lamp:Failure is a cut set from Figure N13 and it agrees with the induction approach trace 1 shown in Table N1. Large FPM cut sets are generated by MBSA tools equipped with special algorithms to perform what is highlighted here.

N.6.2 More Complex MBSA Example

The following MBSA complex example, shown in Figure N15, models a control system which includes:

a. Three engines.

b. Four power supplies.

c. A triple channel main computer.

d. A single channel backup computer.

e. A voter allowing the elaboration of a consolidated value from main computers.

f. A switching function allowing the selection of the backup computer command when main computers are out of order.

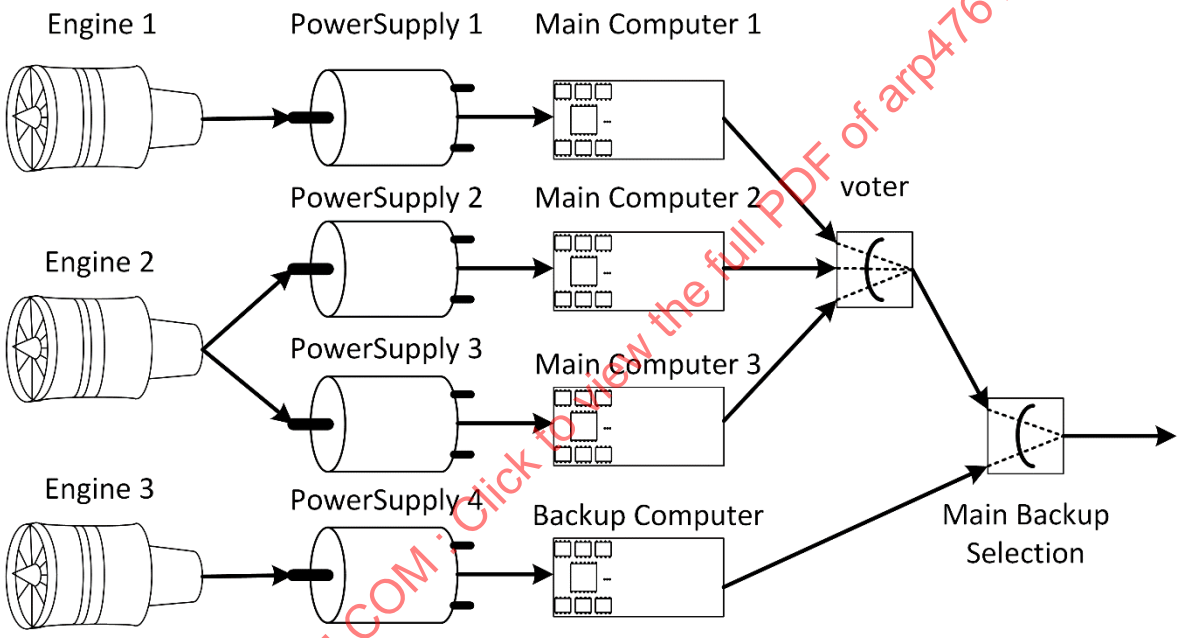


Figure N15 - MBSA complex example, control system

The equipment/functional blocks are as shown in Figures N16 through N20.

SAENORM.COM : Click to view the full PDF of arp4761a

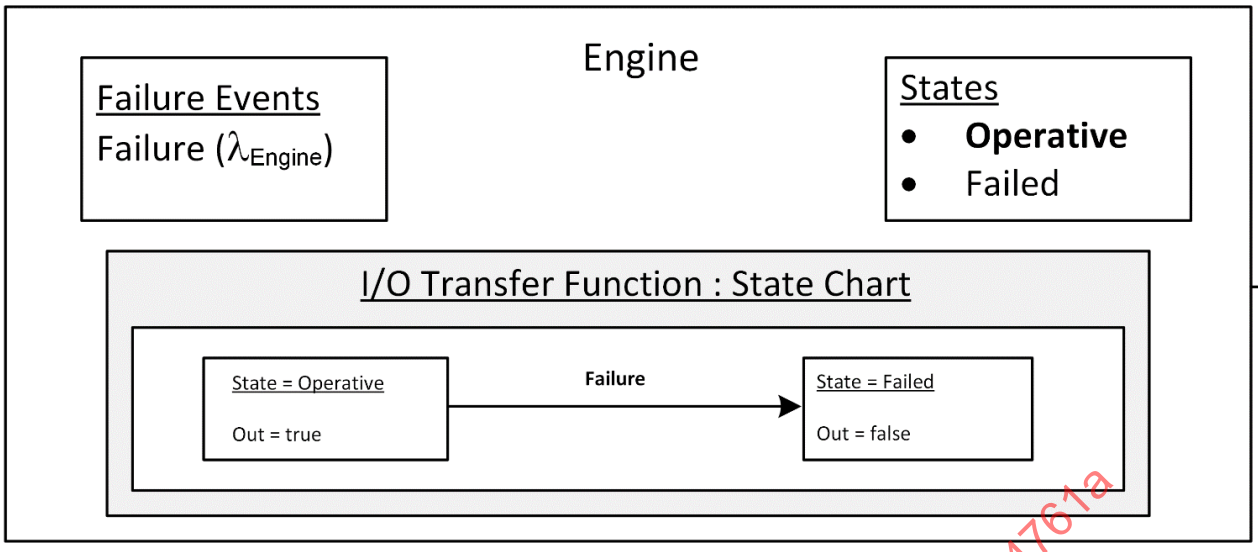


Figure N16 - Engine equipment/functional block

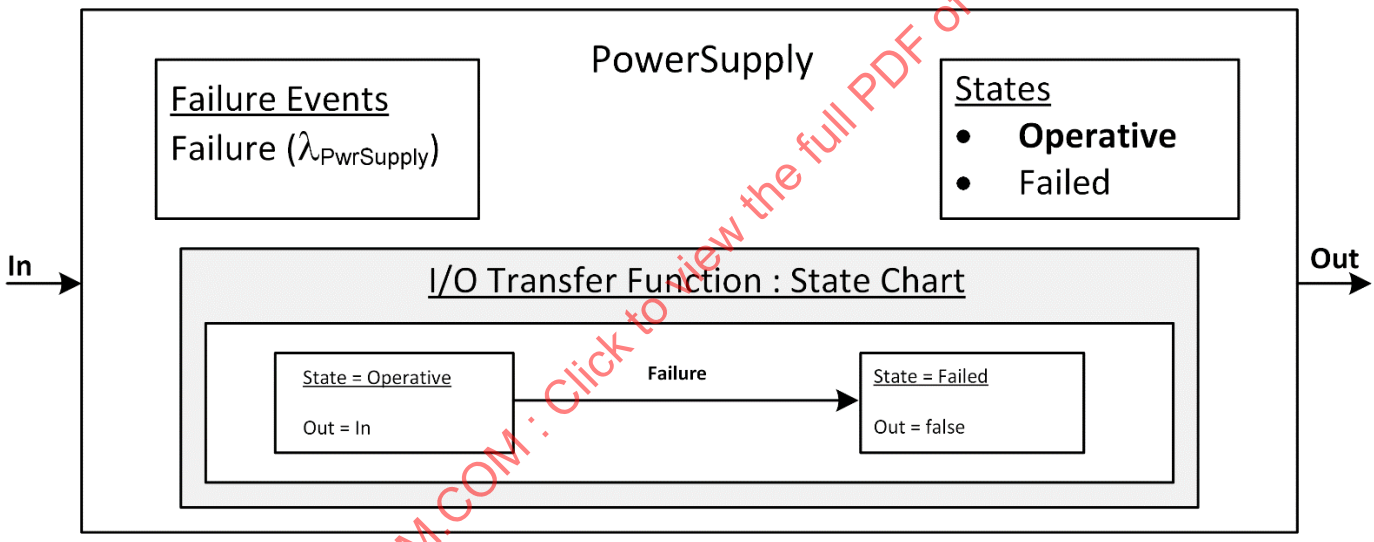


Figure N17 - Power supply equipment/functional block

SAENORM.COM : Click to view the full PDF of arp4761a

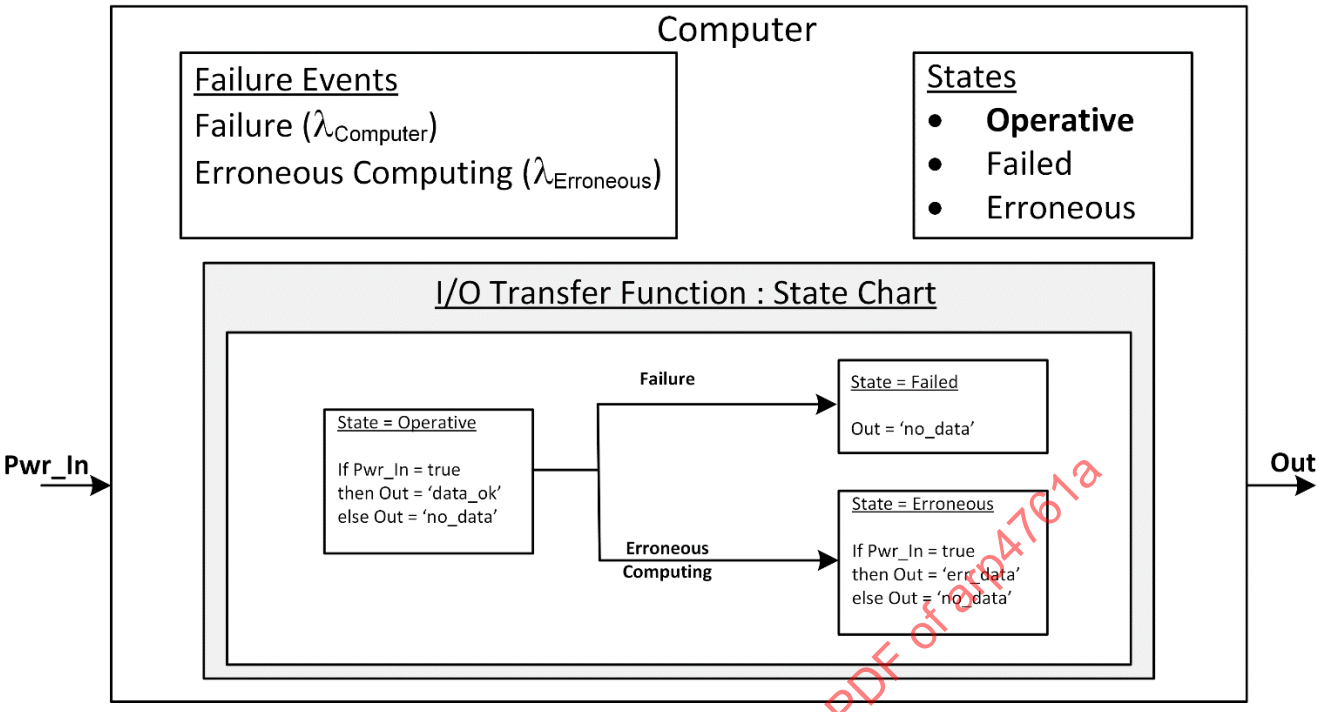


Figure N18 - Computer equipment/functional block

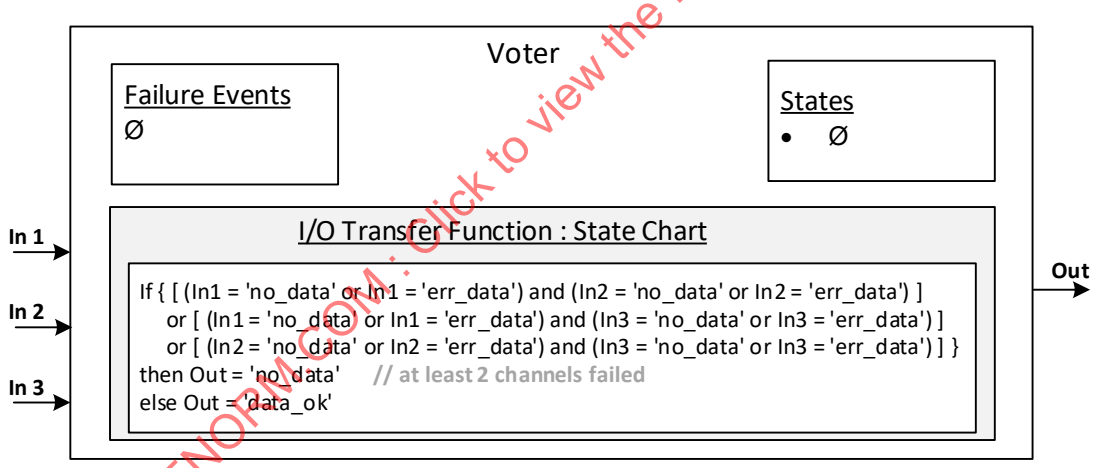


Figure N19 - Voter equipment/functional block

SAENORM.COM : Click to view the full PDF of arp4761a

NOTE: (1) We consider in this voter that two input failures cannot be triggered at the same time. As a consequence, per construction, the case "*two inputs equal to 'err*_data'" sets the voter output invalid.

(2) For simplicity, the voter and the switching logic have no failure events and no state.

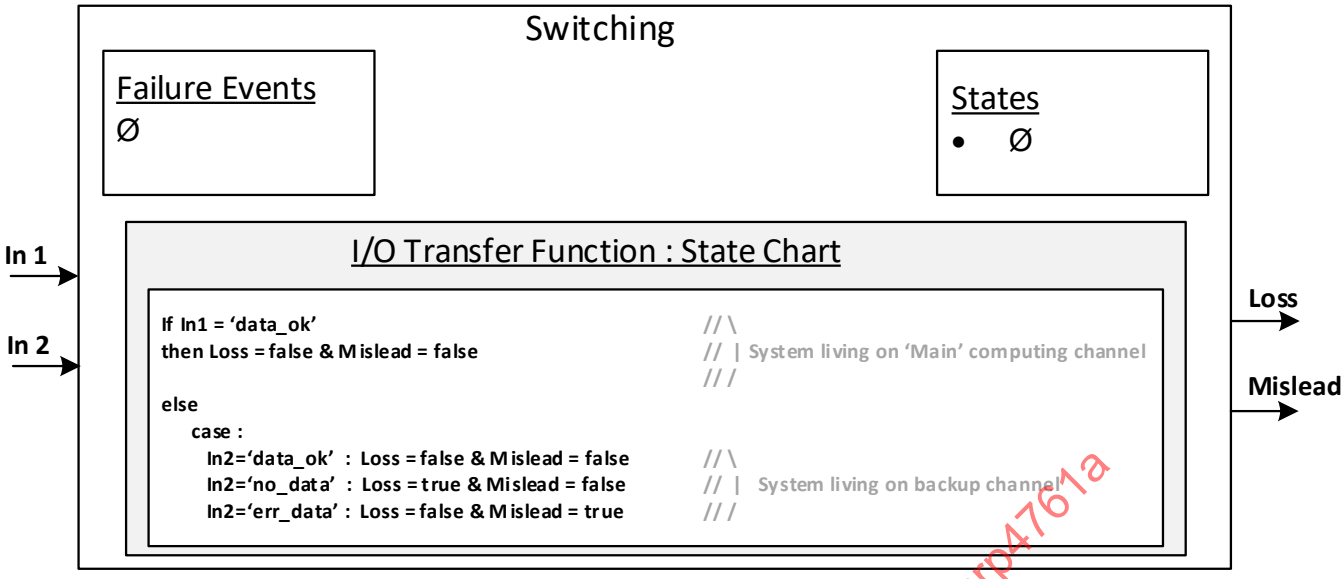


Figure N20 - Switching equipment/functional block

N.6.2.1 Failure Condition Logic

Two failure conditions are studied:

- FC1: Misleading Output of the Control System.
- FC2: Loss of the Control System.

N.6.2.2 Output Generation

Section N.4 discusses two output generation methods: the deductive approach and the inductive approach. The following discussion highlights these approaches to cut set and failure sequence generation for this example.

First, we consider the inductive MBSA approach by means of simulation traces to explore the failure sequences and cut sets. From a safety perspective, the simulation will be performed by first injecting one failure event for each trace, then by injecting two failure events for each trace and so on. The injection process will use the transfer function logic involving the failure event to determine the state changes and the resulting output effects for the equipment/functional blocks containing the transfer function. Changes in outputs will be tracked as input changes to downstream components and component state changes per the FPM. After propagating the injected failure event in the FPM, the failure condition logic will be checked for each trace to see if it is true. If it is true, then that trace will be recorded as a cut set. In case of multiple events, the combination of multiple events under consideration can be injected in different sequence to detect the failure sequences. If all such sequences for the set of multiple events lead to the failure condition becoming true, then the multiple event combination is sequence-independent and will be recorded as a cut set. Table N2 shows a sample of such traces. The highlighted rows are cut sets as they make the failure condition. The FC1 minimal cut set is highlighted in Table N3 and the FC2 minimal cut set is highlighted in Table N2.

SAENORM.COM : Click to view the full PDF of arp4761a

Table N2 - Sample of cut set traces leading to two failure conditions (Switch.Loss = True, Switch.MisLead = False)

		Engines			Power supplies								Computers								Voter				Switch			
		1	2	3	1		2		3		4		Main 1		Main 2		Main 3		Backup									
Simulation trace	Failure Events injected	Out	Out	Out	In	Out	In	Out	In	Out	In	Out	Pwr_In	out	Pwr_In	out	Pwr_In	out	Pwr_In	out	In1	In2	In3	Out	In1	In2	Loss	Mislead
1	Engine 1 stop	F	T	T	F	F	T	T	T	T	T	T	F	no_data	T	data_ok	T	data_ok	T	data_ok	no_data	data_ok	data_ok	data_ok	data_ok	data_ok	F	F
2	Engine 2 stop	T	F	T	T	T	F	F	F	F	T	T	T	data_ok	F	no_data	F	no_data	T	data_ok	data_ok	no_data	no_data	no_data	no_data	data_ok	F	F
3	Engine 3 stop	T	T	F	T	T	T	T	T	T	F	F	T	data_ok	T	data_ok	T	data_ok	F	no_data	data_ok	data_ok	data_ok	data_ok	data_ok	no_data	F	F
4	Engine 2 stop & Backup Computer Failure	T	F	T	T	T	F	F	F	F	T	T	T	data_ok	F	no_data	F	no_data	T	no_data	data_ok	no_data	no_data	no_data	no_data	no_data	T	F
5	Engine 2 stop & Backup Computer Erroneous computing	T	F	T	T	T	F	F	F	F	T	T	T	data_ok	F	no_data	F	no_data	T	err_data	data_ok	no_data	no_data	no_data	no_data	err_data	F	T
6	Engine 2 stop & Engine 3 stop	T	F	T	T	T	F	F	F	F	T	T	T	data_ok	F	no_data	F	no_data	F	no_data	data_ok	no_data	no_data	no_data	no_data	no_data	T	F
7	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Table N3 - Sample of cut set traces leading to two failure conditions (Switch.Loss = False, Switch.MisLead = True)

		Engines			Power supplies								Computers								Voter				Switch			
		1	2	3	1		2		3		4		Main 1		Main 2		Main 3		Backup									
Simulation tra	Failure Events injected	Out	Out	Out	In	Out	In	Out	In	Out	In	Out	Pwr_In	out	Pwr_In	out	Pwr_In	out	Pwr_In	out	In1	In2	In3	Out	In1	In2	Loss	Mislead
1	Engine 1 stop	F	T	T	F	F	T	T	T	T	T	T	F	no_data	T	data_ok	T	data_ok	T	data_ok	no_data	data_ok	data_ok	data_ok	data_ok	data_ok	F	F
2	Engine 2 stop	T	F	T	T	T	F	F	F	F	T	T	T	data_ok	F	no_data	F	no_data	T	data_ok	data_ok	no_data	no_data	no_data	no_data	data_ok	F	F
3	Engine 3 stop	T	T	F	T	T	T	T	T	T	F	F	T	data_ok	T	data_ok	T	data_ok	F	no_data	data_ok	data_ok	data_ok	data_ok	data_ok	no_data	F	F
4	Engine 2 stop & Backup Computer Failure	T	F	T	T	T	F	F	F	F	T	T	T	data_ok	F	no_data	F	no_data	T	no_data	data_ok	no_data	no_data	no_data	no_data	no_data	T	F
5	Engine 2 stop & Backup Computer Erroneous computing	T	F	T	T	T	F	F	F	F	T	T	T	data_ok	F	no_data	F	no_data	T	err_data	data_ok	no_data	no_data	no_data	no_data	err_data	F	T
6	Engine 2 stop & Engine 3 stop	T	F	T	T	T	F	F	F	F	T	T	T	data_ok	F	no_data	F	no_data	F	no_data	data_ok	no_data	no_data	no_data	no_data	no_data	T	F
7	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Note that these tables record the effects on each component when failure events are injected.

SAENORM.COM : Click to view the full PDF of arp4761a

When a combination of failure events injected (Column 2) leads to the failure condition, the simulation trace is colored in grey. The systematic simulation for a large system with many equipment/functional blocks can lead to a large number of traces to explore; to answer this challenge, MBSA tools are equipped to generate cut sets. Note that the simulation traces in the table are highlighted by graphical methods on the FPM to facilitate visualization of fault propagation by the analyst to verify the system behavior.

The deductive MBSA approach will start with the failure condition and back-trace the input and outputs and failure events that are compatible with such inputs and outputs. This will be done by recursive Boolean function evaluation. Thus, the FC2 top failure condition is broken down into intermediate Boolean events as shown in Figure N21.

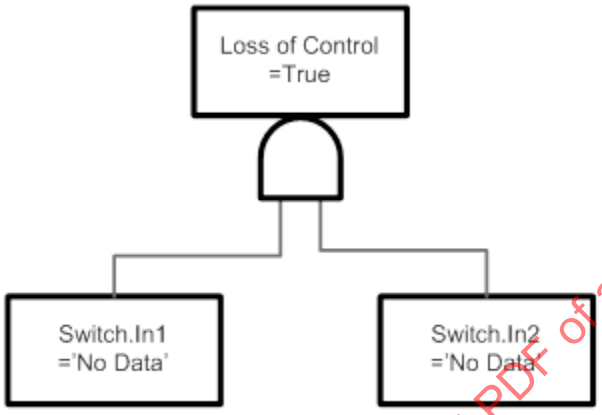


Figure N21 - Top failure condition FC2 deductive Boolean function

Then back propagation from Switch:In2='No Data' condition to backup computer block output and its input helps build the next level of the Boolean logic using the backup computer Block State Chart logic as shown in Figure N22.

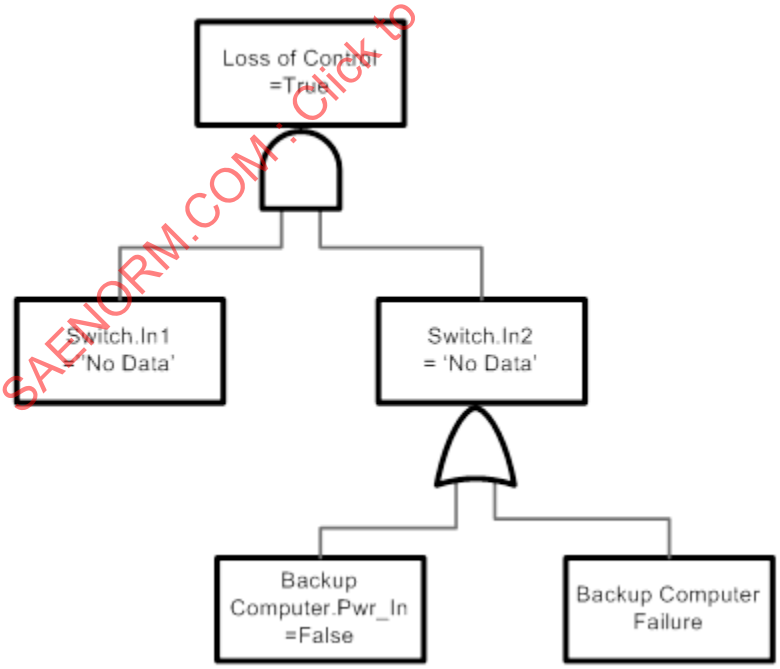


Figure N22 - Next level of failure condition example

This process is continued until the need for back propagation is exhausted (e.g., end in a terminal block with no inputs such as one of the engines). Such a Boolean representation can be processed for cut sets by many tools. Large FPM cut sets are generated by MBSA tools equipped with special algorithms to perform the back propagation highlighted here.

SAENORM.COM : Click to view the full PDF of arp4761a

Figures N23 and N24 extract present the cut sets (limited to order 3) for FC1, FC2 generated by an induction method based tool.

FC1: Misleading Output of the Control System

```
ordersproduct-number
2              1
3             33
Total of Minimal Cut Sets: 34
*/
The following is a MCS subset:
{“BackupComputer.misleading”, “engine2.stop”}
{“BackupComputer.misleading”, “MainComputer1.failure”, “MainComputer2.failure”}
{“BackupComputer.misleading”, “MainComputer1.failure”, “MainComputer2.misleading”}
{“BackupComputer.misleading”, “MainComputer1.failure”, “MainComputer3.failure”}
{“BackupComputer.misleading”, “MainComputer1.failure”, “MainComputer3.misleading”}
{“BackupComputer.misleading”, “MainComputer1.failure”, “PowerSupply2.failure”}
{“BackupComputer.misleading”, “MainComputer1.failure”, “PowerSupply3.failure”}
{“BackupComputer.misleading”, “MainComputer1.misleading”, “MainComputer2.failure”}
{“BackupComputer.misleading”, “MainComputer1.misleading”, “MainComputer2.misleading”}
```

Figure N23 - FC1 cut set example

FC2: Loss of the Control System

```
ordersproduct-number
2              3
3             99
Total of Minimal Cut Sets: 102

The following is a MCS subset:
{“BackupComputer.failure”, “engine2.stop”}
{“PowerSupply4.failure”, “engine2.stop”}
{“engine2.stop”, “engine3.stop”}
{“BackupComputer.failure”, “MainComputer1.failure”, “MainComputer2.failure”}
{“BackupComputer.failure”, “MainComputer1.failure”, “MainComputer2.misleading”}
{“BackupComputer.failure”, “MainComputer1.failure”, “MainComputer3.failure”}
{“BackupComputer.failure”, “MainComputer1.failure”, “MainComputer3.misleading”}
```

Figure N24 - FC2 cut set example

SAENORM.COM : Click to view the full PDF of arp4761a

N.7 POTENTIAL MBSA SERVICES BASED ON RELATIONSHIPS COMPUTATIONS AND DISPLAY

N.7.1 Display of Function and Architecture Dependencies

Dependencies chains can be synthesized from the safety model and displayed and/or browsed interactively. Figure N25 shows an example of dynamic display of functional dependencies, with dynamic focus on an element of interest selected by an MBSA environment user (in this case, shutoff valve).

Note that the name of the function container is displayed above the function name.

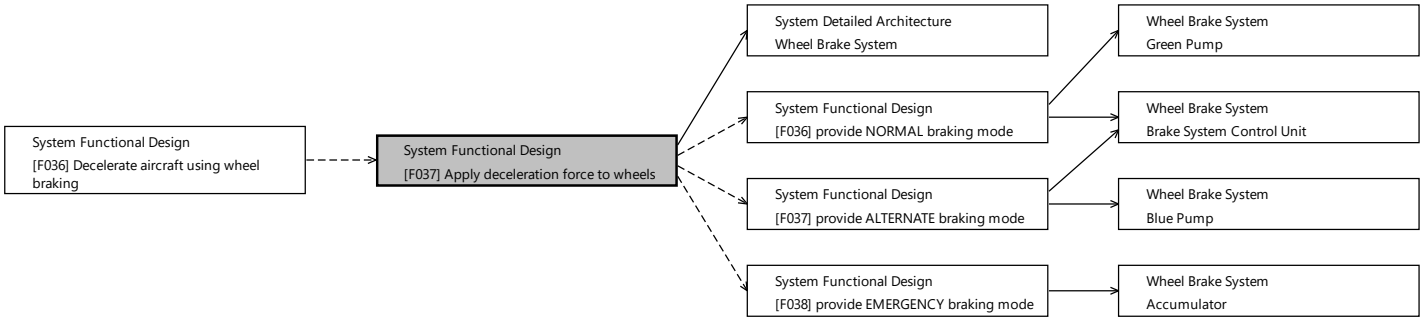


Figure N25 - Focused functions/architecture dependency example

N.7.2 Links Between Functional Safety Requirements and Faults/Failures and Change Impact Analysis

MBSA allows the relationship between functional safety requirements and faults/failures to be managed. It is also possible to define consistency rules that can be checked based on the model information to verify coverage of faults/failures by safety requirements. Such rules could assist in reviews and assessments.

These relationships can also be used for change impact analysis.

N.7.3 Fault Propagation Net Computation and FMES Derivation

Once the failure modes of elements and their failure laws have been captured manually (or re-used from a catalog), it is possible to derive propagation analysis support. For instance, a worst-case failure propagation chain slice is shown in Figure N26.

Note that as with the previous example, this is a focused view, so the size of the view is manageable.

SAENORM.COM : Click to view the full PDF of arp4761a

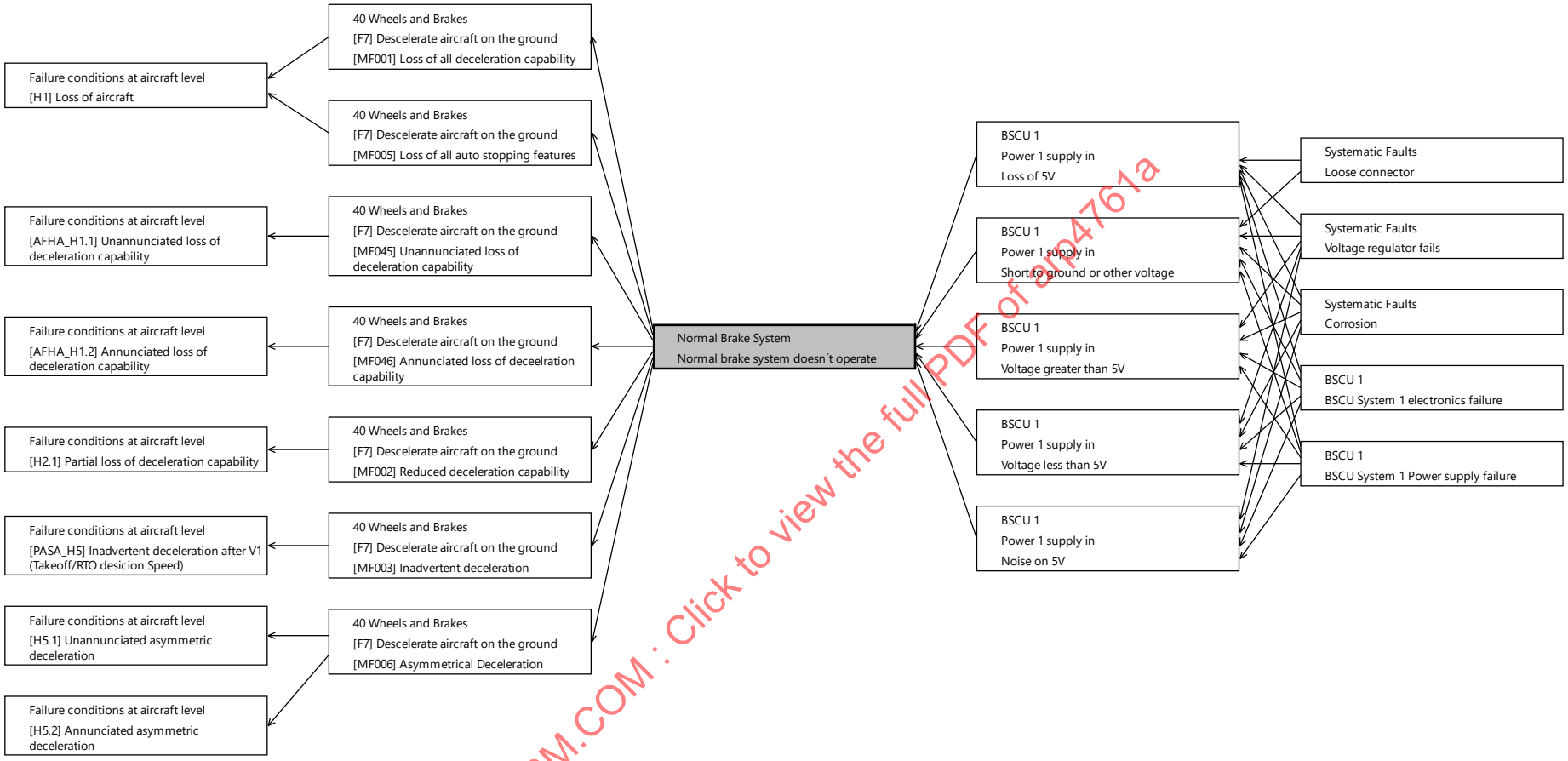


Figure N26 - Focused fault propagation graph example

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX O - CASCADING EFFECTS ANALYSIS (CEA)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

O.1 SCOPE 322
O.1.1 Introduction 322

O.2 DEFINITIONS 322

O.3 CASCADING EFFECTS ANALYSIS INPUTS 323

O.4 CASCADING EFFECTS ANALYSIS METHODOLOGY 323
O.4.1 Determine Cascading Effect Extent 325
O.4.2 Determine the Cascading Aircraft Effects 326
O.4.3 Cascade Effect Analysis Results 329

O.5 CEA OUTPUTS 329

Figure O1 CEA overview 324
Figure O2 Cascading effects extent determination example 326
Figure O3 Aircraft effect determination example, stage 1 327
Figure O4 Aircraft effect determination example, stage 2 327
Figure O5 Aircraft effect determination example, stage 3 328
Figure O6 Aircraft effect determination example, final 329

SAENORM.COM : Click to view the full PDF of arp4761a

O.1 SCOPE

This appendix provides guidelines for conducting a Cascading Effects Analysis (CEA). The methodology described is typically applied as part of aircraft-level analyses, but may be applied at any level.

O.1.1 Introduction

The CEA is a qualitative, bottom-up analysis method which evaluates an initiating condition (e.g., a failure condition, failure mode, or combination of failure modes) and captures the total effect on the aircraft for that initiating condition. The CEA iteratively identifies the direct and indirect effects that propagate from the initiating condition due to system dependencies. All systems directly or indirectly connected to the systems impacted by the initiating condition are considered in the CEA.

The CEA may be used to support any analysis that requires the determination of aircraft-level or multisystem effects for specific initiating conditions. The effects of each initiating condition are returned to the source analysis. Examples of possible CEA applications include:

a. Determining the effects of resource system failure conditions as part of the Aircraft Functional Hazard Assessment (AFHA) or System Functional Hazard Assessment (SFHA).

b. Determining the effects of resource system failure modes or combinations of resource system failure modes as part of the Preliminary Aircraft Safety Assessment (PASA).

c. Determining the effects of shared or integrated equipment failure modes as part of the Preliminary System Safety Assessment (PSSA).

d. Determining the effects of loss of function or malfunction of shared or integrated equipment containing software or airborne electronic hardware as part of the item development assurance level (IDAL) assignment in the PSSA.

e. Determining the effects of failure or damage scenarios identified as part of the Particular Risk Analysis (PRA) or Zonal Safety Analysis (ZSA).

Note that the CEA is not the only method to accomplish the cascading effect identification task. Other methods or testing may be used instead of, or in addition to, a CEA.

O.2 DEFINITIONS

RESOURCE SYSTEM: A system that provides common energy or information to multiple systems. Providing power or data may be the primary function of the resource system (e.g., electrical power systems, hydraulic systems, air data systems, network systems), or a secondary function (e.g., a powerplant system that provides bleed air, a landing gear system that provides “weight on wheels” signals, a flight control system that provides “flap position” signals).

USER SYSTEM: A system that requires inputs from resource systems to perform its intended functions. A resource system may itself also be a user system (e.g., an electrical power system that requires mechanical drive from a powerplant system to perform its intended function).

CASCADING EFFECTS: The complete set of effects resulting from the propagation of an initiating condition, i.e., sum of direct and indirect effects due to the initiating condition.

CASCADE FAILURE: The induced failure result of an initiating failure mode or failure condition.

INITIATING CONDITION: A failure or combination of failures that causes subsequent failures due to dependency between systems or equipment.

DIRECT EFFECT: Effect on a system directly connected to the system(s) subject to the initiating condition.

INDIRECT EFFECT: Effect on a system indirectly connected to the system(s) subject to the initiating condition.

SAENORM.COM : Click to view the full PDF of arp4761a

O.3 CASCADING EFFECTS ANALYSIS INPUTS

The following inputs may be used in the CEA:

a. Aircraft function allocation and high-level architecture from the development process.

b. System functions, architecture, interfaces, and operating logic from the development process.

c. Functional dependencies from the PASA or PSSA.

d. Failure condition effects and failure mode effects from the SFHA, System Safety Assessment (SSA), or lower-level analyses such as fault tree (via fault tree primary events) or Failure Modes and Effects Analysis/Summary (FMEA/FMES).

The CEA is performed on an initiating condition that may be either a failure condition, a failure mode, or a combination of failure modes. The initiating conditions for the CEA are provided from other analysis (e.g., AFHA, SFHA, PASA, PSSA, PRA, or ZSA as mentioned in Section O.1). Depending on the CEA application, some examples of initiating conditions may include:

a. In the frame of AFHA or SFHA, resource system failure conditions may be used as an initiating condition.

b. In the frame of the PASA, relevant scenarios from the PASA may be used as an initiating condition.

c. In the frame of the PSSA, significant failure modes of the shared or integrated equipment of interest may be used as an initiating condition.

d. In the frame of IDAL assignment in the PSSA, failure modes that could potentially be caused by an error in the development of that item may be used as an initiating condition.

e. In the frame of PRA or ZSA, potential combination of failed or damaged equipment resulting from an occurrence of the particular risk or zonal effect may be used as a cascading failure initiator.

O.4 CASCADING EFFECTS ANALYSIS METHODOLOGY

For each initiating condition identified in the source analysis, the CEA consists of the following steps:

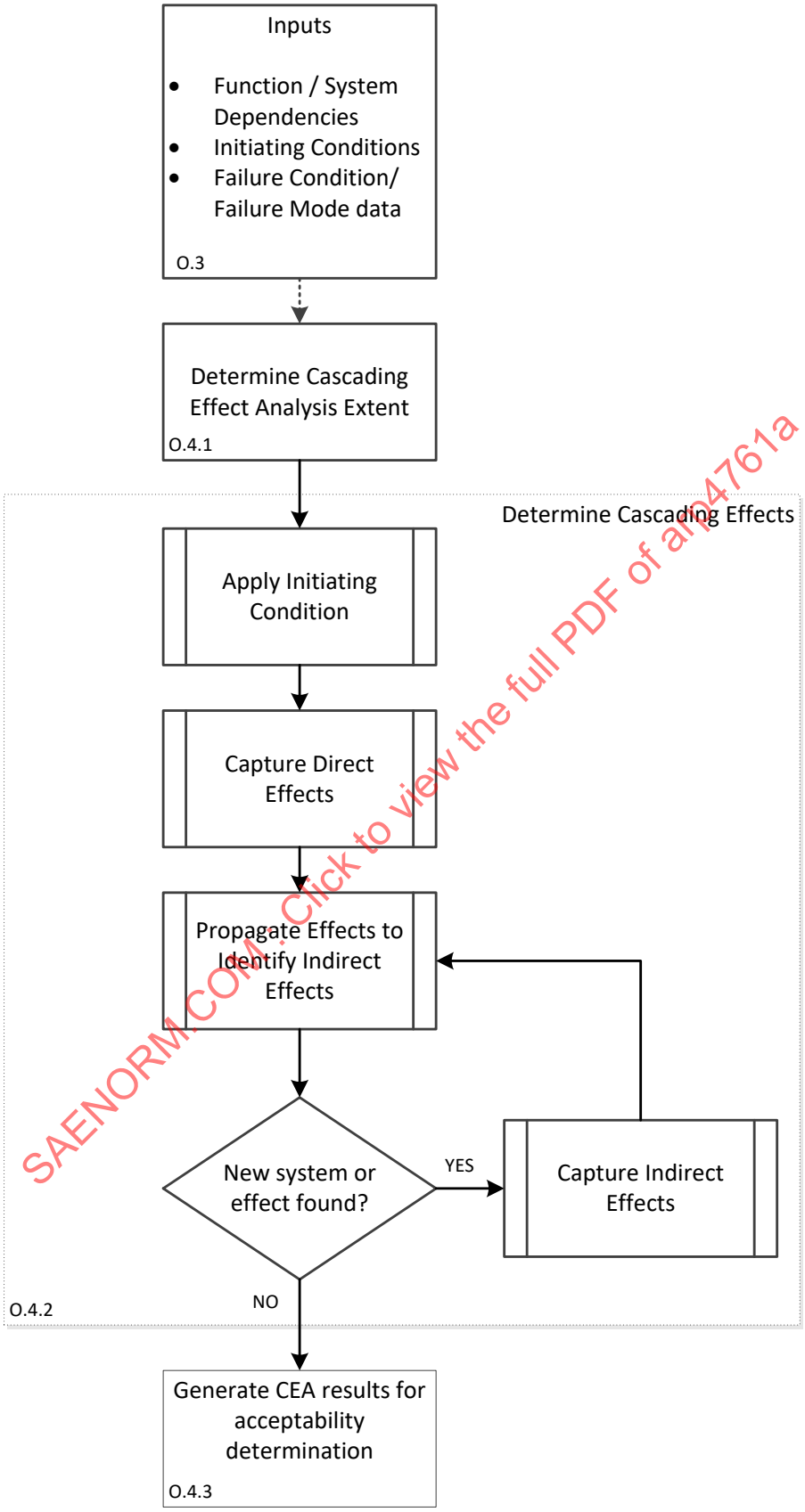
a. Determine the cascading effect extent.

b. Iteratively describe the aircraft effects for the initiating condition.

c. Provide the aircraft effect descriptions of each initiating condition to the source analysis.

Figure O1 summarizes the CEA steps and their sequence. Sections O.4.1 through O.4.3 discuss each step in more detail. For readability purposes, these sections describe a “system” CEA. “System” may be replaced in each activity with “equipment” or “item” when applying the CEA in the frame of a lower-level activity.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure O1 - CEA overview

O.4.1 Determine Cascading Effect Extent

Determining the cascading effect extent identifies the systems that are either directly connected to and affected by the initiating condition or are indirectly connected through one or more systems to the initiating condition. The focus for the CEA extent is to identify and capture preliminary system interfaces and potential interaction pathways.

The following steps may be followed to identify the cascade effect extent:

a. Identify an initial set of systems subject to a particular initiating condition.

b. Initiate the cascading effect extent with the system or set of systems subject to the initiating condition.

c. Enrich the system analysis set by adding systems indirectly connected to the systems set which exhibit cascading effects.

d. Iteratively repeat the previous step as long as any system may be added.

e. The cascading effect extent is complete when no further system can be found that directly or indirectly responds to the initiating condition.

The complete cascading effect extent determined by this method will contain all systems directly or indirectly connected to the systems subject to the initiating condition.

Note that when the extent includes one or more resource systems, every user system for the affected resource systems and every system directly or indirectly connected to those user systems will be within the cascading effect extent.

Figure O2 shows an example where the cascading effects extent (systems presented by a full line box) is determined in four iterations.

The Iteration 1 portion of Figure O2 presents the example starting point. The initiating condition directly affects System 1. The CEA extent enrichment continues in Iteration 2 identifying the System 1 effect relationships to System 4 and 5. In Iteration 3, the identification of additional effect relationships between System 4 and System 7, as well as System 6 and System 8 to System 5 have been captured. Finally, Iteration 4 identifies the last effect relationship between System 6 and System 9. Systems 2 and 3 are shown to highlight that for some initiating conditions a relationship may not be relevant, but may affect another initiating condition yet to be evaluated.

SAENORM.COM : Click to view the full PDF of arp4761a

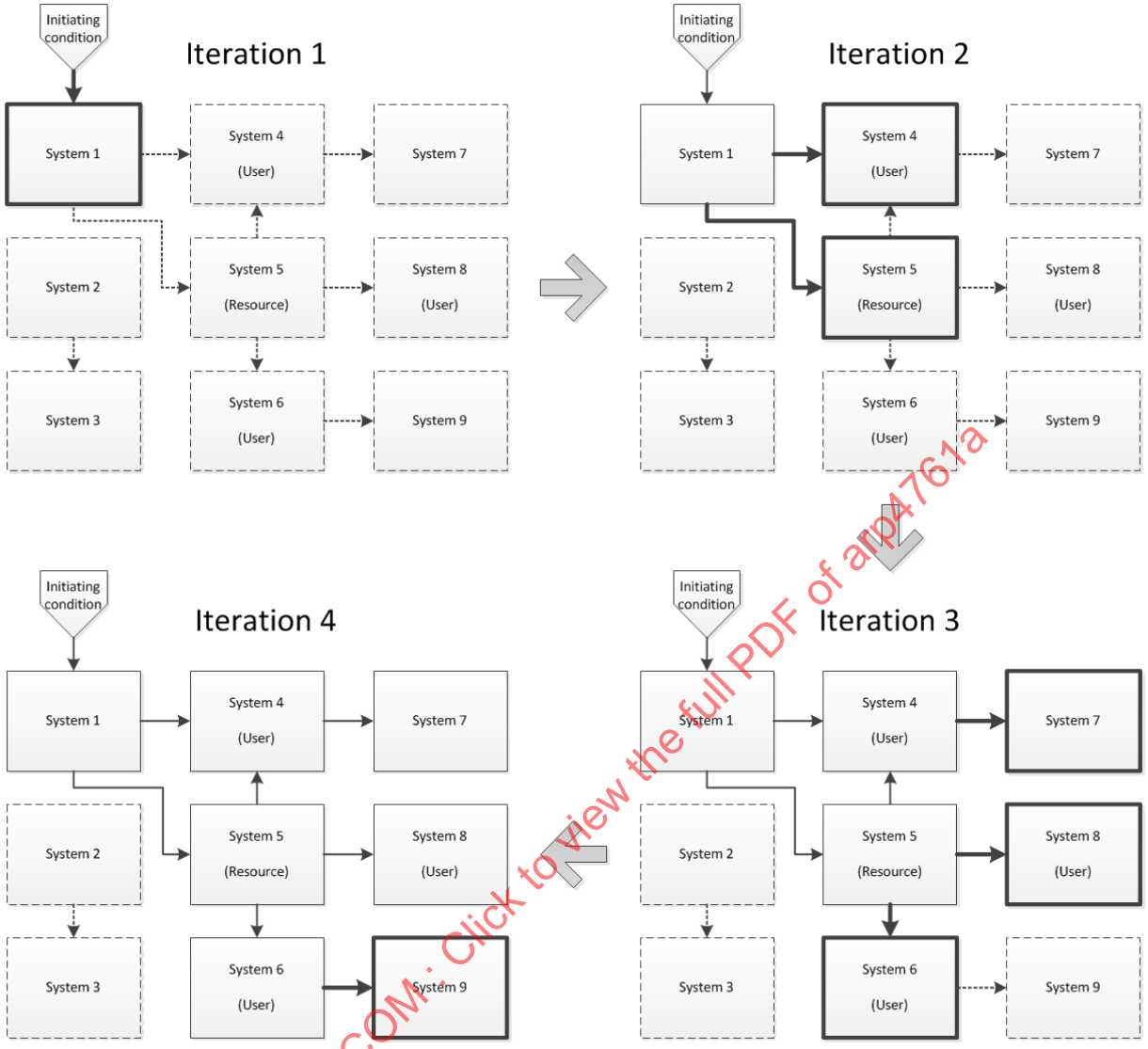


Figure O2 - Cascading effects extent determination example

SAENORM.COM : Click to view the full PDF of arp4761a

O.4.2 Determine the Cascading Aircraft Effects

The cascade effect on the aircraft resulting from each initiating condition is determined by the following iterative method:

a. Analytically apply an initiating condition to the subject systems identified in O.4.1.

b. Capture the direct effects in the systems which are affected directly by the initiating condition.

c. The direct effects propagate and may cause indirect effects on systems connected indirectly to the system(s) where the initiating condition(s) occurred. For each of the system effects captured in item b., determine and capture the system effect for subsequent direct or indirect effects in other interconnected systems.

d. The propagation of effects expands through subsequent cause and effect relationships in their interfacing systems until no further effects are identified. Iteratively repeat item c., adding all new identified cascade effects to the effects list.

e. A complete set of aircraft effects from the initiating condition is reached when no additional cascading effects can be identified.

f. The direct effects and indirect effects are captured as part of the CEA.

The cascade effects to be captured are those occurring at the moment of the failure (initiating condition) and during the remainder of the flight and landing considering all flight phases and operating conditions, crew recognition, and crew workload resulting from the crew alerts and aircraft effects.

Figures O3 through O6 show the progressive, iterative identification of effects on the example of O.4.1. Systems presented by a grey box are those impacted by effects identified and captured in the previous iteration.

In Figure O3, the initiating condition is applied to System 1. Two direct effects are identified which result from the initiating condition. These effects then become “downstream causes” for interfacing systems.

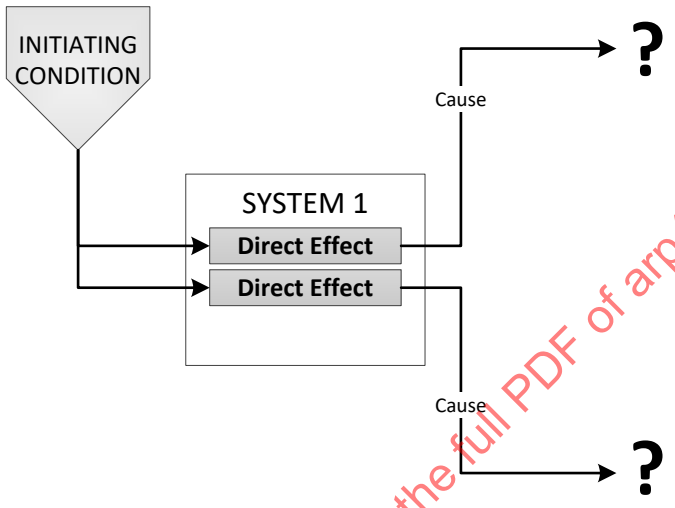


Figure O3 - Aircraft effect determination example, stage 1

In Figure O4, System 1 effects have caused indirect effects in System 4 and System 5. The System 4 and 5 effects become the causes for the “downstream” evaluation.

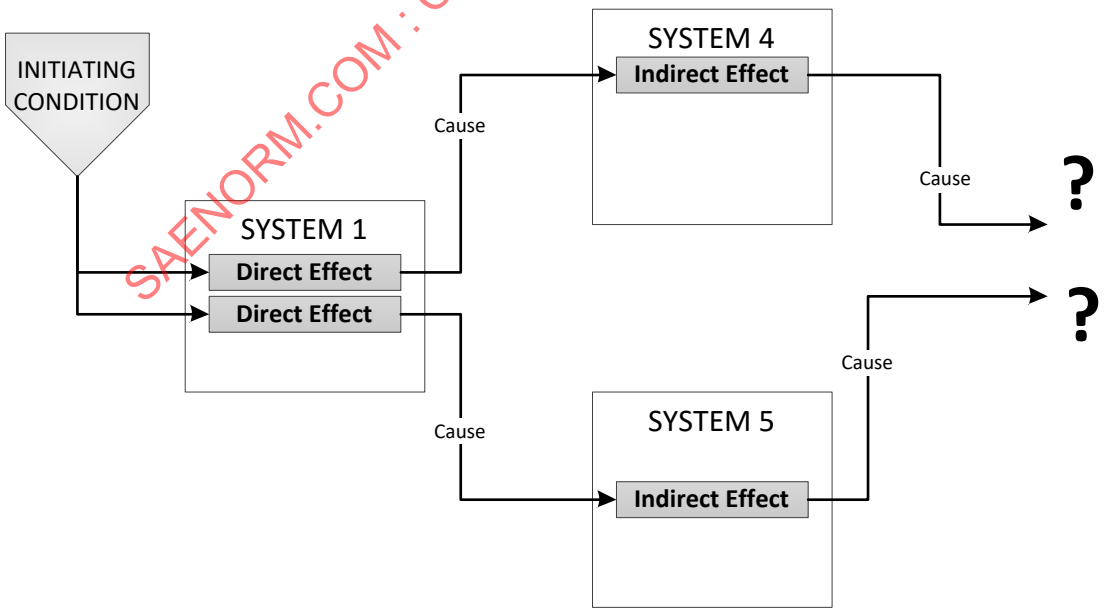


Figure O4 - Aircraft effect determination example, stage 2

SAENORM.COM : Click to view the full PDF of arp4761a

Figure O5 identifies an indirect effect of System 5 which causes an additional indirect effect in System 4. This new indirect effect in System 4 spawns an additional indirect effect which will now be captured. The System 5 indirect effect also causes an additional internal indirect effect which propagates as a cause into System 6. System 6 has indirect effects which will now be captured.

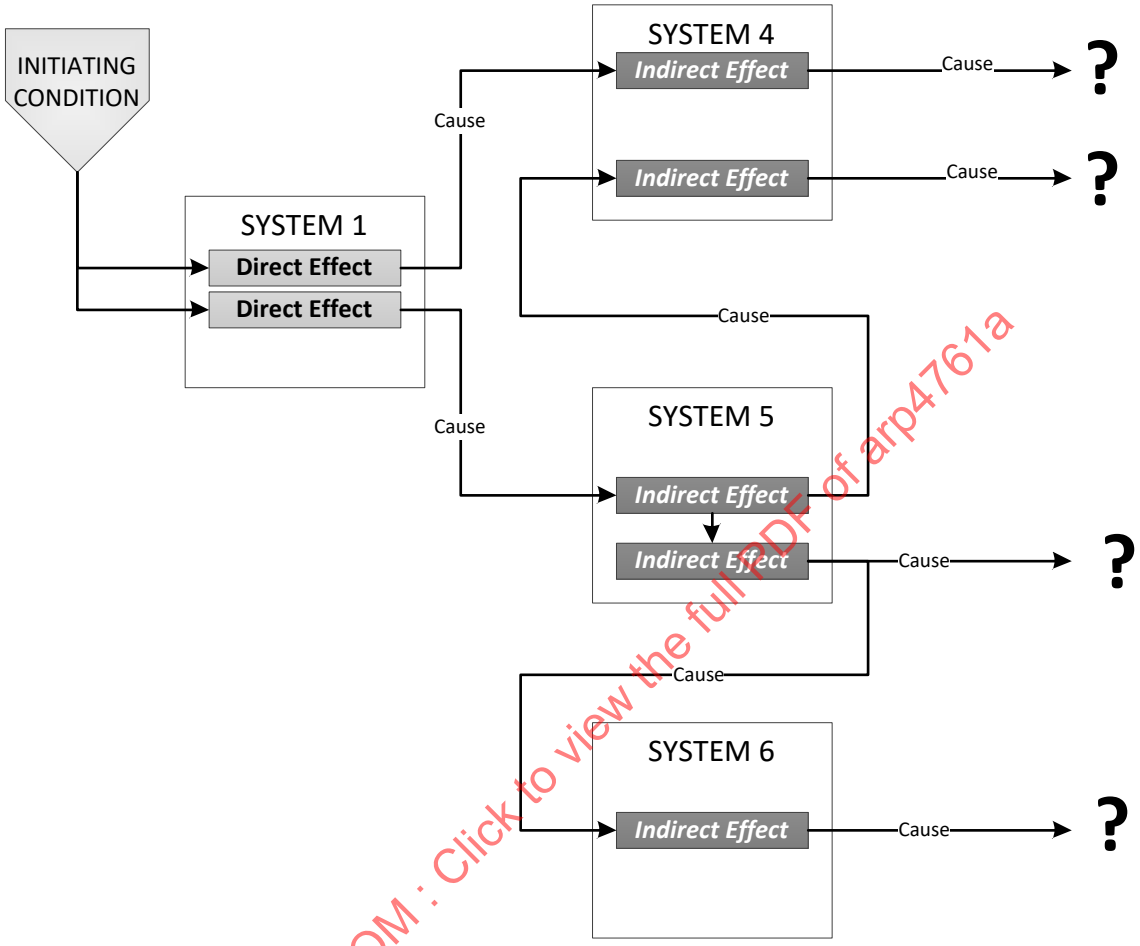


Figure O5 - Aircraft effect determination example, stage 3

Figure O6 captures the final cause effect relationships for the initiating condition. Cascading effects in System 4 have resulted in effects in System 7. The System 5 effects have resulted in effects in System 8, and the indirect effect created internal to System 6 has caused direct effect in System 9. A complete picture of the initiating condition and the cascading relationships have been identified and captured.

Note the use of “indirect effect” is with respect to the initiating condition.

SAENORM.COM : Click to view the full PDF of arp4761a

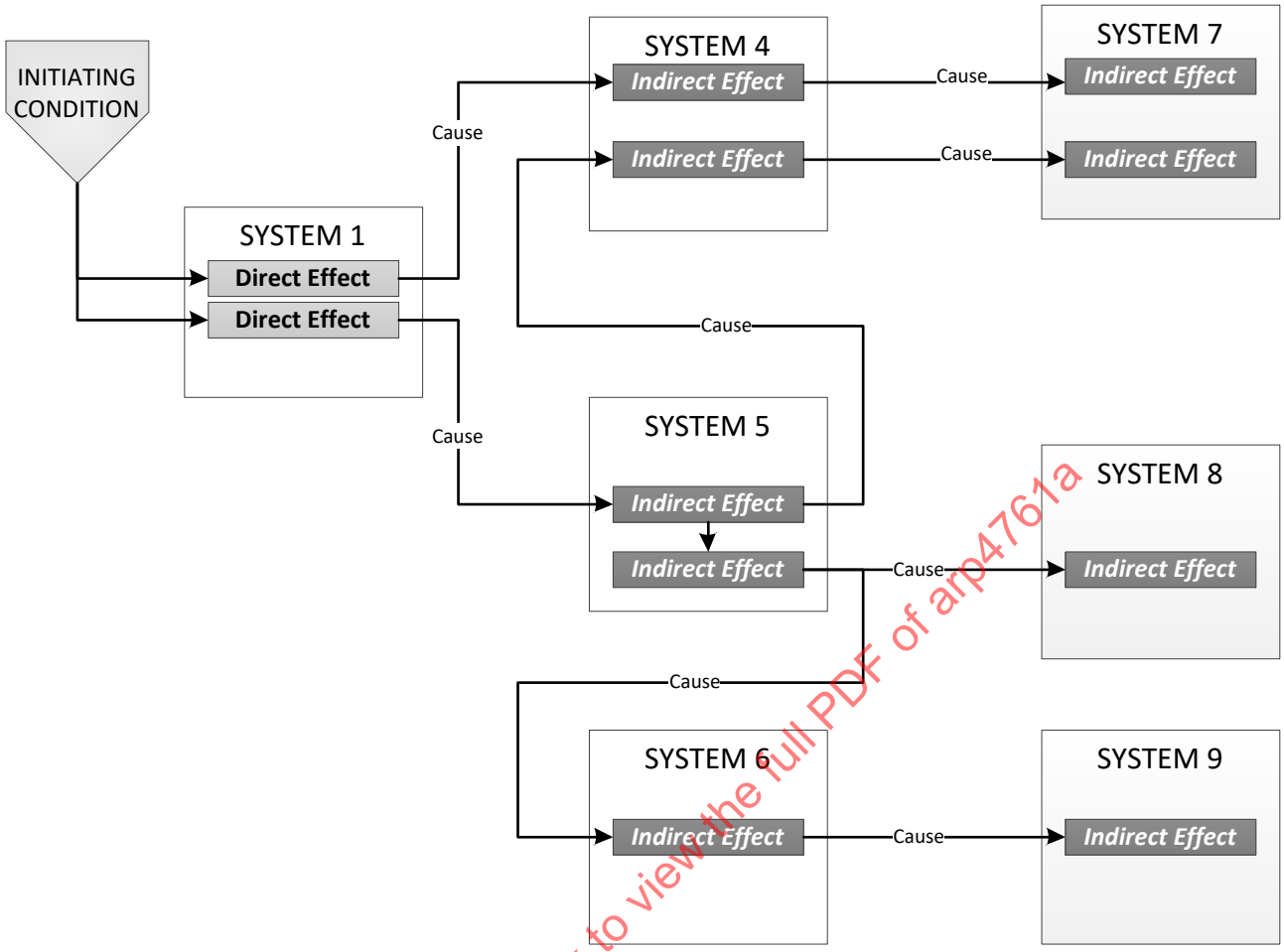


Figure O6 - Aircraft effect determination example, final

O.4.3 Cascade Effect Analysis Results

When the activities in O.4.1 and O.4.2 are complete, the cascade analysis effects results are returned to the source analysis (e.g., AFHA, SFHA, PASA, PSSA). The completed aircraft cascade effect analysis is the combined airplane response for the affected aircraft or system functions, including any crew alerts or indications that will be caused by the condition. The source analysis should determine acceptability of the total aircraft effects. Where the source analysis requires a level of confidence generally obtained by testing, the total aircraft effects for some or all of the initiating conditions may be confirmed by laboratory or prototype tests.

O.5 CEA OUTPUTS

The CEA outputs include:

a. For each CEA initiating condition, the CEA extent definition and rationale.

b. For each CEA initiating condition, a list of the affected systems and effects associated with the initiating condition.

c. Assumptions used in the analysis.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX P - FUNCTION AND ITEM DEVELOPMENT ASSURANCE ASSIGNMENT (FDAL/IDAL)

NOTE: The main body of this document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

TABLE OF CONTENTS

P.1 INTRODUCTION ... 331
P.1.1 Function/Item Development Assurance Level Assignment Process Overview ... 331

P.2 FDAL AND IDAL ASSIGNMENT INPUTS ... 332
P.2.1 AFHA and SFHA Failure Condition Data ... 332
P.2.2 Function/Sub-Function Descriptions ... 332
P.2.3 Proposed Aircraft/System Architecture ... 332
P.2.4 Relevant PASA or PSSA Safety Data ... 332

P.3 FDAL ASSIGNMENT ... 332
P.3.1 FDAL Assignment without Architectural Considerations ... 332
P.3.2 FDAL Assignment with Architectural Considerations ... 333
P.3.3 FDAL Assignment in Consideration of External Events ... 339
P.3.4 Flight Phase Considerations for FDAL Assignment ... 339

P.4 IDAL ASSIGNMENT ... 340
P.4.1 IDAL Assignment Additional Considerations ... 343

P.5 ADDITIONAL CONSIDERATIONS ... 343
P.5.1 Reusing Legacy FDALs and IDALs ... 344
P.5.2 Reusing Legacy Design Assurance Levels or Software Level Assignments ... 344

P.6 FDAL AND IDAL ASSIGNMENT OUTPUTS ... 345

P.7 FDAL AND IDAL ASSIGNMENT CASES ... 345
P.7.1 Case 1: Neither Functional nor Item Development Independence ... 345
P.7.2 Case 2: Functional Independence and Item Development Independence ... 345
P.7.3 Case 3: Functional Independence is Claimed but not Item Development Independence ... 347
P.7.4 Case 4: No Functional Independence but Item Development Independence ... 350

Figure P1 FDAL/IDAL assignment process overview ... 331
Figure P2 FDAL assignment process flow chart with architecture considerations ... 338
Figure P3 Protection function FDAL assignment as a function of probability of an external event ... 339
Figure P4 IDAL assignment process flow chart with architecture considerations ... 341
Figure P5 Function independence and item development independence ... 346
Figure P6 Development dependency of multiple function in the same failure condition ... 349

Table P1 Top-level function FDAL assignment ... 333
Table P2 Development assurance level assignment to members of a Functional Failure Set ... 334
Table P3 Example assurance assignment for design dependency of multiple functions same failure condition ... 347
Table P4 Example assurance assignment for design dependency of multiple functions same failure condition ... 350

SAENORM.COM : Click to view the full PDF of arp4761a

P.1 INTRODUCTION

This appendix provides information on the process for assigning Function Development Assurance Levels (FDAL) and Item Development Assurance Levels (IDAL) within the safety assessment process. The assignment processes described herein are typically accomplished as part of the Preliminary Aircraft Safety Assessment (PASA) and Preliminary System Safety Assessment (PSSA). The acceptable assignment principles and criteria have been established in ARP4754B/ED-79B, Section 5.2. The FDALs modulate the system development rigor (ARP4754B/ED-79B), while IDALs modulate the item development rigor for software (DO-178C/ED-12C) and electronic hardware (DO-254/ED-80). Application of this process should be reconsidered each time any of the Functional Hazard Assessments (FHAs) is revised; the aircraft/system architecture is modified; during the PSSA when all causes of the failure conditions (FCs) need to be identified and reassessed; or any time the development assumptions are changed.

NOTE: Advisory material may specify the FDAL or IDAL at a level different than identified using ARP4754B/ED-79B guidelines. The applicant should discuss the role of the advisory material in the FDAL and IDAL assignment process with the certification authority.

P.1.1 Function/Item Development Assurance Level Assignment Process Overview

The process for assigning the FDALs and IDALs is summarized in Figure P1. The FDAL/IDAL assignment process uses inputs from both the aircraft and system development processes as well as safety assessment processes.

The assurance level assignment process is described in two phases: assigning the FDAL and assigning the IDAL.

- FDAL assignment: During this phase, the FDAL is assigned initially, based only on the function and the associated failure condition classification of the failure conditions to which it is contributing. Then the functions are evaluated for independence in their Functional Failure Sets (FFS) for potential FDAL assignments based on architectural considerations.

- IDAL assignment: The IDAL assignment follows the FDAL assignment process. During this phase, the lower-level item designs that implement the functions are evaluated for independence for assignment of the IDALs, again, based on Functional Failure Sets if architectural considerations are used. If independence cannot be confirmed, then this lack of independence should be fed back to the FDAL and/or IDAL assignment process.

SAENORM.COM : Click to view the full PDF of arp4761a

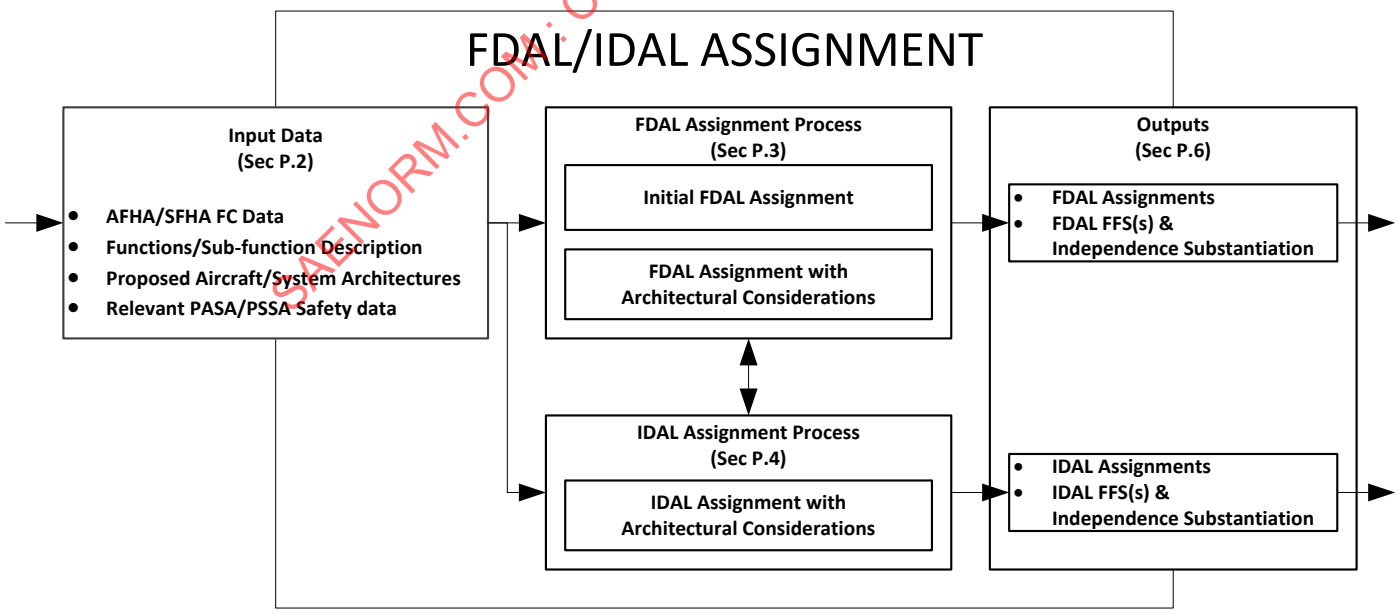


Figure P1 - FDAL/IDAL assignment process overview

P.2 FDAL AND IDAL ASSIGNMENT INPUTS

The inputs outlined in this section constitute the minimum data necessary for the allocation of FDALs and IDALs.

- Aircraft Functional Hazard Assessment (AFHA) and System Functional Hazard Assessment (SFHA) failure condition data.
- Function/sub-functions descriptions.
- Proposed aircraft/system architecture.
- Relevant PASA or PSSA safety data.

P.2.1 AFHA and SFHA Failure Condition Data

The failure conditions and their associated failure condition classifications are input from the AFHA and/or SFHA. Each function may have multiple failure conditions with multiple associated failure condition classifications. The FDAL/IDAL assignment process considers the complete set of failure conditions associated with each function.

P.2.2 Function/Sub-Function Descriptions

The function and sub-function descriptions are provided from the aircraft or system development process to aid the FDAL/IDAL assignment process in describing the FFS relationships.

P.2.3 Proposed Aircraft/System Architecture

The proposed aircraft architecture definition includes the aircraft function allocations to systems, system interactions, common resource systems, and other dependencies. As the design matures, a more detailed representation of the architecture may iteratively be applied to the process.

A conceptual representation of the proposed system architecture from the system development process is essential to allow evaluation of the architecture's ability to meet the objectives associated with the FC classifications from the AFHA or SFHA and the requirements for the architecture. The architecture definition aids the analyst in describing the FFS relationships.

P.2.4 Relevant PASA or PSSA Safety Data

The PASA or PSSA safety assessments have additional architectural or development information useful in establishing independence characteristics. These assessments may include FDALs from the PASA or from another PSSA, FFS information, independence claims evaluation, and other data to support FDAL and IDAL allocation. Also included in this data set are the requirement sets and development process data which will be evaluated to determine if it is reasonable to achieve necessary independence.

P.3 FDAL ASSIGNMENT

P.3.1 FDAL Assignment without Architectural Considerations

The assignment process begins with FDAL assignment to the functions as analyzed in the AFHA and/or SFHA. Each FC is selected and the appropriate development assurance level assignment is made corresponding to the severity of the FC classification. The level assigned is an alphabetical value based on the qualitative failure condition classification as indicated in Table P1. In general, if the FC under consideration is from the AFHA, this FC would be considered the top-level FC. In addition, if there is a unique FC that is at the system-level, then that can also be a top-level FC.

SAENORM.COM : Click to view the full PDF of arp4761a

Table P1 - Top-level function FDAL assignment

Top-Level Failure Condition Classification	Associated Top-Level Function FDAL Assignment
Catastrophic	A
Hazardous	B
Major	C
Minor	D
No Safety Effect	E

If the architecture considerations (specifically functional independence) are not used, the FDAL assignment process is straightforward. Table P1 is used to directly assign the FDAL for all associated functions. For each AFHA/SFHA failure condition, the FDAL commensurate with the failure condition classification is assigned to all functions contributing directly or in combination to this failure condition. If a function has multiple FDAL assignments from this process, then the highest level of FDAL assignment is selected as the final assignment for that function.

When the mitigation strategy for systematic errors is a single FDAL A development process for a Catastrophic failure condition, then the applicant may be required to substantiate that the development process for that member has sufficient independent validation/verification activities, techniques and completion criteria to ensure that potential development error(s) having a Catastrophic effect have been removed or mitigated. In this case, the development assurance process needs to provide confidence that development error(s) will be detected and resolved within the process rather than relying on independence within the architecture.

P.3.2 FDAL Assignment with Architectural Considerations

If the analyst elects to consider the aircraft/system architecture for the FDAL assignment, there are a number of considerations which are to be satisfied. This section describes the process and criteria for considering architectures in the FDAL assignment process.

P.3.2.1 FDAL Assignment Introduction

Once an FDAL is assigned based on a top-level FC, the architecture of the functions involved in that top-level FC may be examined to determine the FDALs of those functions. The process for assigning FDAL with architecture considerations is described in P.3.2.4. The FDAL assignment process relies on the identification of potential error sources which may result in the associated function failure conditions. The error sources may result in loss of, anomalous behavior, or both for a function (or item) for which FDAL (or IDAL) is being assigned. The assignment process also evaluates if it is reasonable to achieve the necessary independence between these sources to mitigate the occurrence of the FC.

P.3.2.2 Independence Between Aircraft/System Functions or Items

Independence between aircraft/system functions (or items) can mitigate potential error sources and is a fundamental attribute to consider when assigning FDALs (and IDALs). Independence is evaluated to identify if it is reasonable that common sources of errors can be minimized between two or more members. This independence ensures that the function requirements should not suffer from a common error as described under independence attributes in ARP4754B/ED-79B, Section 5.2. Functional Failure Sets are the means for identifying the independence necessary between members that, in combination, contribute to FCs. A Common Mode Analysis (CMA), or equivalent techniques, may be used to substantiate that the FFS members claimed to be independent—be they functional or item members—are indeed independent; see the Independence Principles discussed in the PASA, B.4.2, and PSSA, D.4.2.2.1. On that basis, the FFS members can then be assigned FDALs (or IDALs) in line with the assignment principles and criteria which have been established in ARP4754B/ED-79B, Section 5.2, options for multiple members. Table P2 illustrates the principles. ARP4754B/ED-79B should be referenced for more detail on these principles. Considerations for an FFS with a single member can be found in P.3.1.

SAENORM.COM : Click to view the full PDF of arp4761a

Table P2 - Development assurance level assignment to members of a Functional Failure Set

Top-Level Failure Condition Classification	Development Assurance Level		
	Functional Failure Sets with a Single Member (Steps g and s)	Functional Failure Sets with Multiple Members (Steps h and r)	
		Option 1	Option 2
Column 1	**Column 2**	**Column 3**	**Column 4**
Catastrophic	FDAL (IDAL) A	FDAL (IDAL) A for one member, additional member(s) contributing to the top-level failure condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level failure conditions (but no lower than level C for the additional members).	FDAL (IDAL) B for two of the members leading to top-level failure condition. The other member(s) at the level associated with the most severe individual effects of an error in their development process for all applicable top-level failure conditions (but no lower than level C for the additional members).
Hazardous/ Severe Major	FDAL (IDAL) B	FDAL (IDAL) B for one member, additional member(s) contributing to the top-level failure condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level failure conditions (but no lower than level D for the additional members).	FDAL (IDAL) C for two of the members leading to top-level failure condition. The other members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level failure conditions (but no lower than level D for the additional members).
Major	FDAL (IDAL) C	FDAL (IDAL) C for one member, additional member(s) contributing to the top-level failure condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level failure conditions.	FDAL (IDAL) D for two of the members leading to top-level failure condition. The other members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level failure conditions.
Minor	FDAL (IDAL) D	FDAL (IDAL) D for one member, additional member(s) contributing to the top-level failure condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level failure conditions.	
No Safety Effect	FDAL (IDAL) E	FDAL (IDAL) E	

SAENORM.COM : Click to view the full PDF of arp4761a

P.3.2.3 Functional Failure Sets

The systematic approach to assigning FDALs (and IDALs) with architecture considerations employs the concept of Functional Failure Sets (FFS).

Fault Tree Analysis (FTA) combinatorial models typically represent how a system fails and results in the failure condition being analyzed. The minimum set of failures which result in this undesired result is known as a minimal cut set. Conceptually, for FDAL (and subsequently IDAL) assignment purposes, an FFS is analogous to a minimal cut set. Rather than consider combinations of physical failures, the FFS represents the minimum combination of potential development errors that may cause failures, which result in the same effect as those failures. The FFS is used to identify combinations of members which may lead to each FC. This analysis may be used to assign the appropriate rigor to mitigate the potential errors. An FC may be caused by a single FFS or multiple FFSs, and each FFS may contain either single or multiple members.

FFSs are identified using inputs from the proposed aircraft/system architecture as well as the development assurance strategy for the functions. The associated functional members are identified at an appropriate level of functional decomposition to support the development process. The specific tool or method used to develop each FFS is left to the analyst. For illustration purposes, this appendix uses an FTA to capture and present FFS models.

Some inputs or outputs to/from an architecture under consideration may not contribute to the FFS (and, as a result, not appear in the MCS). For such cases, clear substantiation must be provided to establish that these inputs/outputs are not member(s) in the FFS and do not interfere. To establish this, protections provided by the more critical function(s) should be identified and discussed. A bottom-up confirmation should be used to establish that function(s) developed to one FDAL are not adversely affected by errors in the development of functions or items developed to a lesser FDAL or IDAL that are input/output, individually and in combination, but which are not considered part of the FFSs for the FC. Such a confirmation should consider potential erroneous or degraded data or loss of function failure conditions and their associated hazard classifications. These failures, which could result from common modes, must be evaluated to ensure that the lower DAL functions or items cannot affect the higher DAL functions. Requirements may need to be generated to assure the protection of the higher-level function from the lower-level function.

Safety assessment techniques are used to identify sources of error and their combinations which may lead to each failure condition. An FFS for a given failure condition may be identified using qualitative safety modeling techniques such as Fault Tree Analysis (FTA) (see Appendix G), Dependence Diagrams (DDs) (see Appendix H), and other methods used with the modeling of potential development errors that may cause functional failures.

P.3.2.4 Detailed FDAL Process

Figure P2 presents the FDAL assignment process steps which start from a FC identified in the AFHA/SFHA. The assignment identifies FFSs and their members. The process described in Figure P2 is repeated for all of the FCs identified in the AFHA/SFHA. The process is represented in Figure P2 as a single pass. However, it should be understood that there is interaction between the aircraft/system functional levels and thus may require iterations.

Step-by-Step FDAL Assignment Process Description.

a. Select an FC from the AFHA or SFHA.

   Per Section P.2, the lists of FCs identified in the AFHA or SFHA are the input to the FDAL assignment process. Each FC is individually considered at this stage of the assignment process. From the FC input set select one FC for evaluation and FDAL assignment.

b. Assign FDAL per Table P1.

   An FDAL is assigned based on the FC classification per Table P1. For functions that provide protection against an external event, this step may also consider external events per P.3.3.

c. Identify functional level FFSs.

   At this stage of the development process, the generation of the FFSs should be performed to identify associated functional single and multiple members whose errors contribute to the failure condition. See P.3.2.3 for more information on FFSs.

d. Select an FFS.

   Select a single FFS from the identified FFS sets for FDAL assignment. The FDAL assignment process is applied to all identified FFSs and their members for each FC in the AFHA/SFHA.

e. Does FFS have multiple members?

   Determine if the FFS has multiple members. The analyst reviews the FFS to identify if the FFS is made up of a single member or multiple members. A potential FFS multiple member case may be identified when two or more members exist where the FC is caused by a combination of errors from each of those individual members.

   If only a single member exists, proceed to step g.

   If multiple members are identified, proceed to step f.

SAENORM.COM : Click to view the full PDF of arp4761a

f. Are member functional independence claims valid?

The analyst then reviews the FFS multiple members to substantiate independence claims that common sources of error between multiple requirement sets have been minimized at a level of rigor commensurate with the top-level FDAL as described in P.3.2.2 to substantiate independence claims. This confirmation is accomplished by applying a CMA evaluation of the requirement sets and development processes to confirm that the members of the FFS have sufficient differences to satisfy the functional independence. See Appendix M for the CMA evaluation process.

For an FFS with multiple members, functional independence can be claimed when the common sources of error between multiple requirement sets and development processes have been mitigated or minimized. If the presence of common error sources in the requirements and development processes is indeterminate, then functional independence claims are invalid.

If the functional independence claims are valid (i.e., functional independence is true), proceed to step h.

If the functional independence is not substantiated, change the FFS through grouping affected members together in the analysis (i.e., not claiming independence between them) then return to step c. Otherwise, the functional architecture should be reworked in the development process and the FDAL assignment process should be restarted from step a.

g. Assign FDAL to the FFS member per ARP4754B/ED-79B, Section 5.2, as illustrated in Table P2, Column 2.

If the FFS has a single member (i.e., an error in the development of that member can directly result in FC occurrence) then the FDAL is assigned to that member as per its failure condition classification per Table P2, Column 2.

If the FFS has a single member and the mitigation strategy for systematic errors is a single FDAL A development process for a Catastrophic failure condition, then the applicant may be required to substantiate that the development process for that member has sufficient independent validation/verification activities, techniques, and completion criteria to ensure that potential development error(s) having a Catastrophic effect have been removed or mitigated. In this case, the development assurance process needs to provide confidence that development error(s) will be detected and resolved within the process rather than relying on independence within the architecture.

Proceed to step i.

h. Assign FDAL to FFS members per ARP4754B/ED-79B, Section 5.2, as illustrated in Table P2, Option 1 or Option 2.

When the analyst has identified an FFS with multiple members, it is possible to assign the FDAL using either Option 1 or Option 2 of Table P2. The choice to select either Option 1 or Option 2 for FDAL assignment is subject to the discretion/engineering judgement of the analyst.

i. Have all FFSs for the selected FC been assessed?

Once FDALs have been assigned to the members in the selected FFS, the FDAL assignment process is repeated for each of the identified FFSs for the selected FC.

If additional FFS evaluations for a FC remain, return to step d.

After all of the FFSs associated with the selected FC have been evaluated, assign the FDAL based on the highest FDAL identified from all FFSs of which the function is a member.

Once all FFSs have been assessed for a selected FC, proceed to step j.

j. Have all FCs from the AFHA or SFHA for the function been assessed?

Once FDALs have been assigned to all members of all FFSs associated with a selected FC, the FDAL assignment process is applied to each of the other FCs identified in the AFHA/SFHA. Once all FCs from the AFHA/SFHA have been assessed, proceed to step k. Otherwise, return to step a.

SAENORM.COM : Click to view the full PDF of arp4761a

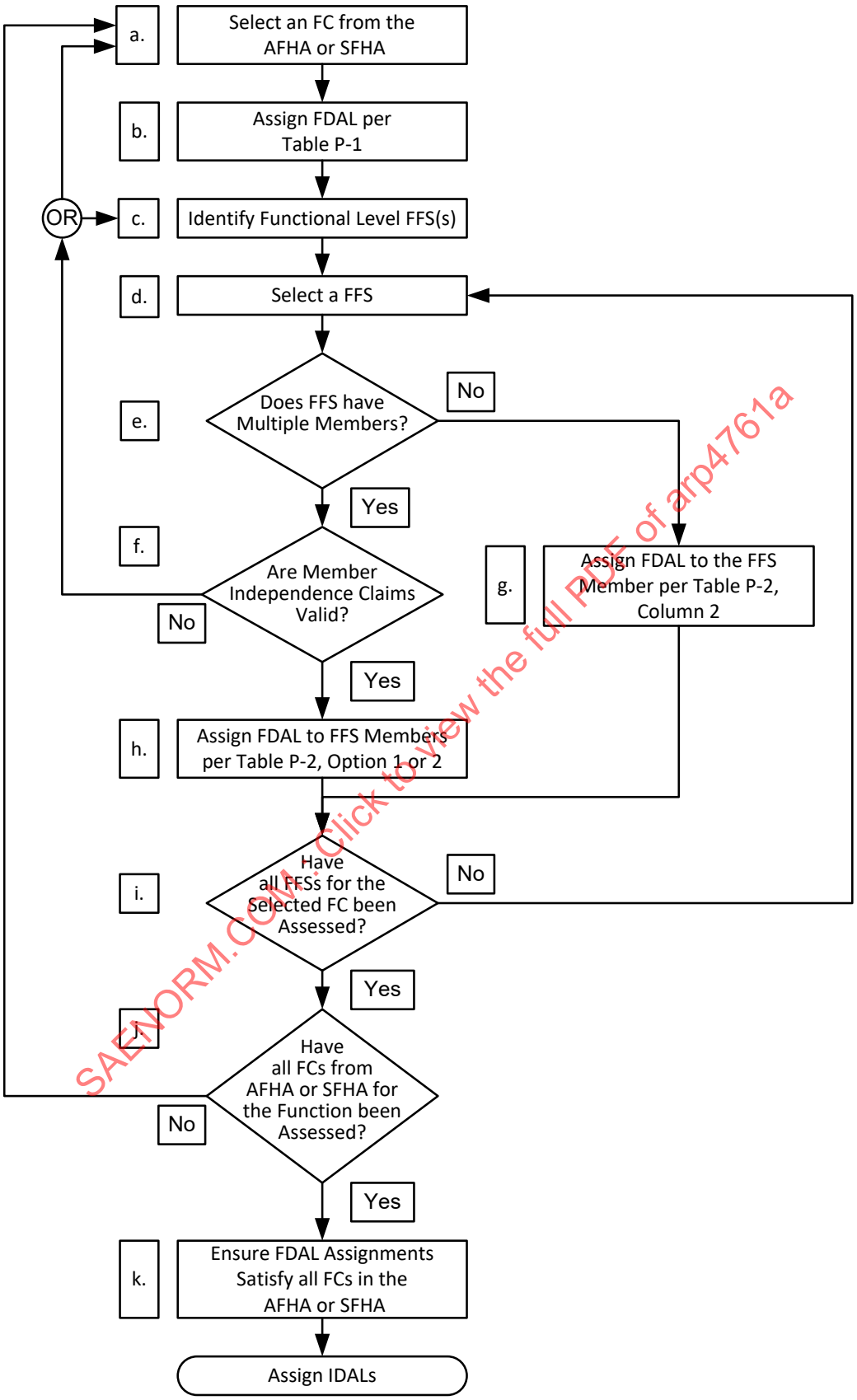
k. Ensure FDAL assignments satisfy all FCs in the AFHA or SFHA.

A final review of the FDAL assignments and failure conditions is initiated to ensure that assignments are consistent across the functions and failure conditions. To accomplish this review, the analyst compiles a list of all functions and ensures that the FDAL assignments satisfy all applicable FFSs and FCs (e.g., FC1 - Level C, FC2 - Level B, FC3 - Level A, FDAL assigned is Level A).

It is recognized that FFSs may share common members and FCs may relate to common functions; therefore, the FDAL assignment to members of all the FFSs for all FCs identified from the AFHA/SFHA are reviewed to ensure that the top-level FDAL for each FC in the AFHA/SFHA is satisfied.

Furthermore, it is recognized that one may need to reassign the appropriate FDAL and/or reallocate functions to ensure the FDAL assignments satisfy the general principles defined in ARP4754B/ED-79B, Section 5.2.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure P2 - FDAL assignment process flow chart with architecture considerations

P.3.3 FDAL Assignment in Consideration of External Events

For systems that provide protection against an event external to the aircraft design, the following guidelines may be applied in cases where there is no existing guidance material prescribing the associated FDAL. An external event is an occurrence which has its origin distinct from the aircraft such as cabin and baggage fires. The concepts illustrated in Table P2 do not apply to functions that protect against an external event. The FHA will consider loss and erroneous operation failure conditions of the protection function which will support assigning an appropriate FDAL to it.

Because the failure condition is defined specifically in relation to the protection against an external event, the consideration of the probability of the event can be used in the determination of the FDAL. This consideration is done in the assignment process of the FDAL of the function protecting against the external event, using Figure P3. First, the failure conditions relative to the protection function are used to identify the top-level failure condition classification. Next, this top-level failure condition classification is used to identify the highest FDAL of the protection function for that loss or erroneous case, from Table P1, which sets the vertical axis value of Figure P3. Finally, the top-level FDAL can be adjusted relative to the probability of the event. This assignment is done by beginning with the FDAL from the top-level FDAL value on the vertical axis of Figure P3 and following the line from that point on the vertical to the right, adjusting the FDAL relative to the stairsteps associated with the probability of the external event identified in the horizontal axis of the figure. If the loss of a protection function combined with the external event is Catastrophic or Hazardous, the FDAL for the protection function alone should be at least Level C. The final FDAL assignment will be the higher of the assignment of the combined loss of the protection function with the external event or the erroneous operation of the protection function.

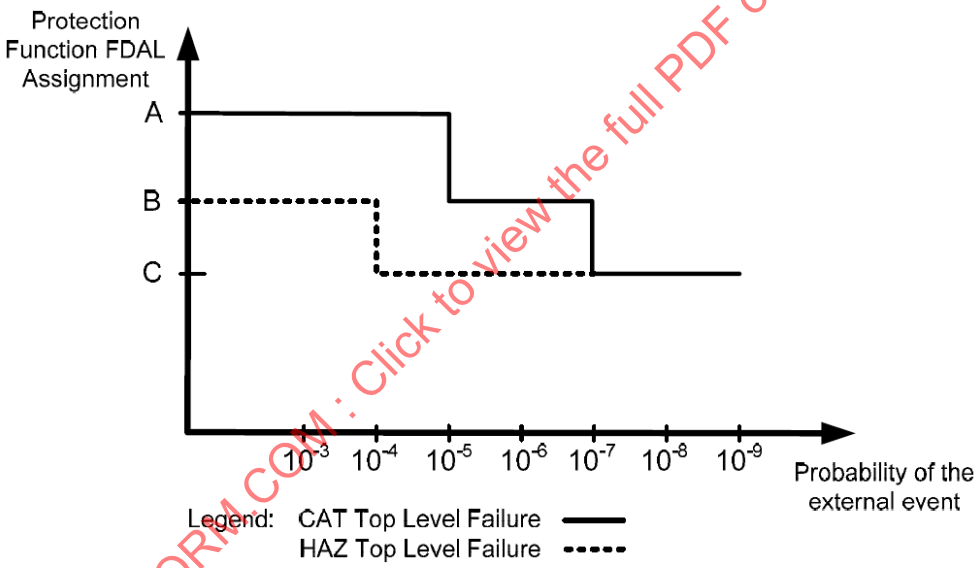


Figure P3 - Protection function FDAL assignment as a function of probability of an external event

SAENORM.COM : Click to view the full PDF of arp4761a

P.3.4 Flight Phase Considerations for FDAL Assignment

Some flight phases occur only occasionally, and these phases may arise in the AFHA/SFHA only when needed to differentiate flight conditions. The circumstances or frequency of any applicable conditional flight phase may be considered when determining the FDAL provided that the conditional flight phase is itself independent of the function, or system whose FDAL is being assigned. Abnormal flight conditions like an impending stall (flying beyond stick shaker), overspeed, or an emergency descent may affect the FDAL assignment and would also be reflected in the associated failure conditions in the FHA. Operations and operational flight phases that are intentionally performed (e.g., autoland or Extended-Range Operations (ETOPS) segments) would not be able to include this consideration in its FDAL justification. In this case, the applicant should substantiate to the Certification Authorities that the applicant's proposed development assurance process meets an acceptable level of safety.

P.4 IDAL ASSIGNMENT

The process for assigning IDALs is shown in Figure P4 and is accomplished as part of a PSSA process. The IDAL assignment process assigns IDALs to identified FFSs and their associated members. The process is again represented as a single pass. However, it should be understood that there is interaction between the system functional levels and thus may require multiple iterations across the FDAL/IDAL boundary.

The IDAL assignment process of Figure P4 is top-down, starting after the assignment of FDALs described in Section P.3 culminating with assignment of the IDALs to items (software/electronic hardware). Per Section P.2, the list of FCs identified in the SFHA is an input to the IDAL assignment process. The assigned FDALs and applicable FFSs are also inputs to the IDAL assignment process, and it is essential the IDAL assignment stay within the same row of Table P2 applied during the FDAL assignment.

Additional inputs for system functions, assigned FDALs, applicable FFSs, and FCs from the FDAL assignment process should also be considered in the IDAL assignment activity.

l. Select an FC from the SFHA.

   Select an FC for evaluation and IDAL assignment.

m. Identify FFS(s) associated with items or combined items and functions.

   Each functional level FFS will have one or more associated item-level FFS(s). Furthermore, FFSs may exist that combine functions and items. The item-level FFS(s) and any FFSs with combined items and functions should be identified using the techniques discussed in P.3.2.3.

n. Select an FFS.

   Select a single FFS from the identified FFSs.

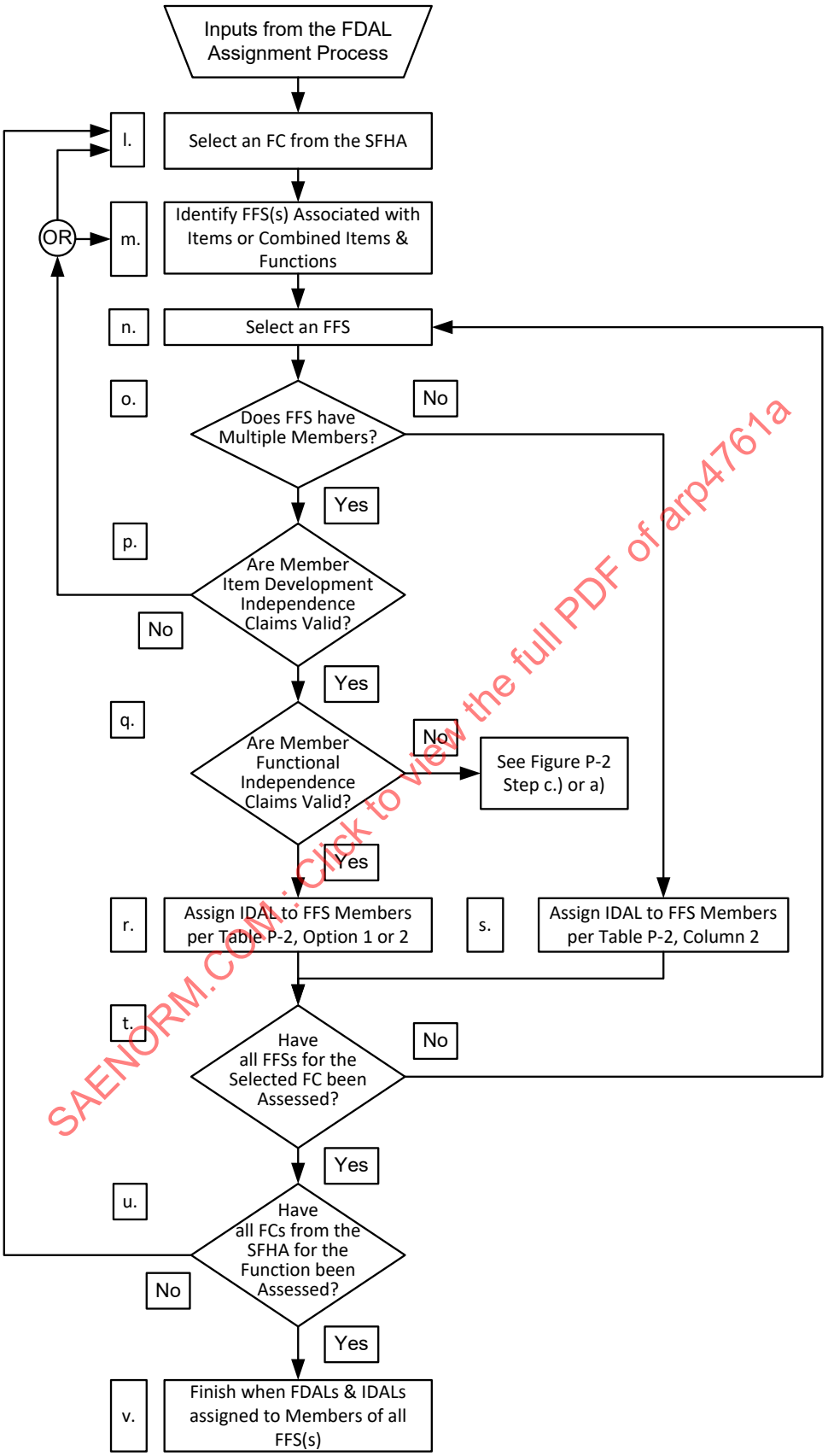
o. Does the FFS have multiple members?

   Determine if the FFS has multiple members. The analyst reviews the FFS to identify if the FFS is made up of a single member or multiple members. A potential multiple member case may be identified when two or more members exist where the FC is caused by a combination of errors from each of those individual members.

   If only a single member exists, proceed to step s.

   If multiple members are identified proceed to step p.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure P4 - IDAL assignment process flow chart with architecture considerations

p. Are member item development independence claims valid?

The analyst then reviews the FFS multiple members to confirm that they are sufficiently independent as described in P.3.2.2 to substantiate independence claims. This confirmation is accomplished by applying a CMA evaluation of the requirements and development processes to confirm that the members of the FFS have sufficient differences to satisfy the item development independence. See Appendix M for the CMA evaluation process. For an FFS with multiple members, item development independence is substantiated when the common sources of error between multiple item requirement sets have been mitigated or minimized. If the presence of common error sources in the item is indeterminate, then item development independence claims are invalid.

If the item development independence is not substantiated, change the FFS through grouping affected members together in the analysis (i.e., not claiming independence between them) then return to step m. Otherwise, the architecture should be reworked in the development process and the IDAL assignment process should be restarted from step l.

If item development independence claims have been maintained, proceed to step q.

q. Are member functional independence claims valid?

If the item development independence claims are valid (item development independence is true), review the functional independence claims for the FC to substantiate that the functional independence claims remain valid.

If the functional independence is not substantiated, change the FFS through grouping affected members together in the analysis (i.e., not claiming independence between them), then return to step c. Otherwise, the architecture should be reworked in the development process and return to step a.

If functional independence claims have been maintained, proceed to step r.

r. Assign IDAL to FFS members per ARP4754B/ED-79B, Section 5.2, as illustrated in Table P2, Option 1 or Option 2.

When the analyst has identified an FFS with multiple members, it is possible to assign the IDAL using either Option 1 or Option 2 of Table P2. It is essential that the IDAL assignment stay within the same row of Table P2 applied during the FDAL assignment, from Section P.3. The choice of which option to select is at the discretion of the analyst.

Proceed to step t.

s. Assign IDAL to FFS member per ARP4754B/ED-79B, Section 5.2, as illustrated in Table P2, Column 2.

If the FFS has a single member (i.e., an error in the development of that member can directly result in the FC being assessed), then the IDAL should be assigned to that member per Column 2 of Table P2, staying within the same row applied during the FDAL assignment.

If the FFS has a single member and the mitigation strategy for systematic errors is a single IDAL A development process for a Catastrophic failure condition, then the applicant may be required to substantiate that the development process for that member has sufficient independent validation/verification activities, techniques and completion criteria to ensure that potential development error(s) having a Catastrophic effect have been removed or mitigated. In this case, the development assurance process needs to provide confidence that development error(s) will be detected and resolved within the process rather than relying on independence within the architecture.

t. Have all FFSs for the selected FC been assessed?

Once IDALs have been assigned to the members in the selected FFS, the IDAL assignment process is repeated for each of the identified FFSs for the selected FC. After all of the FFSs associated with the selected FC have been evaluated, assign the IDAL based on the highest level of rigor identified for all associated FFSs.

Once all FFSs have been assessed for a selected FC, proceed to step u. If additional FFS evaluations for a FC remain, return to step n.

SAENORM.COM : Click to view the full PDF of arp4761a

u. Have all FCs from the SFHA for the function been assessed?

Once IDALs have been assigned to all members of all FFSs associated with the selected FC, the IDAL assignment process should be applied to each of the other FCs identified in the SFHA. Once all FCs have been assessed proceed to step v. Otherwise, return to step l.

v. Finish when FDALs and IDALs assigned to members of all FFSs.

The FDAL and IDAL assignment process is complete, when all FCs identified in the AFHA and SFHA have been addressed, and FDALs and IDALs for all members have been identified to satisfy the general principles defined in ARP4754B/ED-79B, Section 5.2.

It is recognized that FFSs may share common members and FCs may relate to common functions and/or items; therefore, the FDAL and IDAL assignment to members of all the FFSs members for all FCs identified in the AFHA and SFHA should be reviewed to ensure that the top-level FDAL for each FC in the AFHA and SFHA is satisfied, and that FDALs and IDALs for all FFS members have been identified to satisfy the general principles defined in ARP4754B/ED-79B, Section 5.2 (e.g., FC1 - Level C, FC2 - Level B, FC3 - Level A, IDAL assigned is Level A).

P.4.1 IDAL Assignment Additional Considerations

When applying the IDAL process to a given aircraft/system architecture, the architecture should be reviewed in the context of the following scenarios:

- For some simpler hardware items (e.g., mechanical hardware, electro-mechanical devices, electro valves, or servo valves), their design, including the identification of all their failure modes, can be fully assured by a combination of testing and analysis. Such simpler hardware items do not have an IDAL although the system function using them will have an FDAL. When assigning FDALs and IDALs to other members in the associated FFSs, assignment credit can be taken for these simpler hardware items. Single failures of those simpler hardware items in combination with an error of a complex item leading to a Catastrophic failure condition are key considerations in assigning the IDAL to the complex item(s) involved. In these cases, rationale to substantiate the FDAL and IDAL assignments to the other related FFS members should be provided.

- When assigning IDALs where there is an independence claim between multiple items that may use common hardware or software (e.g., Commercial Off The Shelf (COTS) designs, microprocessors, or other intellectual property), consideration should be given to how these common components are used in the architecture. Different usage contexts and a proper understanding of how these differences provide protection from common development errors directly causing a failure condition may be sufficient to justify independence.

P.5 ADDITIONAL CONSIDERATIONS

Some advisory materials (e.g., Traffic Collision Avoidance System) drive the FDAL/IDAL assignment to be more severe than this process would reach; in such a case, the FDAL/IDAL assignment from the advisory material becomes an additional design constraint.

The application of the concepts illustrated in Table P2, Option 1 or Option 2 when assigning FDALs and IDALs to an FFS with multiple members is the choice of the analyst. However, consideration for these choices may include:

- For a given top-level failure condition, it is necessary to stay in the same row of Table P2 no matter the number of functional decompositions performed (for example, for a Catastrophic failure condition any level of decomposition below that top-level failure condition should include at least one FDAL A or two FDAL B members. Any additional members FDAL should not be lower than FDAL C).

- The assignment of FDAL to each FFS member is independent of their numerical availability. However, if there is a large disparity between the numerical availability of the members in the FFS, it may be beneficial to assign the higher-level FDAL to the higher availability member.

The FDAL and IDAL of reused members may also be considered. Guidance for determining the applicability of reused FDALs and IDALs is presented in P.5.1.

SAENORM.COM : Click to view the full PDF of arp4761a

P.5.1 Reusing Legacy FDALs and IDALs

Some development projects include plans to reuse systems, hardware or software from a prior approved baseline configuration. These reuse cases may be based on systems, hardware or software that were previously developed using FDALs and IDALs assigned per ARP4754A/ED-79A or subsequent revisions. See P.5.2 for cases using legacy design assurance levels or software level assignments. For reuse, a modification impact analysis is performed per the development process. Refer to ARP4754B/ED-79B for more information on modification impact analysis.

The FDALs associated with reused systems or items may be applicable to a new aircraft. This applicability would be determined through a modification impact analysis of that system or item for similarity in the new aircraft. This analysis should show that the reused system or item is applying its functionality in the same or similar way on this new aircraft, resulting in the same or similar failure conditions, which result in the same failure condition classifications. It should further be confirmed that these functions were developed using FDALs and IDALs per ARP4754B/ED-79B in alignment with these failure conditions and their classifications. The evaluation should also ensure that legacy functionality will not result in unintended functionality for the new aircraft. This evaluation should include consideration of the whole of the reused system, both the portions that are being reused, and those portions not being reused, but are resident. The prior PASA and PSSAs FDAL and IDAL assignment results can be integrated into the new aircraft analysis to demonstrate alignment so long as all of the legacy failure conditions of that system aligns with its new usage.

P.5.2 Reusing Legacy Design Assurance Levels or Software Level Assignments

For baselines that were developed using older standards that did not distinguish between FDALs and IDALs or that focused only on what are now called IDALs (e.g., DO-178B/ED-12B, DO-254/ED-80), these legacy design assurance levels or software level assignments may be considered as initial IDAL assignments subject to confirmation by the assignment process described in this section.

If there is no clear FDAL for the legacy system baseline, it should be shown that these legacy design assurance levels satisfy the general principles defined in ARP4754B/ED-79B, Section 5.2. The use of legacy design assurance levels or software levels in the new application may consider:

- Any changes to the applicable AFHA and SFHAs to identify any new failure conditions or changes to the failure condition classification of legacy failure conditions.
- Whether the architecture is changed or if any functional independence or item development independence explicitly or implicitly claimed in the legacy system is affected. This scenario is for cases where the legacy design assurance levels or software levels were assigned with consideration of the architecture.
- The legacy design assurance levels or software levels as possible constraints when deciding whether to use Option 1 or Option 2 of Table P2 to address new failure conditions or those with changed failure condition classification.

If the legacy design assurance levels or software level cannot be confirmed as an IDAL in the new application, a developer may change either the new (non-legacy) functions or allocations of functions in order to preserve the legacy design assurance level or software level assignments. If the new function or allocations of functions are modified, then the IDAL assignment process should be repeated to confirm that the assignment is successful in preserving the legacy design assurance level or software level. The designer should ultimately confirm that the legacy design assurance level or software level is still appropriate for any shared environment with the new function or allocations of functions (e.g., any implicit, explicit, architectural, or use case assumptions that were used to obtain the legacy IDAL should be revalidated in the context of the item's operating environment).

FDAL and IDAL assignment steps for new application:

a. Identify all items being reused within the aircraft or system and their design assurance levels or software level assignments.

b. Identify all new items within the system and their design assurance levels or software level assignment (if it has been assigned yet).

c. With the new AFHA, SFHA, and proposed system architecture information, perform the FDAL and IDAL assignment process described in this appendix.

SAENORM.COM : Click to view the full PDF of arp4761a

d. Assign FDALs for the functions performed by the system.

e. Use the reused item's legacy design assurance levels or software levels as their initial IDAL assignments if the project plan is to leave them unchanged.

f. Assign IDALs as needed to new or significantly changed items.

g. Affirm the FDALs and IDALs based on the checks described in this appendix.

h. If shortcomings in the FDAL and/or IDAL assignment arise, refine the legacy design assurance levels or software level assignment. To refine the legacy design assurance levels or software level assignment it may become necessary to change the architecture, constrain the functions being performed, reallocate the planned system changes to affect the modification impact analysis, or elevate the new IDAL of certain items to meet the needs of the assignment process described in this appendix. This may include a reassessment of unmodified software partitions.

i. Capture the results of the final assignment, impact on system requirements, and other relevant information in accordance with the output section of the relevant process (i.e., PSSA).

P.6 FDAL AND IDAL ASSIGNMENT OUTPUTS

Completion of FDAL and IDAL assignment includes a description of the FFS analysis per failure condition and architecture. The FFS provides context for these outputs by identification of necessary independencies between functions or items in order to prevent common error sources from resulting in more than one member failing. The FDAL and IDAL assignment process generates the following outputs.

- Assigned FDALs.
- FDAL FFS(s) and Independence Principles.
- Assigned IDALs.
- IDAL FFS(s) and Independence Principles.

P.7 FDAL AND IDAL ASSIGNMENT CASES

The following cases illustrate how the FDAL and IDAL assignment principles in ARP4754B/ED-79B apply. The cases include the identification of steps defined in the preceding sections.

P.7.1 Case 1: Neither Functional nor Item Development Independence

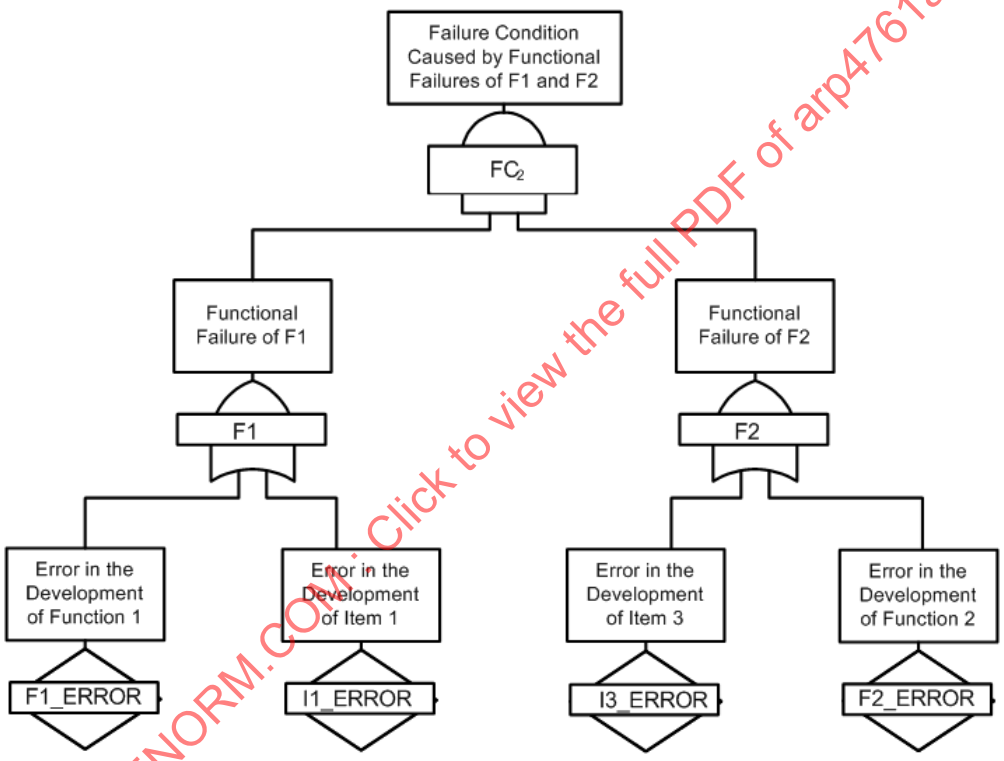
If there is no functional independence and no item development independence, Table P1 is used to assign the FDAL and IDAL. The FDAL and IDAL are the same and are equal to the FDAL of the top-level function.

P.7.2 Case 2: Functional Independence and Item Development Independence

This case represents the activities if both functional and item development independence are present. After proceeding through steps a. through d. of P.3.2.4, this case will assume that the FFS has multiple members in step e. Once independence is validated per step f., assign the FDAL, per step h., using the assignment principles in ARP4754B/ED-79B, Section 5.2, as illustrated in Table P2, Option 1 or Option 2. After assignment, confirm the successful review of all FFSs and FCs, per steps i. through j.. Per step k., a review of the FFSs representing combinations of errors in both aircraft/system functions should be performed to ensure FDAL assignments are compliant with the general principles defined in ARP4754B/ED-79B, Section 5.2. The purpose of reviewing these is to ensure that all possible combinations of errors in the development of aircraft/system functions are adequately mitigated by FDAL assignment.

SAENORM.COM : Click to view the full PDF of arp4761a

Similar to the assignment of FDALs, the assignment of IDALs will proceed through the steps in P.3.3. After proceeding through steps l. through n., this case will assume that the FFS has multiple members in step o. Once the item development independence claims are validated, per step p), review functional independence in step q. to assure it has not been violated. Assuming the independence is valid for this case, assign the IDAL, per step r., using the assignment principles per ARP4754B/ED-79B, Section 5.2, as illustrated in Table P2 (by substituting IDAL to FDAL). Option 1 or Option 2 of the decision related to the top-level FC classification (i.e., same decision of Figure P4 as FDAL assignment) can be used for the IDAL assignment. The example shown in Figure P5 and Table P3 illustrates two invalid IDAL assignments given an FDAL assignment for F1 and F2 of B for a Catastrophic top-level failure condition FC2 with a FDAL A. After assignment, confirm the successful review of all FFSs and FCs, per steps t. through u. Per step v., a review of the FFSs representing combinations of errors in the items should be performed to ensure IDAL assignments are compliant with the general principles defined in ARP4754B/ED-79B, Section 5.2. The purpose of reviewing these is to ensure that all possible combinations of errors in the development of items are adequately mitigated by IDAL assignment. (Figure P5 shows the combinations of independent errors which lead to the FC. Table P3 describes proposed FDAL and IDAL assignment combinations based on the independent error combinations identified in Figure P5 to illustrate the points of Case 2 and the general principles of ARP4754B/ED-79B, Section 5.2 and is not intended to illustrate presentation methodologies.)



SAENORM.COM : Click to view the full PDF of arp4761a

Figure P5 - Function independence and item development independence

The minimal equation or terms identifying the FFSs for the FC2 failure condition is:

- F1 error and F2 error, or
- F1 error and I3 error, or
- I1 error and F2 error, or
- I1 error and I3 error.

Table P3 - Example assurance assignment for design dependency of multiple functions same failure condition

FDAL Assignment		IDAL Assignment		Comment
F1	F2	I1	I3	
B	B	B	B	Acceptable
		A	C	Unacceptable: I3 level C does not support FC2 classification as F1 level B and I3 level C not allowed
		C	A	Unacceptable: I1 level C does not support FC2 classification as F2 level B and I1 level C not allowed
A	C	A	C	Acceptable
		C	A	Unacceptable: I1 level C does not support FC2 classification as F2 level C and I1 level C not allowed
		B	B	Unacceptable: I1 level B does not support FC2 classification as F2 level C and I1 level B not allowed
C	A	A	C	Unacceptable: I3 level C does not support FC2 classification as F1 level C and I3 level C not allowed
		C	A	Acceptable
		B	B	Unacceptable: I3 level B does not support FC2 classification as F1 level C and I3 Level B not allowed

Note that some of the FFSs in Table P3 represent combinations of FDAL and IDAL assignments in both aircraft/system functions and items.

P.7.3 Case 3: Functional Independence is Claimed but not Item Development Independence

If independent functions are implemented using non-independent items (or portions of the items that are not independent) and if an error in the development of the non-independent items can lead to a common cause error between some or all of the functions, then the IDAL of the "common" non-independent items needs to be assigned the level of the highest FDAL of the functions implemented by the item. Figure P6 illustrates this condition with item I2 affecting F1 and F2 which leads to the Catastrophic top-level FC with a FDAL A. In other words, if the common cause error can lead directly to a top-level failure condition, the IDAL of the common items is the FDAL of the top-level function assigned based on the top-level failure condition classification. In the Catastrophic case presented in Figure P6, a single member FFS is made up of item I2 and thus an IDAL A is assigned.

The functions implemented in the common design should be partitioned in order to be able to confirm the functional independence claimed for FDAL assignment in step f. of P.3.2.4 and to avoid an error in the development process of one function affecting the other functions through the common design. In step h., the FDAL of the partitioning function should be assigned the FDAL commensurate with the most severe effect of an error in its development; this would be no lower than the highest FDAL of the functions implemented in the common design. In the Catastrophic FC example case provided, the independence requirements defined for F1 and F2 would be an example of a subset of requirements of F1 and F2 having to be developed at FDAL A to ensure the functional independence claims of F1 and F2 are maintained.

Multiple functions with different FDALs may be implemented in a common item with an IDAL that is assigned a level corresponding to at least the highest FDAL of the functions. If partitioning is not used or if its independence cannot otherwise be substantiated in step f., the IDAL of the common design might force a reconsideration of the FFS and reassignment of the FDAL of the Functions implemented in that design at the level of IDAL of the common item design. This reconsideration may cause the FFS to become a single member per step e. in which case the FDALs will be assigned per step g. This is typically the case when the implementation layer of a function, or part of a function, cannot be protected by the partitioning mechanism (e.g., implementation of real time sequencing functions in operating system layer or in micro-program layer). In that case, the FDAL of the functions that cannot be protected by the partition mechanism will need to be reassigned at the IDAL of the common item. Alternately, a new multi-member FFS may be identified for the FC in step e., validated in step f., and then FDALs assigned to those members per step h. In this case, the upper-level functions may be reallocated to the items to separate the independent and common portions of the design.

SAENORM.COM : Click to view the full PDF of arp4761a

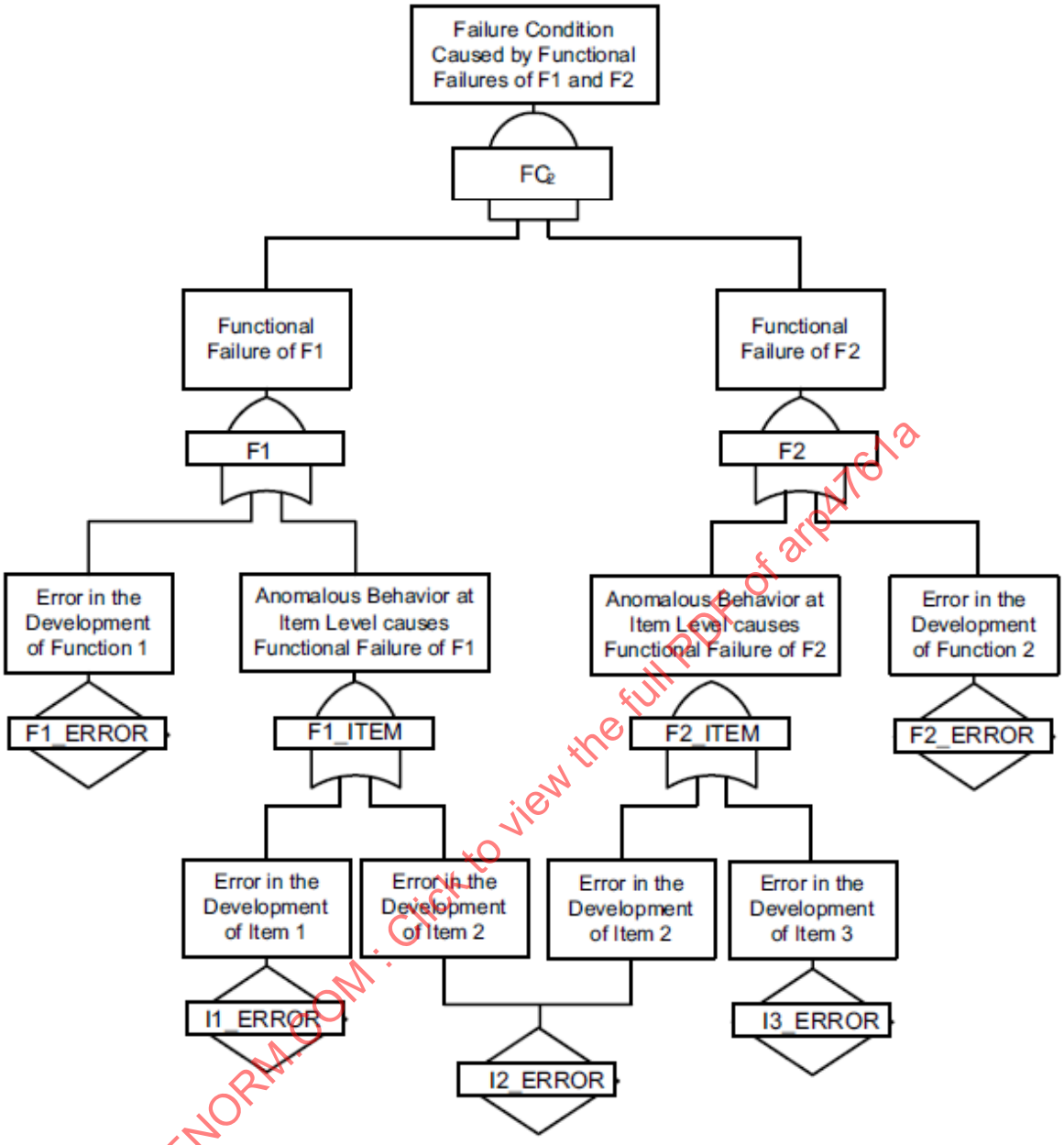
IDAL assignments that reflect the FDAL assignment of independent aircraft/system functions will need to substantiate that their development have minimized the sources of common development errors across the functional independence boundary. For example, if two functions (F1 and F2 in Figure P6) performing a FDAL A function are performing functions established as independent from one another and assigned a FDAL B (Option 2 in Table P2), the functional requirements are required to be developed to an FDAL B and it will be necessary to substantiate functional independence for these two functions. Further, the interactions between the pair of FDAL B Functions and interactions between their IDAL B items (Item I1 and Item I3 in Figure P6) need to be captured and validated at FDAL A under the aircraft function even though these independent aircraft/system functions and items are individually level B.

If the items implementing the functionally independent FDAL B functions have any common items that would prevent a claim for item development independence, an IDAL A assignment would be necessary for at least the common portion as shown as Item I2 in Figure P6. The item boundaries may be shaped iteratively along interfaces that can be used to substantiate the independence, but any common portion that remains would need to be assigned IDAL A. As in the case noted above of completely independent IDAL B items, the interactions between the pair of FDAL B functions and interactions between their IDAL B items and their common IDAL A item need to be validated at FDAL A under the complete aircraft-level function even though some portions of this aircraft-level function are individually level B.

Review the FFSs representing combinations of errors in both aircraft/system functions and items to ensure FDAL and IDAL assignments are compliant with the general principles of ARP4754B/ED-79B, Section 5.2. The purpose of reviewing these is to ensure that all possible combinations of errors in the development of aircraft/system functions and items are adequately mitigated by FDAL and IDAL assignment in accordance with the general principles. The example shown in Figure P6 and Table P4 illustrates two invalid IDAL assignments given an FDAL assignment for F1 and F2 of B. (Figure P6 shows the combinations of independent errors which lead to the FC. Table P4 describes proposed FDAL and IDAL assignment combinations based on the independent error combinations identified in Figure P6 to illustrate the points of Case 3 and the general principles of ARP4754B/ED-79B, Section 5.2 and is not intended to illustrate presentation methodologies.)

Independent functions using common resources based on the same designs (e.g., computers, networks, interfaces, and IMA) are likely to require careful consideration.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure P6 - Development dependency of multiple function in the same failure condition

The minimal equation or terms identifying the FFSs for the FC2 failure condition is:

- F1 error and F2 error, or
- F1 error and I3 error, or
- I1 error and F2 error, or
- I1 error and I3 error, or
- I2 error.

Table P4 - Example assurance assignment for design dependency of multiple functions same failure condition

FDAL Assignment		IDAL Assignment			Comment
F1	**F2**	**I1**	**I2**	**I3**	
B	B	B	A	B	Acceptable
		B	B	B	Unacceptable: the common item I2 Level B does not support the top-level failure condition
		A	A	C	Unacceptable: I3 level C does not support FC2 classification as F1 level B and I3 level C not allowed
		C	A	A	Unacceptable: I1 level C does not support FC2 classification as F2 level B and I1 level C not allowed
A	C	A	A	C	Acceptable
		A	C	C	Unacceptable: the common item I2 level C does not support the top-level failure condition
		C	A	A	Unacceptable: I1 level C does not support FC2 classification as F2 level C and I1 level C not allowed
		B	A	B	Unacceptable: I1 level B does not support FC2 classification as F2 level C and I1 level B not allowed
C	A	A	A	C	Unacceptable: I3 level C does not support FC2 classification as F1 level C and I3 level C not allowed
		C	C	A	Unacceptable: the common item I2 level C does not support the top-level failure condition
		C	A	A	Acceptable
		B	A	B	Unacceptable: I3 level B does not support FC2 classification as F1 level C and I3 Level B not allowed

Note that additional cases could be evaluated but are not shown; the common item I2 has to be Level A to support the top-level hazard.

P.7.4 Case 4: No Functional Independence but Item Development Independence

The top-level function is created in one system function which is decomposed into multiple items that are independent from one another. The system function FDAL is assigned the top function FDAL as per step g. of P.3.2.4. Once the validity of the item development independence claims for an FFS has been confirmed in step p. of P.3.3, the item IDALs are assigned per step r. using either Option 1 or Option 2 in the decision in Table P2 corresponding to the top-level failure condition classification.

SAENORM.COM : Click to view the full PDF of arp4761a

APPENDIX Q - CONTIGUOUS SAFETY ASSESSMENT PROCESS EXAMPLE

NOTE: The basic ARP4761A/ED-135 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body and the other appendices of the document.

TABLE OF CONTENTS

Q.1 INTRODUCTION 358
Q.1.1 Scope 358
Q.1.2 Outline 358
Q.1.3 Description of the Example Function 360
Q.1.4 Acronym List for Appendix Q Example 360

Q.2 RESERVED 363

Q.3 S18 AIRPLANE - AIRCRAFT FUNCTIONAL HAZARD ASSESSMENT (AFHA) EXAMPLE 364
Q.3.1 AFHA Example Introduction 364
Q.3.2 Glossary 364
Q.3.3 Aircraft Description Summary 364
Q.3.4 AFHA Development 364

Q.4 S18 AIRPLANE - PRELIMINARY AIRCRAFT SAFETY ASSESSMENT (PASA) EXAMPLE 376
Q.4.1 PASA Example Introduction 376
Q.4.2 Input 376
Q.4.3 Interdependence Analysis 381
Q.4.4 Failure Condition Evaluation 382
Q.4.5 Output 396

Q.5 S18 AIRPLANE - WHEEL BRAKE SYSTEM (WBS) SYSTEM FUNCTIONAL HAZARD ASSESSMENT (SFHA) EXAMPLE 399
Q.5.1 SFHA Example Introduction 399
Q.5.2 Glossary 399
Q.5.3 System Description Summary 399
Q.5.4 WBS SFHA Development 399

Q.6 S18 AIRPLANE - WBS PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA) EXAMPLE 408
Q.6.1 PSSA Example Introduction 408
Q.6.2 WBS PSSA Activities - Initial 408
Q.6.3 BSCU PSSA Activities - BSCU First Iteration 429
Q.6.4 PSSA BSCU Activities - BSCU Update Iteration 433
Q.6.5 WBS PSSA Update Based on BSCU PSSA 460

Q.7 S18 AIRPLANE - BRAKE SYSTEM CONTROL UNIT (BSCU) DEPENDENCE DIAGRAM (DD) EXAMPLE 463
Q.7.1 DD Example Introduction 463
Q.7.2 Summary of BSCU DD Results 463
Q.7.3 BSCU DD Detail 463

Q.8 S18 AIRPLANE - MARKOV ANALYSIS (MA) EXAMPLE 469
Q.8.1 MA Example Introduction 469
Q.8.2 Background 469
Q.8.3 Markov Analysis Steps 469
Q.8.4 Summary of WBS MA Results for Failure Condition: Total Loss of Wheel Deceleration (80% or More) 470
Q.8.5 Summary of WBS MA Results for Failure Condition: BSCU Fails to Output Command to Open SOV 474
Q.8.6 Summary of WBS MA Results for Failure Condition: Loss of Braking Command to NMV from BSCU 478

SAENORM.COM : Click to view the full PDF of arp4761a

Q.8.7 Summary of WBS MA Results for Failure Condition: BSCU Provides Unannunciated Erroneous Output to NMV Inadvertently 485
Q.8.8 Summary and Conclusions 491

Q.9 S18 AIRPLANE - WBS PSSA EXAMPLE USING MODEL BASED SAFETY ANALYSIS (MBSA) 492
Q.9.1 MBSA Example Introduction 492
Q.9.2 MBSA Modeling 492
Q.9.3 High-Level Model of the Wheel Brake System 492
Q.9.4 Satisfying PASA and Proposed Safety Requirements 500
Q.9.5 High-Level WBS MBSA Model Outputs 502
Q.9.6 Low-Level WBS Model - First Iteration 505
Q.9.7 Low-Level WBS Model Iterations 513
Q.9.8 First Iteration MBSA Failure Condition Evaluation 517
Q.9.9 Low-Level Model - Second Iteration 520
Q.9.10 Conclusion 533

Q.10 S18 AIRPLANE - BSCU FAILURE MODES AND EFFECTS ANALYSIS AND SUMMARY (FMEA/FMES) EXAMPLE 534
Q.10.1 BSCU Power Supply FMEA Introduction 534
Q.10.2 Power Supply Description 535
Q.10.3 Power Supply Detailed Analysis and Results 537
Q.10.4 FMES for the BSCU Introduction 540
Q.10.5 References 541
Q.10.6 BSCU Description 541
Q.10.7 FMES Data 541

Q.11 S18 AIRPLANE - BSCU COMMON MODE ANALYSIS (CMA) FOR THE BSCU EXAMPLE 542
Q.11.1 CMA Example Introduction 542
Q.11.2 Function/System Description 543
Q.11.3 BSCU CMA Detail 544

Q.12 S18 AIRPLANE - BSCU SYSTEM SAFETY ASSESSMENT (SSA) FAULT TREE ANALYSIS (FTA) EXAMPLE 551
Q.12.1 BSCU FTA Example Introduction 551
Q.12.2 Summary of BSCU FTA Results 551
Q.12.3 BSCU FTA Detail 551

Q.13 S18 AIRPLANE - WBS SYSTEM SAFETY ASSESSMENT (SSA) EXAMPLE 558
Q.13.1 WBS SSA Example Introduction 558
Q.13.2 BSCU SSA Activities 558
Q.13.3 WBS SSA Activities 558

Q.14 S18 AIRPLANE - ZONAL SAFETY ANALYSIS (ZSA) EXAMPLE 572
Q.14.1 ZSA Example Introduction 572
Q.14.2 References 573
Q.14.3 Inputs 574
Q.14.4 Methodology 577

Q.15 S18 AIRPLANE - PARTICULAR RISK ANALYSIS (PRA) EXAMPLE 600
Q.15.1 PRA Example Introduction 600
Q.15.2 Uncontained Engine Rotor Failure Analysis 600

Q.16 S18 AIRPLANE - CASCADING EFFECTS ANALYSIS (CEA) EXAMPLE 659
Q.16.1 CEA Example Introduction 659
Q.16.2 Inputs 659
Q.16.3 Function/System Description 660
Q.16.4 Cascading Effects Analysis 663
Q.16.5 CEA Summary 667

SAENORM.COM : Click to view the full PDF of arp4761a

Q.17 S18 AIRPLANE - AIRCRAFT SAFETY ASSESSMENT (ASA) EXAMPLE 668
Q.17.1 ASA Example Introduction 668
Q.17.2 ASA Process Summary 668
Q.17.3 ASA Inputs 668
Q.17.4 Aircraft Safety Assessment 670
Q.17.5 ASA Completion 692

Figure Q.1 Safety process example flow 359
Figure Q.4-1 (PASA) FTA 3.2.2.TL.A 388
Figure Q.6-1 (PSSA - WBS) WBS initial architecture 410
Figure Q.6-2 (PSSA - WBS) Electro-hydraulic equipment descriptions 411
Figure Q.6-3 (PSSA - WBS) WBS revised architecture 413
Figure Q.6-4 (PSSA - WBS) WBS mode transitions 414
Figure Q.6-5 (PSSA - WBS) Conceptual representation of thought process for Failure Condition Functional Mapping 416
Figure Q.6-6 (PSSA - WBS) Detailed Functional Failure Condition Mapping for “Loss of wheel braking” 417
Figure Q.6-7 (PSSA - WBS FTA) Total loss of wheel deceleration on command FTA (page 1) 421
Figure Q.6-8 (PSSA - WBS FTA) Total loss of wheel deceleration on command FTA (page 2) 421
Figure Q.6-9 (PSSA - WBS FTA) Total loss of wheel deceleration on command FTA (page 3) 422
Figure Q.6-10 (PSSA - WBS FTA) Total loss of wheel deceleration on command FTA (page 4) 423
Figure Q.6-11 (PSSA - WBS) WBS - architecture: identify the main function of the equipment 425
Figure Q.6-12 (PSSA - WBS) Independence Principle mapped on WBS architecture drawing 426
Figure Q.6-13 (PSSA - BSCU) BSCU iteration 1 430
Figure Q.6-14 (PSSA - BSCU - FTA) BSCU first Iteration 432
Figure Q.6-15 (PSSA - BSCU) BSCU update iteration 434
Figure Q.6-16 (PSSA - BSCU) BSCU update iteration (NORMAL Mode: Channel 1 in control) 436
Figure Q.6-17 (PSSA - BSCU) BSCU update iteration (NORMAL Mode: Channel 2 in control) 437
Figure Q.6-18 (PSSA - BSCU) BSCU update iteration: ALTERNATE Mode (when HYD 2 working)/Emergency Mode (when HYD 2 not working) 438
Figure Q.6-19 (PSSA - BSCU) BSCU functional mapping 440
Figure Q.6-20 (PSSA - BSCU) BSCU requirements traceability 443
Figure Q.6-21 (PSSA - BSCU) BSCU update iteration: IDAL assignment 444
Figure Q.6-22 (PSSA - BSCU - FTA) BSCU update iteration: loss of a valid braking command output to the NMV lifetime latency (page 1 of 3) 447
Figure Q.6-23 (PSSA - BSCU - FTA) BSCU update iteration: loss of a valid braking command output to the NMV lifetime latency (page 2 of 3) 448
Figure Q.6-24 (PSSA - BSCU - FTA) BSCU update iteration: loss of a valid braking command output to the NMV lifetime latency (page 3 of 3) 448
Figure Q.6-25 (PSSA - BSCU - FTA) BSCU update with 100-hour check (only first page shown) 449
Figure Q.6-26 (PSSA - BSCU - FTA) BSCU update iteration: unannunciated erroneous braking command to the NMV (page 1 of 4) 450
Figure Q.6-27 (PSSA - BSCU - FTA) BSCU update iteration: unannunciated erroneous braking command to the NMV (page 2 of 4) 451
Figure Q.6-28 (PSSA - BSCU - FTA) BSCU update iteration: unannunciated erroneous braking command to the NMV (page 3 of 4) 451
Figure Q.6-29 (PSSA - BSCU - FTA) BSCU update iteration: unannunciated erroneous braking command to the NMV (page 4 of 4) 452
Figure Q.6-30 (PSSA - BSCU - FTA) Unannunciated erroneous braking command to the NMV (PS monitor added) (first page) 453
Figure Q.6-31 (PSSA - BSCU - FTA) BSCU fails to output command to open SOV 454
Figure Q.6-32 (PSSA - WBS) Final PSSA WBS architecture (NORMAL Mode: Channel 1 in control) 461
Figure Q.7-1 (SSA - BSCU - DD) Loss of normal braking command to NMV from BSCU (page 1) 464
Figure Q.7-2 (SSA - BSCU - DD) Loss of normal braking command to NMV from BSCU (page 2) 465
Figure Q.7-3 (SSA - BSCU - DD) BSCU provides erroneous output to NMV: inadvertent (page 1) 466
Figure Q.7-4 (SSA - BSCU - DD) BSCU provides erroneous output to NMV: inadvertent (page 2) 467
Figure Q.7-5 (SSA - BSCU - DD) BSCU fails to output command to open SOV 468
Figure Q.8-1 (PSSA - WBS - MA) Total loss of wheel deceleration (80% or more) 473
Figure Q.8-2 (PSSA - BSCU - MA) BSCU fails to output command to open SOV 477

SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.8-3 (PSSA - BSCU - MA) Loss of braking command to NMV from BSCU 484
Figure Q.8-4 (PSSA - BSCU - MA) BSCU provides unannunciated erroneous output to NMV inadvertently 491
Figure Q.9-1 (PSSA - WBS - MBSA) WBS high-level model 494
Figure Q.9-2 (PSSA - WBS - MBSA) Detailed Wheel Brake System high-level model 497
Figure Q.9-3 (PSSA - WBS - MBSA) Detailed Control Wheel Braking “CTRL” block 499
Figure Q.9-4 (PSSA - WBS - MBSA) Proposed architecture with two hydraulic paths 502
Figure Q.9-5 (PSSA - WBS - MBSA) Proposed architecture with active/inhibited paths 503
Figure Q.9-6 (PSSA - WBS - MBSA) Architecture rationale to justify what is necessary to mitigate the command failures 504
Figure Q.9-7 (PSSA - WBS - MBSA) WBS initial architecture diagram 506
Figure Q.9-8 (PSSA - WBS - MBSA) WBS architecture diagram revision 507
Figure Q.9-9 (PSSA - WBS - MBSA) NORMAL mode 508
Figure Q.9-10 (PSSA - WBS - MBSA) NORMAL Mode with Channel 1 failure 509
Figure Q.9-11 (PSSA - WBS - MBSA) ALTERNATE Mode with anti-skid 510
Figure Q.9-12 (PSSA - WBS - MBSA) EMERGENCY Mode 511
Figure Q.9-13 (PSSA - WBS - MBSA) ALTERNATE Mode using emergency accumulator 512
Figure Q.9-14 (PSSA - WBS - MBSA) WBS low-level model first iteration 513
Figure Q.9-15 (PSSA - WBS - MBSA) WBS detailed low-level model first iteration 515
Figure Q.9-16 (PSSA - WBS - MBSA) BSCU detailed low-level model first iteration 516
Figure Q.9-17 (PSSA - WBS - MBSA) Failure Conditions Observers block 517
Figure Q.9-18 (PSSA - WBS - MBSA) WBS upgraded architecture 521
Figure Q.9-19 (PSSA - WBS - MBSA) WBS reviewed architecture second iteration 522
Figure Q.9-20 (PSSA - WBS - MBSA) BSCU detailed low-level model second iteration 523
Figure Q.10-1 (SSA - BSCU - FMEA) BSCU physical implementation 536
Figure Q.10-2 (SSA - BSCU - FMEA) Power supply block diagram 536
Figure Q.10-3 (SSA - BSCU - FMEA) Schematic of power supply monitor 537
Figure Q.11-1 (SSA - BSCU - CMA) BSCU architecture diagram 543
Figure Q.11-2 (SSA - BSCU CMA) BSCU physical implementation 549
Figure Q.12-1 (SSA - BSCU - FTA) Loss of normal braking command to NMV from BSCU (page 1) 552
Figure Q.12-2 (SSA - BSCU - FTA) Loss of normal braking command to NMV from BSCU (page 2) 552
Figure Q.12-3 (SSA - BSCU - FTA) Loss of normal braking command to NMV from BSCU (page 3) 553
Figure Q.12-4 (SSA - BSCU - FTA) BSCU provides erroneous output to NMV: inadvertent (page 1) 554
Figure Q.12-5 (SSA - BSCU - FTA) BSCU provides erroneous output to NMV: inadvertent (page 2) 555
Figure Q.12-6 (SSA - BSCU - FTA) BSCU provides erroneous output to NMV: inadvertent (page 3) 555
Figure Q.12-7 (SSA - BSCU - FTA) BSCU provides erroneous output to NMV: inadvertent (page 4) 556
Figure Q.12-8 (SSA - BSCU - FTA) BSCU fails to output command to open SOV 557
Figure Q.13-1 (SSA - WBS) Final Wheel Brake System architecture 559
Figure Q.13-2 (SSA - WBS - FTA) Total loss of wheel deceleration on command FTA (page 1) 566
Figure Q.13-3 (SSA - WBS - FTA) Total loss of wheel deceleration on command FTA (page 2) 567
Figure Q.13-4 (SSA - WBS - FTA) Total loss of wheel deceleration on command FTA (page 3) 568
Figure Q.13-5 (SSA - WBS - FTA) Total loss of wheel deceleration on command FTA (page 4) 569
Figure Q.14-1 (ZSA) Inputs and outputs for a Zonal Safety Analysis (with references to Appendix K) 572
Figure Q.14-2 (ZSA) Aircraft major zones 578
Figure Q.14-3 (ZSA) Aircraft major sub-zones 579
Figure Q.14-4 (ZSA) Detailed zones (landing gear bay, Zones 147/148) 580
Figure Q.14-5 (ZSA) Simplified fault tree 583
Figure Q.14-6 (ZSA) Diagram depicts overall physical installation of wheel braking and flaps functions 585
Figure Q.14-7 (ZSA) Landing gear bay zone: system identification (landing gear extended) 587
Figure Q.14-8 (ZSA) Diagram depicts findings of the zonal inspection within the MLGB zone 591
Figure Q.14-9 (ZSA) Diagram depicts proposed solution to resolve issue discovered during zonal inspection 593
Figure Q.14-10 (ZSA) Fuel tank in center wing box and potential heat source in MLGB 595
Figure Q.14-11 (ZSA) Proposed resolutions for cross-zonal interaction considerations 596
Figure Q.14-12 (ZSA) Ventilation of MLGB and adjacent zones 597
Figure Q.15-1 (PRA) PRA methodology step (L.3.a) discussed in the current section 601
Figure Q.15-2 (PRA) Single 1/3 disc fragment definition 605
Figure Q.15-3 (PRA) PRA methodology step (L.3.b) discussed in the current section 606
Figure Q.15-4 (PRA) Airplane concept drawing 608
Figure Q.15-5 (PRA) Area of the airplane affected by the single 1/3 disk fragments 612
Figure Q.15-6 (PRA) Fuselage areas available for system electrical installations 613
Figure Q.15-7 (PRA) PRA methodology step (L.3 c.) discussed in the current section 614

SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.15-8 (PRA) RH engine hydraulic elements exposed to LH engine UERF debris 618
Figure Q.15-9 (PRA) Trajectory affecting pump lines in the rear part of the RH engine pylon 619
Figure Q.15-10 (PRA) Airplane-level Wheel Brake System architecture 620
Figure Q.15-11 (PRA) High-level Wheel Brake System architecture 622
Figure Q.15-12 (PRA) Physical elements the damage of which could cause loss of one or more wheel braking modes 626
Figure Q.15-13 (PRA) System-level WBS architecture modified to implement the required redundancy 630
Figure Q.15-14 (PRA) Examples of Engine 1 UERF trajectories 632
Figure Q.15-15 (PRA) PRA methodology step (L.3 d.) discussed in the current section 635
Figure Q.15-16 (PRA) PRA methodology step (L.3 e.) discussed in the current section 638
Figure Q.15-17 (PRA) Examples of debris trajectories crossing the wing boxes 639
Figure Q.15-18 (PRA) Particular trajectory considered 643
Figure Q.15-19 (PRA) PRA methodology step (L.3 f.) discussed in the current section 648
Figure Q.15-20 (PRA) Type of outputs of the PRA methodology (L.4.1) discussed in the current section 650
Figure Q.15-21 (PRA) Type of outputs of the PRA methodology (L.4.2) discussed in the current section 654
Figure Q.16-1 (CEA) High-level airplane braking interface diagram 661
Figure Q.16-2 (CEA) Airplane wheel speed interface diagram 662
Figure Q.16-3 (CEA) Loss of single WBS A429 wheel speed data 663
Figure Q.16-4 (CEA) Loss of all WBS A429 wheel speed data 664
Figure Q.16-5 (CEA) Erroneous wheel speed data from WBS A429 Ch1 or Ch2 665
Figure Q.16-6 (CEA) Erroneous wheel speed data from both WBS A429 Ch1 and Ch2 666
Figure Q.17-1 (ASA) Unable to decelerate within available runway with crew aware, landing (page 1) 685
Figure Q.17-1 (ASA) Unable to decelerate within available runway with crew aware, landing (page 2) 686
Figure Q.17-1 (ASA) Unable to decelerate within available runway with crew aware, landing (page 3) 687
Figure Q.17-1 (ASA) Unable to decelerate within available runway with crew aware, landing (page 4) 687

Table Q.3-1 (AFHA) S18 airplane function list 364
Table Q.3-2 (AFHA) “Decelerate on ground” failure condition identification matrix 365
Table Q.3-3 (AFHA) Revised Failure conditions considering crew awareness 366
Table Q.3-4 (AFHA) S18 AFHA assumptions/notes 368
Table Q.3-5 (AFHA) S18 AFHA (“Decelerate on ground” function only) 369
Table Q.4-1 (PASA) Interdependence table 381
Table Q.4-2 (PASA) Interdependence (common resource) table 382
Table Q.4-3 (PASA) System functional failures and SFHA failure conditions: Total loss 383
Table Q.4-4 (PASA) System functional failures and SFHA failure conditions: Partial loss 383
Table Q.4-5 (PASA) System functional failures and SFHA failure conditions: malfunction 383
Table Q.4-6 (PASA) CoFFE table 384
Table Q.4-7 (PASA) CoFFE table summary 386
Table Q.4-8 (PASA) CoFFE table result: High-speed overrun 387
Table Q.4-9 (PASA) Potential failures combinations (FT cut set) 391
Table Q.4-10 (PASA) Hydraulic common power source failures 392
Table Q.4-11 (PASA) Electrical common power source failures 392
Table Q.4-12 (PASA) Multisystem and multifunction type failures combination 393
Table Q.4-13 (PASA) FDAL assignment to system functions 395
Table Q.4-14 (PASA) FDAL assignment to system functions (option 4) 396
Table Q.4-15 (PASA) PASA output (safety objective) 397
Table Q.4-16 (PASA) PASA output (proposed safety requirement) 397
Table Q.4-17 (PASA) PASA assumption 398
Table Q.5-1 (SFHA - WBS) WBS function list 399
Table Q.5-2 (SFHA - WBS) “Decelerate the wheels on the ground” failure condition identification matrix 400
Table Q.5-3 (SFHA - WBS) Revised failure conditions considering crew awareness 402
Table Q.5-4 (SFHA - WBS) S18 wheel brake SFHA (partial; “Decelerate wheels on the ground” function only) 405
Table Q.6-1 (PSSA - WBS) SFHA failure conditions and classifications 409
Table Q.6-2 (PSSA - WBS) Allocated requirements from safety process 409
Table Q.6-3 (PSSA - WBS) Evaluated SFHA Failure Conditions 418
Table Q.6-4 (PSSA - WBS) Proposed independence requirements 427
Table Q.6-5 (PSSA - WBS) Proposed safety requirements, not related to independence 427
Table Q.6-6 (PSSA - BSCU) Safety requirements from WBS PSSA 431
Table Q.6-7 (PSSA - BSCU) BSCU contributions to Failure Conditions 441
Table Q.6-8 (PSSA - BSCU) Safety requirements from WBS PSSA 441

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.6-9 (PSSA - BSCU) Functional failure set summary 445
Table Q.6-10 (PSSA - BSCU) BSCU update iteration: IDAL assignment 445
Table Q.6-11 (PSSA - BSCU - FTA) Summary of fault tree latent failures 455
Table Q.6-12 (PSSA - BSCU - FTA) Cut sets for FTA BSCU-CMD-LOSS 456
Table Q.6-13 (PSSA - BSCU) BSCU Independence Principles 456
Table Q.6-14 (PSSA - BSCU - CMA) CMA questionnaire for independence between command and monitor 457
Table Q.6-15 (PSSA - BSCU) Proposed safety requirements 458
Table Q.6-16 (PSSA - BSCU) Assumptions to WBS level 460
Table Q.7 1 (SSA - BSCU - DD) BSCU DD results summary 463
Table Q.8-1 (PSSA - WBS - MA) Markov Model event table 470
Table Q.8-2 (PSSA - WBS - MA) WBS Markov Model state space table 471
Table Q.8-3 (PSSA - WBS - MA) Markov Model state transitions table 472
Table Q.8-4 (PSSA - WBS - MA) Markov Model results table 473
Table Q.8-5 (PSSA - BSCU - MA) Markov Model event table 474
Table Q.8-6 (PSSA - BSCU - MA) BSCU Markov Model state space table 475
Table Q.8-7 (PSSA - BSCU - MA) Markov Model state transitions table 476
Table Q.8-8 (PSSA - BSCU - MA) Markov Model results table 477
Table Q.8-9 (PSSA - BSCU - MA) Markov Model event table 478
Table Q.8-10 (PSSA - BSCU - MA) Markov Model state space table 479
Table Q.8-11 (PSSA - BSCU - MA) Markov Model state transitions table 481
Table Q.8-12 (PSSA - BSCU - MA) Markov Model results table 482
Table Q.8-13 (PSSA - BSCU - MA) Markov Model event table 485
Table Q.8-14 (PSSA - BSCU - MA) Markov Model state space table 486
Table Q.8-15 (PSSA - BSCU - MA) Markov Model state transitions table 488
Table Q.8-16 (PSSA - BSCU - MA) Markov Model results table 489
Table Q.9-1 (PSSA - WBS - MBSA) High-level model probability budget allocation for PASA-SR-015 501
Table Q.9-2 (PSSA - WBS - MBSA) High-level model probability budget allocation for PASA-SR-XY 501
Table Q.9-3 (PSSA - WBS - MBSA) Quantity of “Loss of wheel braking” FFSs/MCSs 517
Table Q.9-4 (PSSA - WBS - MBSA) “Loss of wheel braking” probability computation first iteration 518
Table Q.9-5 (PSSA - WBS - MBSA) Quantity of “Uncommanded Wheel Braking” FFSs/MCSs 518
Table Q.9-6 (PSSA - WBS - MBSA) “Uncommanded Wheel Braking” probability computation 518
Table Q.9-7 (PSSA - WBS - MBSA) Quantity of “Loss of wheel braking” FFSs second iteration 524
Table Q.9-8 (PSSA - WBS - MBSA) “Loss of wheel braking” probability computation second iteration 525
Table Q.9-9 (PSSA - WBS - MBSA) Quantity of Uncommanded wheel braking” FFSs second iteration 526
Table Q.9-11 (PSSA - WBS - MBSA) Minimal IDAL allocations 529
Table Q.9-12 (PSSA - WBS - MBSA) Final minimal IDAL allocations 530
Table Q.9-13 (PSSA - WBS - MBSA) Safety assumptions for confirmation 532
Table Q.9-14 (PSSA - WBS - MBSA) Proposed MBSA Safety Requirements 532
Table Q.10-1 (SSA - BSCU - FMEA) Cross reference to FMEA process appendix 534
Table Q.10-2 (SSA - BSCU - FMEA) Functional FMEA for BSCU power supply 538
Table Q.10-3 (SSA - BSCU - FMEA) Failure effect categories 538
Table Q.10-4 (SSA - BSCU - FMEA) Piece-part FMEA for BSCU power supply monitor 539
Table Q.10-5 (SSA - BSCU - FMEA) BSCU power supply and power supply monitor FMEA summary 540
Table Q.10-6 (SSA - BSCU - FMEA) Failure effects summary 541
Table Q.11-1 (SSA - CMA - BSCU) Example to Appendix M cross reference 542
Table Q.11-2 (SSA - CMA - BSCU) Channels 1 and 2 independence evaluation 546
Table Q.11-3 (SSA - CMA - BSCU) Command-monitor independence evaluation 548
Table Q.11-4 (SSA - CMA - BSCU) Signals violating segregation zone evaluation 550
Table Q.12-1 (SSA - BSCU - FTA) BSCU FTA Results Summary 551
Table Q.13-1 (SSA - WBS) Interface requirements 560
Table Q.13-2 (SSA - WBS) SFHA failure conditions and classifications 561
Table Q.13-3 (SSA - WBS) Allocated safety requirements 562
Table Q.13-4 (SSA - WBS) WBS independence requirements 562
Table Q.13-5 (SSA - WBS) Independence Principles 563
Table Q.13-6 (SSA - WBS) PSSA requirements verification summary 564
Table Q.13-7 (SSA - WBS) PSSA requirements verification summary 564
Table Q.13-8 (SSA - WBS) Wheel Brake System FTA events 565
Table Q.13-9 (SSA - WBS) Quantitative safety requirements verification summary 570
Table Q.13-10 (SSA - WBS) Safety requirements verification summary 571
Table Q.14-1 (ZSA) Standards of system and structure design 574

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.14-2 (ZSA) Lessons learned from manufacturing and maintenance of aircraft similar to the S18 (partial list) 575
Table Q.14-3 (ZSA) Lessons learned from in-service experience of aircraft similar to the S18 (partial list) 575
Table Q.14-4 (ZSA) Segregation requirements from PRA to be checked by ZSA (partial list) 575
Table Q.14-5 (ZSA) Independence Principles resulting from PASA and PSSA (partial list) 576
Table Q.14-6 (ZSA) Physical hazards inherent to the system equipment technology of aircraft similar to the S18 (partial list) 576
Table Q.14-7 (ZSA) PSSA references of systems closely associated with the main landing gear zone (partial list) 577
Table Q.14-8 (ZSA) System installation drawings, descriptions, and mockup of the S18 airplane (partial list) 577
Table Q.14-9 (ZSA) Questionnaire (partial) 581
Table Q.14-10 (ZSA) Failure condition failure combinations 583
Table Q.14-11 (ZSA) Independence Principles and requirements 584
Table Q.14-12 (ZSA) Questionnaire (continued) 584
Table Q.14-13 (ZSA) Inherent hazards relative to MLGB zone 586
Table Q.14-14 (ZSA) MLGB zone perimeter boundary description 587
Table Q.14-15 (ZSA) Inherent hazard considerations within the MLGB zone 589
Table Q.14-16 (ZSA) Issues discovered within same zone ZSA 590
Table Q.14-17 (ZSA) Same zone ZSA: proposed solutions 592
Table Q.14-18 (ZSA) Summary of issues discovered and proposed resolutions for cross-zonal interaction considerations 595
Table Q.14-19 (ZSA) Specialist participation 598
Table Q.14-20 (ZSA) ZSA summary sheet 599
Table Q.15-1 (PRA) Examples relevant to the S18 airplane and to the selected PRA 603
Table Q.15-2 (PRA) Failure condition of the AFHA example used as input in this part of the PRA example 615
Table Q.15-3 (PRA) Independence Principles developed by the PASA example to satisfy the “no single failure” requirement associated with the Catastrophic failure condition 3.2.2.TL.A 615
Table Q.15-4 (PRA) Failure conditions of the SFHA example used as inputs in this part of the PRA example 616
Table Q.15-5 (PRA) Independence Principle developed by the PSSA example to satisfy the “no single failure” requirement associated with the Catastrophic failure condition 1.1.MF1 616
Table Q.15-6 (PRA) Failure conditions considered in this UERF example 616
Table Q.15-7 (PRA) Resulting requirements 627
Table Q.15-8 (PRA) Requirements verification matrix: requirements derived from Independence Principles 636
Table Q.15-9 (PRA) Requirements verification matrix: additional requirements 637
Table Q.15-10 (PRA) Proposed requirements derived from Independence Principles established by the PASA 651
Table Q.15-11 (PRA) Additional proposed requirements not derived from Independence Principles established by the PASA 653
Table Q.15-12 (PRA) Cascade of requirements developed within Q.15.2.3 655
Table Q.15-13 (PRA) Assumptions made in Q.15.2.3 658
Table Q.16-1 (CEA) BSCU wheel speed sensor CEA summary 667
Table Q.17-1 (ASA) Evaluation of inputs 669
Table Q.17-2 (ASA) Aircraft-level reference data 670
Table Q.17-3 (ASA) System-level reference data 671
Table Q.17-4 (ASA) AFHA failure condition confirmation (partial; “Decelerate on Ground” function only) 674
Table Q.17-5 (ASA) Fault tree gates 688
Table Q.17-6 (ASA) Undeveloped events 688
Table Q.17-7 (ASA) Cut set report 689
Table Q.17-8 (ASA) Reference data 689
Table Q.17-9 (ASA) Safety objectives 690

SAENORM.COM : Click to view the full PDF of arp4761a

Q.1 INTRODUCTION

Q.1.1 Scope

This appendix describes, in detail, a contiguous example of the safety assessment process for a function on a fictitious aircraft design. In order to present a clear picture, an airplane function was broken down into elements of a single system. A function was chosen which has sufficient complexity to allow use of all the methodologies, yet was simple enough to present a clear picture of the flow through the methodologies. This function/system/item was analyzed using all the methods and tools described in this SAE Aerospace Recommended Practice (ARP). Each method was employed to show how it may be applied. In practice, for example, one might choose a single analysis method to determine the potential combinatorial causes of functional failures. However, all methods are presented in the example to give the reader an understanding of their similarities and differences.

The methodologies applied here are an example of one way to utilize the methods defined in the document. Other formats may be used to accomplish the documentation, so long as the principles outlined in the descriptive text of this ARP are followed.

While ARP4761A/ED-135 does not provide guidelines for planning the safety assessment process, safety planning is required as part of the development assurance planning defined in ARP4754B/ED-79B, Section 3.

The safety assessment process should be planned and managed so as to provide the necessary assurance that all relevant failure conditions (FCs) have been identified, and that all significant combinations of failures that could cause those failure conditions have been considered. The safety assessment process is of fundamental importance in establishing appropriate safety objectives for the aircraft and systems and determining that the implementation satisfies these objectives.

For appropriate management of the safety assessment process, a safety program plan should be created. An example aircraft-level Safety Program Plan (SPP) is provided in ARP4754B/ED-79B, Appendix B.

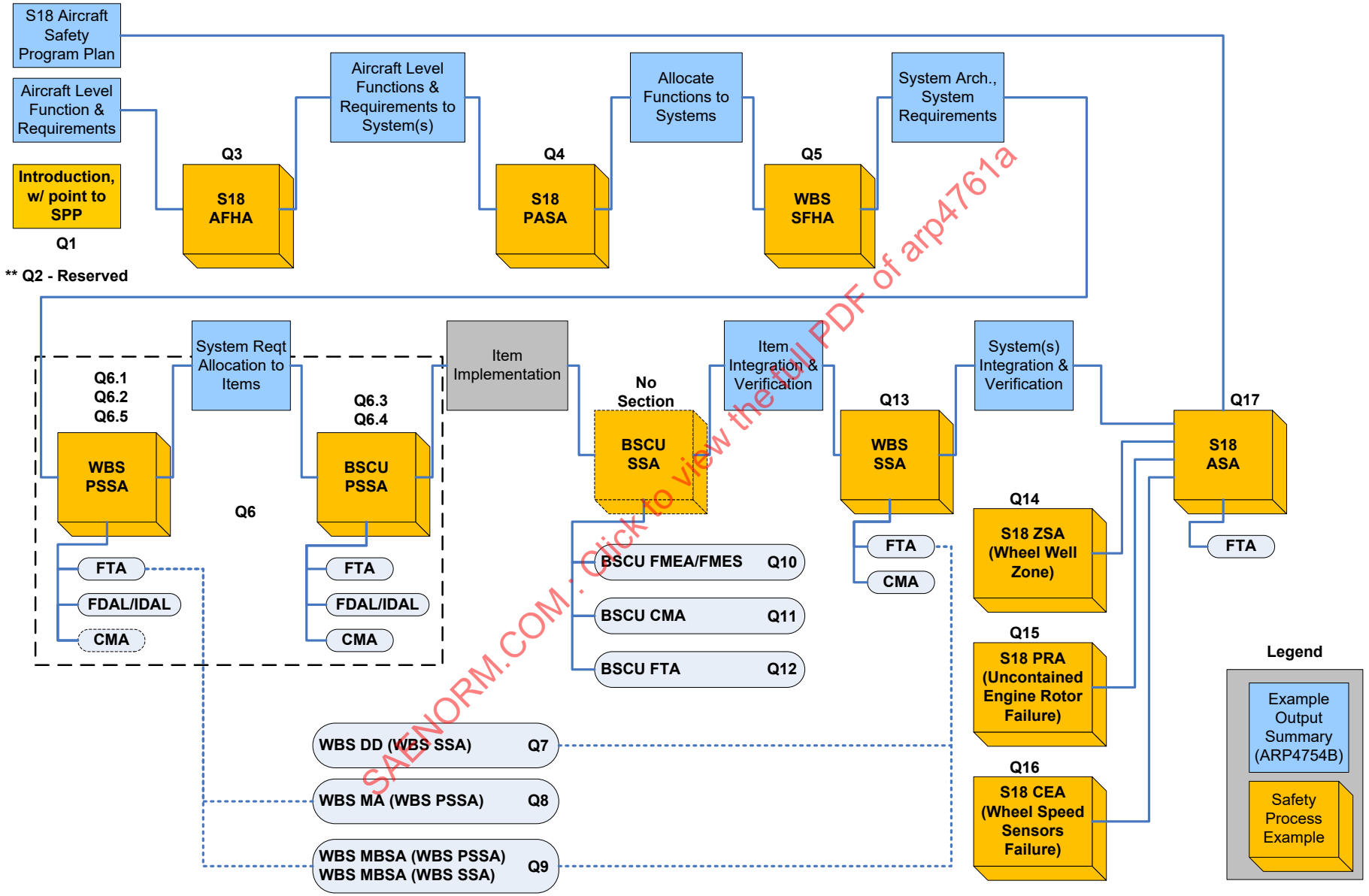
This example contains references to representative documentation that a company may use to assure itself of the safety of its products. Some of these documents are submitted to the Certification Authorities for the purpose of certification (e.g., the Wheel Brake System Functional Hazard Assessment). Other documents are internal to the company and not required for certification (e.g., the S18 Design Requirements Document). No implication is made that these documents should be submitted to a Certification Authority and none should be implied. “Safety” and “certification” are not synonymous terms. The authors are trying to simply illustrate the process for safety assessment, including those processes that may be beyond certification requirements.

Q.1.2 Outline

The function chosen is analyzed using the methods described in the appendices. The order of the methods presented represents a nominal course of accomplishing the safety activities through the design cycle. Figure Q.1 presents the top-level aircraft, system, and item-level tasks to provide the reader a reference point. The system development and safety assessment activities are sequenced as they might typically be in a development program. An actual development program for the function chosen would be more complex than included herein.

Figure Q.1 shows the interactions between the system development process and the safety assessment process of the fictional S18 airplane with information flow from the system development process into the safety assessment process and outputs of the safety assessment process flowing into system development process. Alternate combinatorial analysis methods to Fault Tree Analysis (FTA) are also presented and linked to the FTA they represent. The reader is encouraged to use this flow diagram to help navigate through the example.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.1 - Safety process example flow

In this example, each figure and table title starts with an indication as to what section of the example the figure or table supports (e.g., (SSA - BSCU - FMEA) for the FMEA as part of the BSCU SSA).

The safety assessment process and system development process are concurrent processes with data interfaces. This safety assessment process example contains a number of data inputs (documents, tables, etc.) that would be produced by following the development process in ARP4754B/ED-79B and documented in the contiguous aircraft/system development process example in ARP4754B/ED-79B, Appendix E. Inputs from the system development process are enclosed in boxes to distinguish the data inputs from explanatory text. An example of such a data input is shown below.

The operational profile for the WBS safety assessment includes:

a. An average flight duration of 5 hours.

b. An airplane life of 100000 flight hours.

c. A power on time of 100 operating hours.

Editor's Notes are enclosed in parenthesis and provided in italics. Where necessary, the reader will be directed to the appropriate section of ARP4754B/ED-79B or ARP4761A/ED-135 for further information on the method or process involved. Editor's Notes may also provide clarification to the reader; e.g., when the scope of the example is limited for brevity.

When the reader sees the term "main body," it implies the main body of ARP4761A/ED-135 and the section called out in reference to the example given.

Q.1.3 Description of the Example Function

The aircraft function analyzed in the example is:

"Decelerate on ground."

The safety process example developed in this appendix concentrates on an aircraft braking system, the details of which are evolved through each section of this appendix approximately as they would in a real life situation.

A companion, system development example of the S18 Airplane Wheel Brake System, is provided in ARP4754B/ED-79B, Appendix E.

Q.1.4 Acronym List for Appendix Q Example

AC	Advisory Circular or Alternating Current
Alt.	Alternate
APU	Auxiliary Power Unit
BIT	Built-in Test
BSCU	Brake System Control Unit
CCMR	Candidate Certification Maintenance Requirement
CFR	Code of Federal Regulation
ChX or CHX	Channel X (where X=1,2)
Cmd or CMD	Command

SAENORM.COM : Click to view the full PDF of arp4761a

Com or COM	Command (lane or path)
COMX	Command (lane or path) X (where X=1,2)
CS	Certification Specification
Ctrl or CTRL	Control
DC	Direct Current
EBU	Electric Brake Unit
Elec.	Electrical
Emer.	Emergency
EECU	Electronic Engine Control Unit
EFCU	Electronic Flight Control Unit
ELS	Electrical System
EPWR	Electrical Power
F.R.	Failure Rate
FCS	Flight Control System
FLS	Flap System
GDI	Ground Detection Information
GSS	Ground Spoiler System
/h	Per Hour
h	Hour
HAS	Hardware Accomplishment Summary
HIRF	High-Intensity Radiated Field
HL	High-Level
HPS	Hydraulic Power Supplies
hr	Hour
HW	Hardware
Hyd. or HYD	Hydraulic
HYS	Hydraulic System
I/O	Input/Output
IC	Integrated Circuit

SAENORM.COM : Click to view the full PDF of arp4761a

LH	Left Hand
LL	Low-Level
LOF	Loss of Function
LRU	Line Replaceable Unit
MF	Malfunction
MF&MS	Multifunction and Multisystem Analysis
min	Minute
MLGB	Main Landing Gear Bay
MM	Markov Model
Mon or MON	Monitor
MONX	Monitor (lane or path) X (where X=1,2)
NMV	Normal Meter(ing) Valve
NTSB	National Transportation Safety Board
OEI	One Engine Inoperative
OEM	Original Equipment Manufacturer
pfh	Per Flight Hour
PL	Partial Loss
Pos.	Position
PR	Problem Report
PRS	Propulsion System
PS or P/S	Power Supply
psi	Pounds per Square Inch
PUP	Power-Up (Interval)
Pwr or PWR	Power
RH	Right Hand
rpm	Revolutions per Minute
RTL	Return to Land
RTO	Rejected Takeoff

SAENORM.COM : Click to view the full PDF of arp4761a

S/ASV	Shutoff/Anti-Skid Valve
SAS	Software Accomplishment Summary
SOV	Shutoff Valve
SPD	Speed
SPP	Safety Program Plan
ST	State
SW	Software
TL	Total Loss
TRS	Thrust Reverser System
UERF	Uncontained Engine Rotor Failure
V&V	Validation and Verification
V1	Takeoff Decision Speed
VHDL	Very High-Speed Integrated Circuit Hardware Design Language
VR	Rotation Speed
WBS	Wheel Brake System
WHL	Wheel
WOW	Weight on Wheels

Q.2 RESERVED

This section is reserved for future use.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.3 S18 AIRPLANE - AIRCRAFT FUNCTIONAL HAZARD ASSESSMENT (AFHA) EXAMPLE

AFHA Example

Q.3.1 AFHA Example Introduction

This section contains the aircraft-level functional hazard assessment of the “S18” airplane. This is a fictitious aircraft which was created for this document. All airplane level functions were considered.

Q.3.2 Glossary

This section captures specific terms and definitions used within this example.

Term	Definition
Uncommanded	Activation of a function without crew command input or erroneously activated due to equipment failure
V1	The speed beyond which takeoff should no longer be aborted
VR	The speed at which the pilot begins to apply control inputs to cause the aircraft nose to pitch up (rotation), after which the aircraft will leave the ground

Q.3.3 Aircraft Description Summary

The S18 airplane is a two-engine transport category airplane designed to carry 300 to 350 passengers up to 5000 nautical miles at 0.86 Mach with an altitude ceiling of 41000 feet altitude. The average flight duration is 5 hours.

(Editor’s Note: The other initial features defining this airplane would be included in this paragraph, but are not described for the sake of brevity. These features are typically developed from the marketing and business decisions made during the initial marketing effort.)

Q.3.4 AFHA Development

Q.3.4.1 AHFA Inputs

The S18 airplane development process identifies the airplane level functions presented in Table Q.3-1.

Table Q.3-1 - (AFHA)
S18 airplane function list

1. Provide aerodynamic performance
2. Control airplane trajectory
3. Control airplane energy
   - 3.1. Maintain or increase airplane energy
   - 3.2. Reduce airplane energy
     - 3.2.1. Provide controlled aerodynamic drag
     - 3.2.2. Decelerate on ground
   - 3.3. Provide high lift capability
4. Provide survivable environment
5. Provide crew situational awareness
6. Maintain structural integrity
7. Provide emergency services
8. Provide passenger/cargo services

SAENORM.COM : Click to view the full PDF of arp4761a

Q.3.4.2 Review and Confirm Aircraft Functions/Sub-Functions

The function list in Table Q.3-1 and the sub-function breakdowns have been reviewed and confirmed to be complete. The review has also confirmed that the functions are described at a consistent level of abstraction and avoid references to particular design solutions. Where functional breakdown was provided, the lower-level functions have been confirmed to be necessary and sufficient to accomplish the higher-level function. This list of functions is, therefore, appropriate for development of the AFHA.

Q.3.4.3 Determine Failure Conditions

(Editor's Note: Only the "Decelerate on ground" function is developed in this example. All other airplane functions, at the level of the functional breakdown defined in Table Q.3-1 would be developed in a similar fashion. For the "Decelerate on ground" example function no related functions were identified, therefore, no combined failures were defined. See A.3.1 for examples of combined failure conditions.)

Q.3.4.3.1 Failure Condition Identification Matrix

A failure condition identification matrix was constructed for the function "Decelerate on ground." This initial matrix is presented in Table Q.3-2. Postulated failure condition descriptions are captured for total loss of function, partial loss of function, and malfunction (erroneous operation) of function.

(Editor's Note: Note that the unique numbering scheme used in the example has been established to enable readability as well as traceability to later assessment examples. Suffixes for total loss (TL), partial loss (PL), and malfunction (MF) have been appended to differentiate the different function 3.2.2 failure condition mechanisms. Other numbering mechanisms may also be used.)

Table Q.3-2 - (AFHA)
"Decelerate on ground" failure condition identification matrix

ID #	Aircraft Function	Total Loss	Partial Loss	Malfunction
3	Control aircraft energy			
3.2	Reduce aircraft energy			
3.2.2	Decelerate on ground	3.2.2.TL Loss of ability to decelerate	3.2.2.PL Partial loss of ability to decelerate	3.2.2.MF1 Uncommanded deceleration 3.2.2.MF2 Excessive deceleration intensity 3.2.2.MF3 Reduced deceleration intensity

SAENORM.COM : Click to view the full PDF of arp4761a

The following rationale was used when populating the Table Q.3-2 failure condition identification matrix:

3.2.2.TL: Loss of ability to decelerate

Total loss of deceleration capability may lead the airplane to an overrun available runway length during any high-speed ground operation.

3.2.2.PL1: Partial loss of ability to decelerate

The interaction of certain groundspeeds in combination with partial loss of deceleration capability and available runway may result in unsafe airplane conditions. Therefore, a partial loss of deceleration resulting in overrun is another loss of function to be considered.

3.2.2.MF1: Uncommanded deceleration

The “Decelerate on ground” function is understood to have operational situations and different deceleration intensities as relevant parameters. The “Uncommanded deceleration” malfunction addresses activation of the deceleration function at an incorrect operational time.

3.2.2.MF2: Excessive deceleration intensity

The “Excessive deceleration intensity” malfunction addresses operation of the decelerate function with greater than commanded intensity.

3.2.2.MF3: Reduced deceleration intensity

The “Reduced deceleration intensity” malfunction addresses operation of the decelerate function with less than commanded intensity.

(Editor’s Note: This failure condition has been captured to show completeness of failure condition development. Further evaluation is necessary to establish any difference between this failure condition and the partial loss failure condition (3.2.2.PL1). This evaluation has not been included herein.)

Q.3.4.3.2 Crew Awareness

The effect of crew awareness on the severity of the failure condition (FC) has been reviewed. Crew awareness has been determined to be significant to the effects of the loss of function and partial loss of function failure conditions. These conditions have therefore been separated into new failure conditions with or without crew awareness as shown in Table Q.3-3.

Table Q.3-3 - (AFHA)
Revised Failure conditions considering crew awareness

Revised FC ID	Revised Failure Condition Description
3.2.2.TL.A	Loss of ability to decelerate with crew aware
3.2.2.TL.U	Loss of ability to decelerate with crew unaware
3.2.2.PL.A	Partial loss of ability to decelerate with crew aware
3.2.2.PL.U	Partial loss of ability to decelerate with crew unaware

Q.3.4.4 Assess Failure Condition Effects

The effects of each of the identified failure condition on the airplane, flight crew, and occupants other than the flight crew have been assessed. The effects are captured based on their immediate effect on airplane, flight crew, and occupants during the phase of flight being analyzed. This includes immediate effects as well as effects that would occur during subsequent flight phases.

The captured effects of each failure condition are shown in Column 4 of Table Q.3-5.

Q.3.4.4.1 Flight Phases

Effects are described for each flight phase. The flight phase indicates the operational moment when the failure condition occurs. For this assessment, the 5-hour average duration flight has been divided into the following anticipated flight phases:

- Taxi
- Takeoff
- Climb
- Cruise

SAENORM.COM : Click to view the full PDF of arp4761a

- Descent
- Approach
- Landing

(Editor's Note: Operational flight phase divisions (e.g., takeoff before V1, takeoff after V1) are typically included in the flight phase list, but have been omitted here for brevity.)

Q.3.4.4.2 Operational Conditions

For the determination of failure effects, operational conditions such as airplane weight, center of gravity, and speed are determined based on each flight phase and considered to be at their worst-case value within the allowed operating envelope. Note that for takeoff and landing phases, runway distance is a function of airplane configuration parameters, per airplane performance defined in the airplane requirements specification.

Potential operational events that could independently occur and increase the severity of the failure condition have been reviewed. The following event(s) have been identified as relevant: Rejected Takeoff (RTO).

An RTO, occurring independently and concurrently with the failure condition, can increase the severity of the effects of loss of function and partial loss of function by creating the potential for a runway overrun during the takeoff flight phase.

Loss of ability to decelerate in combination with RTO (3.2.2.TL.RTO).

Partial loss of ability to decelerate in combination with RTO (3.2.2.PL.RTO).

Reduced deceleration intensity when commanded in combination with RTO (3.2.2.MF3.RTO).

(Editor's Note: Other relevant operational conditions—e.g., high-speed landing, airplane landing long—have been omitted for brevity.)

Q.3.4.4.3 Environmental Conditions

For the determination of failure effects, environmental conditions such as runway conditions, airfield temperature, and altitude are considered at their worst-case value within the allowed operating envelope. Note that for takeoff and landing phases, runway distance is a function of environmental parameters, per airplane performance defined in the airplane requirements specification.

Q.3.4.5 Classify Based on Effect Severity

Each failure condition has been classified based on its effects by applying the qualitative classification criteria provided in AC 25.1309 draft ARSENAL revised/AMC 25.1309, as applicable to this type of airplane.

The classification of each failure condition for each flight phase is shown in Column 5 of Table Q.3-5.

Q.3.4.6 AFHA Assumptions and Failure Condition Classification Criteria

Assumptions made while accomplishing the effect evaluation of each failure condition have been captured and numerically identified for reference. Table Q.3-4 presents the analysis assumptions, notes, or failure condition classification criteria which have been captured during the development of this AFHA.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.3-4 - (AFHA)
S18 AFHA assumptions/notes

Assumption Identifier	Description
ASMP 3.2.2-1	Overrunning the runway length above “XYZ” knots is considered a high-speed overrun. *(Editor’s Note: “XYZ” overrun speed value would be defined in a normal assessment.)*
ASMP 3.2.2-2	The directional aspect of asymmetric failures of deceleration systems are functionally addressed by failure conditions of the “Control direction on ground” airplane function. See function 2.3 AFHA *(Editor’s Note: not included in this example)*.
ASMP 3.2.2-3	The flight crew will divert to a suitable airfield if aware of a condition that renders the airplane incapable of landing at the originally intended destination.
ASMP 3.2.2-4	Crew awareness is not a factor for the identified malfunction, as these are immediately evident due to airplane behavior and do not have their effects intensified or mitigated by crew awareness features.
ASMP 3.2.2-5	The flight crew will not initiate an RTO in response to an annunciated failure of deceleration features during takeoff due to alert suppression.
ASMP 3.2.2-6	Taxi is performed at groundspeeds below 30 knots.
ASMP 3.2.2-7	Landings with the failure condition in combination with environmental factors have been assessed. *(Editor’s Note: For brevity, environmental effects on landing failure conditions are not explicitly stated and described.)*
ASMP 3.2.2-8	Failures of deceleration capability will be detected and annunciated by on-board systems.

(Editor’s Note: The airplane/systems development process will evaluate the validity of the assumptions as part of normal activities.)

Q.3.4.7 AFHA Outputs

In addition to the list of assumptions, the AFHA output includes the populated worksheets with functions, failure conditions, effects, and severity classifications.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.3-5 - (AFHA)
S18 AFHA ("Decelerate on ground" function only)

(Editor's Note: The effects for each airplane flight phase (Q.3.4.4.1) have been captured in the example S18 Airplane FHA worksheets in order to present a comprehensive FHA concept. This may not be normal practice in all organizations. The specific effects and classifications shown here are for illustrations purposes and may not reflect real-world situations.)

1 **Function/ ID No.**	2 **Failure Condition**	3 **Flight Phase**	4 **Effects**	5 **Classification**	6 **References/ Notes**
3.2.2 Decelerate on ground					
3.2.2.TL.A	Loss of ability to decelerate with crew aware	Taxi	**Aircraft:** Slight reduction/loss of deceleration capability. **Flight crew:** Aware of the condition, crew will abort flight operation. Slight increase in crew workload to avoid collision. **Other occupants:** Inconvenience due to delayed flight.	Minor	ASMP 3.2.2-6
		Takeoff Climb Cruise Descent Approach	**Aircraft:** No immediate effect. Severe reduction/loss in deceleration capability. Potential inability to decelerate airplane using airplane flight manual guidelines within any available runway. Potential hull loss. **Flight crew:** Aware of the condition, crew will execute emergency procedures (e.g., divert to a more suitable landing location, minimize landing airspeed and minimize airplane weight for landing). Excessive crew workload increase due to execute emergency procedures and need to perform the abnormal landing. **Other occupants:** Potential multiple fatal injuries in the event of collision with obstacles or terrain due to runway overrun.	Catastrophic	ASMP-3.2.2-1 ASMP 3.2.2-3 ASMP 3.2.2-7
		Landing	**Aircraft:** Severe reduction in deceleration capability. Unable to decelerate airplane using airplane flight manual guidelines any available runway. Runway overrun above "XYZ" knots. Potential hull loss. **Flight crew:** Though aware of the condition, crew will already be committed to the landing. Excessive crew workload to attempt to avoid obstacle collision during the high-speed overrun. **Other occupants:** Potential multiple fatal injuries in the event of collision with obstacles or terrain.	Catastrophic	ASMP 3.2.2-1 ASMP 3.2.2-7

SAENORM.COM : Click to view the full PDF of arp4761a

1 Function/ ID No.	2 Failure Condition	3 Flight Phase	4 Effects	5 Classification	6 References/ Notes
3.2.2 Decelerate on ground					
3.2.2.TL.U	Loss of ability to decelerate with crew unaware	Taxi	**Aircraft:** Slight reduction/loss deceleration capability. Reduction of functional capability during taxi. **Flight crew:** Crew is unaware of the condition until attempting to decelerate. Crew may be unable to fully stop the airplane resulting in low taxi speed collision or taxiway overrun. Significant increase in crew workload to avoid these conditions. **Other occupants:** Potential injury to unrestrained cabin crew in case of collision.	Major	ASMP 3.2.2-6
		Takeoff Climb Cruise Descent Approach	**Aircraft:** No immediate effect. Severe reduction/loss of deceleration capability when needed in Landing phase. **Flight crew:** No immediate effect. Crew unaware of condition and will proceed with normal flight operation until landing. **Other occupants:** No immediate effect. Potential fatalities during landing.	Catastrophic	
		Landing	**Aircraft:** Severe reduction/loss of deceleration capability. Severely reduced deceleration capability results in overrun above “XYZ” knots. Potential hull loss. **Flight crew:** Unaware of the condition, crew will proceed with normal flight operation until landing. Excessive crew workload to attempt to avoid obstacle collision during the runway length overrun. **Other occupants:** Potential multiple fatal injuries in the event of collision with obstacles or terrain.	Catastrophic	ASMP 3.2.2-1 ASMP 3.2.2-7
3.2.2.TL.RTO	Loss of ability to decelerate in combination with Rejected Takeoff (RTO)	Taxi	Not applicable. RTO is operational situation performed only during takeoff phase.	No Effect	
		Takeoff	**Aircraft:** Severe reduction/loss of deceleration capability. Unable to decelerate within takeoff runway. Runway overrun above “XYZ” knots. Potential hull loss. **Flight crew:** Crew will initiate RTO due to an independent failure or occurrence. During RTO, excessive crew workload to attempt to avoid obstacle collision during the overrun. **Other occupants:** Potential multiple fatal injuries in the event of collision with obstacles or terrain.	Catastrophic	ASMP 3.2.2-1 ASMP 3.2.2-4
		Climb Cruise Descent Approach Landing	Not applicable. RTO is operational situation performed only during takeoff phase.	No Effect	

SAENORM.COM : Click to view the full PDF of arp4761a

1 Function/ ID No.	2 Failure Condition	3 Flight Phase	4 Effects	5 Classification	6 References/ Notes
3.2.2 Decelerate on ground					
3.2.2.PL.A	Partial loss of ability to decelerate with crew aware	Taxi	**Aircraft:** Reduced deceleration capability. Slight reduction of functional capability during taxi. **Flight crew:** Aware of the condition, crew will abort flight operation. Slight increase in crew workload to avoid collision. **Other occupants:** Inconvenience due to delayed flight.	Minor	ASMP 3.2.2-6 ASMP 3.2.2-8
		Takeoff	**Aircraft:** Reduced deceleration capability. Slight reduction in safety margins for takeoff. **Flight crew:** Crew will continue the takeoff normally. Aware of the condition, crew will divert to a suitable landing location and minimize weight for landing. Significant increase in crew workload to plan and perform the abnormal landing. **Other occupants:** Inconvenience due to diversion.	Major	ASMP 3.2.2-3 ASMP 3.2.2-5
		Climb Cruise Descent Approach	**Aircraft:** No immediate effect. Reduced deceleration capability when needed in landing phase. **Flight crew:** Aware of the condition, crew will divert to a suitable landing location and minimize weight for landing. Excessive crew workload increase to execute emergency procedures and perform the abnormal landing. **Other occupants:** Inconvenience due to diversion.	Hazardous	ASMP 3.2.2-3
		Landing	**Aircraft:** Reduced deceleration capability. Unable to decelerate within destination runway. Runway overrun above “XYZ” knots. Potential hull loss. **Flight crew:** Crew awareness of loss of deceleration capability occurs as crew is already committed to the landing. Excessive workload to minimize damage during the high-speed overrun. **Other occupants:** Potential multiple fatal injuries in the event of collision with obstacles or terrain.	Catastrophic	ASMP 3.2.2-1 ASMP 3.2.2-4 ASMP 3.2.2-7

SAENORM.COM : Click to view the full PDF of arp4761a

1 Function/ ID No.	2 Failure Condition	3 Flight Phase	4 Effects	5 Classification	6 References/ Notes
3.2.2 Decelerate on ground					
3.2.2.PL.U	Partial loss of ability to decelerate with crew unaware	Taxi	**Aircraft:** Reduced deceleration capability. Reduction of functional capability during taxi. **Flight crew:** Crew is unaware of the condition until attempting to decelerate. Crew may be unable to fully stop the airplane resulting in low taxi speed collision or taxiway overrun. Significant increase in crew workload to avoid these conditions. **Other occupants:** Potential injury to unrestrained cabin crew in case of collision.	Major	ASMP 3.2.2-6
		Takeoff Climb Cruise Descent Approach Landing	**Aircraft:** Reduced deceleration capability. Unable to decelerate within destination runway. Overrun below “XYZ” knots. **Flight crew:** Unaware of the condition, crew will proceed with normal flight operation on landing. During landing, excessive crew workload to minimize damage during the overrun due to inability to decelerate. **Other occupants:** Potential multiple fatal injuries in the event of collision with obstacles or terrain.	Catastrophic	ASMP 3.2.2-2 ASMP 3.2.2-7
3.2.2.PL.RTO	Partial loss of ability to decelerate in combination with RTO	Taxi	Not applicable. RTO is operational situation performed only during takeoff phase.	No Effect	
		Takeoff	**Aircraft:** Reduced deceleration capability. May be unable to decelerate within takeoff runway. Runway overrun above “XYZ” knots. Potential hull loss. **Flight crew:** Crew will initiate RTO due to an independent failure or occurrence. During RTO, excessive crew workload to attempt to avoid obstacle collision during the overrun. **Other occupants:** Potential multiple fatal injuries in the event of collision with obstacles or terrain.	Catastrophic	ASMP 3.2.2-1
		Climb Cruise Descent Approach Landing	Not applicable. RTO is operational situation performed only during takeoff phase.	No Effect	

SAENORM.COM : Click to view the full PDF of arp4761a

1 Function/ ID No.	2 Failure Condition	3 Flight Phase	4 Effects	5 Classification	6 References/ Notes
3.2.2 Decelerate on ground					
3.2.2.MF1	Uncommanded deceleration on ground	Taxi	**Aircraft:** Partial or total application of uncommanded deceleration may cause the airplane to be incapable of continuing taxi. **Flight crew:** Crew will observe the condition and will abort taxi operation. **Other occupants:** Inconvenience due to missed flight.	Minor	ASMP 3.2.2-2 ASMP 3.2.2-4
		Takeoff	**Aircraft:** Partial or total deceleration applied. Uncommanded deceleration above V1 may prevent successful takeoff and result in overrun above “XYZ” knots. **Flight crew:** Crew will be unaware of uncommanded brake application. Uncommanded deceleration application prior to airplane achieving V1 will be observed by crew and successful rejected takeoff will be achieved. Uncommanded deceleration application after airplane achieves V1 will result in airplane not achieving VR. Crew unable to takeoff resulting in a high-speed overrun. **Other occupants:** Potential multiple fatal injuries in the event of collision with obstacles or terrain.	Catastrophic	ASMP 3.2.2-1 ASMP 3.2.2-2 ASMP 3.2.2-4
		Climb Cruise Descent Approach	Airborne flight phases are not applicable to this failure condition.	No Effect	
		Landing	**Aircraft:** Partial or total uncommanded deceleration on touch down or during the landing roll. Landing roll may be abbreviated. Airplane may be incapable of taxi-in. **Flight crew:** Crew will observe the condition and continue the landing rollout normally. **Other occupants:** Inconvenience due to inability to taxi.	Minor	ASMP 3.2.2-2 ASMP 3.2.2-4

SAENORM.COM : Click to view the full PDF of arp4761a

1 Function/ ID No.	2 Failure Condition	3 Flight Phase	4 Effects	5 Classification	6 References/ Notes
3.2.2 Decelerate on ground					
3.2.2.MF2	Excessive deceleration intensity when commanded on ground	Taxi Takeoff	**Aircraft:** Excessive deceleration when commanded. **Flight crew:** Crew will note unusual airplane response to deceleration commands. Slight increase in crew workload may be necessary to counter the condition. Crew may abort flight operation if airplane ground handling is significantly affected. **Other occupants:** Inconvenience due to missed flight.	Minor	ASMP 3.2.2-4
		Climb Cruise Descent Approach	Airborne flight phases are not applicable to this failure condition.	No Effect	
		Landing	**Aircraft:** Increased deceleration intensity when commanded resulting in shorter stopping distances. **Flight crew:** Crew will note the increased deceleration capability condition and continue the landing/rollout normally. Slight increase in crew workload may be necessary to counter the condition during taxi-in. **Other occupants:** Occupant discomfort due to increased forward body forces due to high than normal applied stopping intensity.	Minor	ASMP 3.2.2-4

SAENORM.COM : Click to view the full PDF of arp4761a

1 Function/ ID No.	2 Failure Condition	3 Flight Phase	4 Effects	5 Classification	6 References/ Notes
3.2.2 Decelerate on ground					
3.2.2.MF3	Reduced deceleration intensity when commanded on ground	Taxi Takeoff	**Aircraft:** Reduced deceleration intensity when commanded resulting in longer stopping distances. **Flight crew:** Crew will note the decrease in deceleration capability condition. Slight increase in crew workload may be necessary to counter the condition during taxi. Crew may abort flight operation if airplane ground handling is significantly affected. **Other occupants:** Inconvenience due to missed flight.	Minor	ASMP 3.2.2-4
		Climb Cruise Descent Approach	Airborne flight phases are not applicable to this failure condition.	No Effect	
		Landing	**Aircraft:** Reduced deceleration intensity when commanded resulting in longer stopping distances. **Flight crew:** Crew will note the decrease in deceleration capability condition and continue the landing/rollout normally. Slight increase in crew workload may be necessary to counter the condition during rollout and taxi. **Other occupants:** No effect.	Minor	ASMP 3.2.2-4
3.2.2.MF3.RTO	Reduced deceleration intensity when commanded in combination with RTO	Taxi	Not applicable to this failure condition.	No Effect	ASMP 3.2.2-4
		Takeoff	**Aircraft:** Reduced deceleration intensity when commanded resulting in longer stopping distances. **Flight crew:** Crew will note the decrease in deceleration capability condition. Significant increase in crew workload may be necessary to counter the condition during taxi. Crew may abort flight operation if airplane ground handling is significantly affected. **Other occupants:** Inconvenience due to missed flight.	Major	
		Climb Cruise Descent Approach	Airborne flight phases are not applicable to this failure condition.	No Effect	
		Landing	Not applicable to this failure condition.	No Effect	
Etc.					

SAENORM.COM : Click to view the full PDF of arp4761a

Q.4 S18 AIRPLANE - PRELIMINARY AIRCRAFT SAFETY ASSESSMENT (PASA) EXAMPLE

PASA EXAMPLE

Q.4.1 PASA Example Introduction

This section comprises the Preliminary Aircraft Safety Assessment (PASA) example for the S18 airplane.

For the sake of brevity, only one failure condition from the AFHA example has been selected to be developed in detail for this PASA example, since this provides sufficient complexity to allow use of all methodologies, yet it is simple enough to present a clear picture of this process. All other failure conditions would be assessed by the same method shown here. Other failure conditions from the AFHA example may be cited where appropriate, but are not developed in detail.

Q.4.2 Input

Q.4.2.1 Airplane Functions

The S18 airplane level functions have been defined and are captured in ARP4754B/ED-79B, Appendix E.

The selected function to exemplify the S18 PASA process is “**Decelerate on Ground**”. This function is a decomposition of “Reduce Airplane Energy”, which is a second level function of the first level airplane function “Control Airplane Energy”.

3. Control Airplane Energy
  3.2 Reduce Airplane Energy
  3.2.2 Decelerate on Ground

Q.4.2.2 Selected Failure Conditions from AFHA

The selected failure condition from AFHA example (Table Q.3-5) to be developed in detail for this PASA example, which is related to the function “Decelerate on Ground”, is:

ID Number	Failure Condition	Flight Phase	Classification
3.2.2.TL.A	**Loss of ability to decelerate with crew aware**	Landing	Catastrophic

The phases of takeoff, climb, cruise, descent, and approach are also indicated as Catastrophic in Table Q.3-5 - although there is no immediate effect on the airplane in these phases, the effect is realized in the landing phase so the PASA also considers the earlier flight phases impacting the landing.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.4.2.3 S18 Airplane Architecture Information

The following airplane architecture information is provided by the development process (ARP4754B/ED-79B, Appendix E), as an input to the PASA:

Review of the S18 airplane architecture shows that the “Decelerate on Ground” function is intended to be accomplished using two independent systems:

Wheel Brakes. The S18 airplane has two main landing gear struts with four wheels each for a total of eight wheels. Each wheel is equipped with a brake.

Thrust Reversers. The S18 airplane is equipped with a thrust reverser on each engine. The thrust reversers are intended to aid deceleration; especially in conditions where friction-based deceleration is ineffective (wet or iced runways).

The following airplane features can affect the “Decelerate on Ground” function:

Engines. The S18 airplane has two under wing mounted turbofan engines in order to produce forward thrust. The engine thrust must be reduced to a minimum during deceleration on ground, to maximize deceleration and allow deployment of the thrust reversers.

Flaps. The S18 airplane’s wings are each equipped with two flap panels. The flaps are extended to increase the wing’s lift and drag coefficients. The flaps are extended to allow lower takeoff and landing speeds, which facilitates deceleration on ground.

Spoilers. The S18 airplane’s wings are each equipped with two spoiler panels. The spoilers are intended to be deployed on landing, to reduce lift and increase the effectiveness of the wheel brakes.

The airplane-level architecture would be reviewed in a similar fashion with regard to contribution or interference with each of the airplane-level functions.

Q.4.2.4 S18 Systems Architecture Information

The systems information available at the beginning of the PASA process may be incomplete or prone to change. The PASA may be initiated using assumptions where development data is not available. The use of assumptions is captured as part of the assessment.

The following systems architecture information based on the airplane functional, operational and certification requirements is provided by the development process (ARP4754B/ED-79B, Appendix E), as input to PASA:

1) **Wheel Brake System (WBS).** The WBS actuates all eight brakes on the main gear wheels. An EBU provides brake pedal position inputs to the WBS. The WBS is hydraulically actuated and powered by hydraulic system 1 (HYD 1) and hydraulic system 2 (HYD 2). The WBS is electrically controlled. The WBS uses redundant electrical buses such that no single electrical bus loss results in loss of the WBS. The WBS uses the ground detection information as an input. The WBS implements the function “Decelerate the Wheels on the Ground (F1).”

F1 - Decelerate wheels on ground by providing WBS control and capability

FF1 - Fail to provide WBS control and capability

FF1.1 - Total loss of wheel braking capability

FF1.2 - Partial loss of wheel braking capability

The following notation is used: Fx is the function while FFx is the general functional failure of Fx, and FFx.y is a detailed functional failure of Function Fx.

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: This description reflects the WBS architecture at this point in the development however other changes emerge as the Preliminary Aircraft Safety Assessment (PASA) and Preliminary System Safety Assessment (PSSA) identify issues.)

2) **Ground Spoiler System.** The ground spoiler system actuates all four spoilers on the wings. The symmetric spoilers on the left and right wings are controlled in pairs. The two pairs of spoilers may be commanded symmetrically in response to pilot manual commands. There is no automatic spoiler command in the S18 airplane. There is no other method of controlling or actuating the spoilers. The ground spoiler system is hydraulically actuated and powered by HYD 1 and hydraulic system 3 (HYD 3). The ground spoiler system is electrically controlled by an Electronic Flight Control Unit (EFCU). The ground spoiler system uses redundant electrical buses such that no electrical single loss results in loss of any EFCU channel. The ground spoiler system uses the ground detection information and wheel speed data as inputs. The ground spoiler system implements the function "Aerodynamic Braking (F2)."

F2 - Aerodynamic braking by providing ground spoiler system control and capability

FF2 - Fail to provide ground spoiler system control and capability

FF2.1 - Total loss of aerodynamic braking capability

FF2.2 - Partial loss of aerodynamic braking capability

3) **Thrust Reverser System.** The thrust reverser system controls and actuates the thrust reversing mechanisms on each engine. Each reversing mechanism is controlled independently in response to pilot manual commands. There is no automatic thrust reverser command in the S18 airplane. The thrust reverser system is hydraulically actuated and powered by HYD 1 and HYD 2. The thrust reverser system is electrically controlled by an Electronic Engine Control Unit (EECU). The thrust reverser system uses redundant electrical buses such that no electrical single loss results in loss of any EECU channel. The thrust reverser system uses the ground detection information as an input. The thrust reverser system implements the function "Reverse Thrust on Ground (F3)."

F3 - Thrust reversing on ground by providing thrust reverser system control and capability

FF3 - Fail to provide thrust reverser system control and capability

FF3.1 - Total loss of thrust reversing capability

FF3.2 - Partial loss of thrust reversing capability

4) **Flap System.** The flap system actuates the multiple flap surfaces on the wings. All flap surfaces are controlled simultaneously in response to pilot manual commands. There is no automatic flap command in the S18 airplane. There is no other method of controlling or actuating the flaps. The flap system is hydraulically actuated and powered by HYD 1 and HYD 3. The flap system is electrically controlled by the EFCU. The EFCU uses redundant electrical buses such that no electrical single loss results in loss of any EFCU channel. The flap system implements the function "Provide High Lift (F4)."

F4 - High lifting by providing flap system control and capability

FF4 - Fail to provide flap system control and capability

FF4.1 - Total loss of high lifting capability

FF4.2 - Partial loss of high lifting capability

SAENORM.COM : Click to view the full PDF of arp4761a

5) **Propulsion System.** The propulsion system controls forward thrust on each engine in response to pilot manual commands. There is no automatic propulsion command in this S18 airplane. The propulsion system is electrically controlled through 2 EECUs. The left-hand engine EECU controls the left-hand engine and the right-hand engine EECU controls the right-hand engine. The propulsion system relies only on ground detection information from other airplane systems as an input. The propulsion system implements the function “Control Engine Thrust on Ground (F5).”

F5 - Controlled engine thrust on ground by providing propulsion system control and capability

FF5 - Fail to provide propulsion system control and capability

FF5.1 - Total loss of engine thrust and control

FF5.2 - Partial loss of engine and thrust

FF5.3 - Propulsion sys malfunction: uncommanded engine high thrust on ground

R1) **Hydraulic System.** The hydraulic system provides power to multiple airplane systems. There are three hydraulic systems on the S18 airplane. HYD 1 is driven by engine 1 (left hand). HYD 2 is driven by engine 2 (right hand). An additional hydraulic system, HYD 3, provides minimal flight control capability in case of the loss of all engines in flight, ref. 14 CFR/CS 25.671(d).

FR1 - Provide hydraulic power generation and distribution

R2) **Electrical System.** The electrical system provides power to multiple airplane systems. There are three major electrical buses distributing power to airplane systems. Each major electrical bus can be powered by one or more engine driven generators. The system architecture was conceived to provide power to multiple systems such that no single electrical system failure causes loss of any essential loads.

FR2 - Provide electrical power generation and distribution.

R3) **Ground Detection Information System.** The ground detection information system provides information to multiple airplane systems. The in-air or on-ground status of the airplane is determined by detecting compression of the left and right main landing gear shock absorbers and its information is consolidated using both signals. Whenever the signals mismatch, an additional input from wheel speed is used to accommodate this failure. The air/ground system is electrically powered.

FR3 - Provide ground detection information generation and distribution function.

Q.4.2.5 S18 Systems Functional Hazard Assessment Information

(*Editor´s Note: The System Functional Hazard Assessments (SFHAs) are not needed to start the PASA, as the SFHAs might not be ready when the PASA process begins, since the PASA and the SFHA may be in different states of completion. In that case, using system functions as inputs to PASA, the system functional failure effects may be identified in the Combined Functional Failure Effects (CoFFE) Analysis (Q.4.4.1), and these failure states may later support the SFHA completion. It is considered that irrespective of whether the crew is aware of the failure (see 1.1.TL1.A and 1.1.TL1.U), the Total loss of wheel deceleration capability (≥ 80%) is Hazardous (except for taxi phase). Thus, the failure condition: WBS.TL is the combination of 1.1.TL1.A or 1.1.TL1.U from the WBS SFHA in Q5.)*

The system-level functions are defined by the development process, and captured by the various SFHA. The system-level failure conditions are developed in the SFHA for each system.

SAENORM.COM : Click to view the full PDF of arp4761a

The SFHA for the WBS has been developed in the WBS SFHA example (Section Q.5). The relevant failure conditions for the other systems affecting the “Decelerate on Ground” function have been assumed to be as shown below.

1) Wheel Brake System failure conditions (from Wheel Brake SFHA, provided in this example):

WBS.TL Total loss of wheel deceleration capability (80% or more)
WBS.PL1.A Symmetric loss of 50% to 80% wheel deceleration capability with crew aware
WBS.PL2.A Symmetric loss of less than 50% wheel deceleration capability, crew aware

2) Ground Spoiler System failure conditions (from Ground Spoiler SFHA, assumed):

GSS.TL Total loss of ground spoiler deployment
GSS.PL Loss of deployment of 2 or less ground spoiler panels

3) Thrust Reverser System failure conditions (from Thrust Reverser SFHA, assumed):

TRS.TL Loss of thrust reverser deployment
TRS.PL Loss of deployment of 1 thrust reverser

4) Flap System failure conditions (from Flap SFHA, assumed):

FLS.TL Total loss of flap deployment
FLS.PL Loss of deployment of 2 or less flap panels

5) Propulsion System failure conditions (from Propulsion SFHA, assumed):

PRS.MF Uncommanded high thrust on one or more engines

Resource Systems:

R1) Hydraulic System failure conditions (from Hydraulic SFHA, assumed):

HYS.TL Total loss of hydraulic power
HYS.PL1 Loss of hydraulic power from any one subsystem
HYS.PL2 Loss of hydraulic power from any two subsystems

R2) Electrical System failure conditions (from Electrical SFHA, assumed):

ELS.TL Total loss of electric power
ELS.PL1 Loss of electrical power to any one bus

R3) Ground Detection Information System failure conditions (from Ground Detection Information SFHA, assumed):

AGS.TL Total loss of ground detection information
AGS.MF Erroneous information from all ground detection information

(Editor´s Note: Except for 1) Wheel Brake System, all other systems’ failure conditions have not been developed in Appendix Q. They are just assumed to allow this example to show PASA process flow.)

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor´s Note: There may be interdependencies such as (1) the propulsion system powers the hydraulics and electrical systems, and (2) the electrical power system powers the hydraulic system controllers and the ground detection logic; these details are not shown in this limited example.)

Q.4.3 Interdependence Analysis

The Interdependence Analysis may be supported through an interdependence diagram and/or an interdependence table. For this example, it is represented in the interdependence Table Q.4-1.

This analysis is conducted by systematically following steps: (1) selecting airplane-level function and associated AFHA failure conditions to be analyzed; (2) listing all contributing systems based on the S18 airplane architecture; (3) identifying with “x” those systems that contribute to that airplane-level failure conditions.

Table Q.4-1 - (PASA)
Interdependence table

Airplane Function	**Airplane Failure Condition ID**	**Airplane Failure Condition Description**	**Airplane Systems (Function)**					
			1	**2**	**3**	**4**	**5**	**…**
			Wheel Brake (F1 - decelerate wheels on ground)	**Ground Spoiler (F2 - aero brake on ground)**	**Thrust Reverser (F3 - reverse thrust on ground)**	**Flap (F4 - high lift flight)**	**Propulsion (F5 - control thrust on ground)**	**...**
3.2.2 Decelerate on ground	3.2.2. TL.A	Loss of ability to decelerate with crew aware	X	X	X	X	X	
…	…	…	…	…	…	…	…	…

(Editor’s Note: Interdependence analysis should also identify systems which do not contribute to the airplane level function but whose functional failures may contribute to the airplane level failure condition, e.g., the high-lift system does not contribute, per se, to the airplane level function deceleration on ground; however, a non-extension of the flaps may contribute to the failure condition insufficient deceleration on ground as the airplane approach speed will be higher than normal. Another example is the propulsion system does not contribute to deceleration on ground function but rather its malfunction, i.e., uncontrollable high thrust (UHT) on ground, leads to the considered failure condition.)

(Editor’s Note: Not all systems in the airplane architecture have been included for brevity.)

(Editor´s Note: When developing the interdependence table, common resource systems, which provide power and information across the airplane systems, and sometimes known as multisystem, might not be identified in the first iteration to build the interdependence table, mostly when the data is not available. As the development progresses, these resource systems may be identified. This example will show a development stage when this data is available.)

SAENORM.COM : Click to view the full PDF of arp4761a

In the interdependence (common resource) Table Q.4-2, an “x” is identified for those common resource systems that make contribution to each of the airplane systems functions:

Table Q.4-2 - (PASA)
Interdependence (common resource) table

		Airplane Systems (Function)				
		1	**2**	**3**	**4**	**5**
		Wheel Brake (F1 - decelerate wheels on ground)	**Ground Spoiler (F2 - aero brake on ground)**	**Thrust Reverser (F3 - reverse thrust on ground)**	**Flap (F4 - high lift in flight)**	**Propulsion (F5 - control thrust on ground)**
Common Sources and Resources (Generation and Distribution)	**R1. Hydraulic Power**	x	x	x	x	--
	R2. Electrical Power	x	x	x	x	--
	R3. Ground Detection Information	--	x	x	--	--

SAENORM.COM : Click to view the full PDF of arp4761a

Q.4.4 Failure Condition Evaluation

The airplane-level failure conditions are evaluated combining failures of the systems which contribute to the airplane level function. These contributing systems are identified in the Interdependence Analysis of Q.4.3.

Later, this is to be verified across the SFHAs in order to trace the system failure conditions up to the airplane level failure conditions.

Q.4.4.1 Combined Functional Failure Effects Analysis

A Combined Functional Failure Effects (CoFFE) table is used to analyze system failure effects individually and in combination with one another. The CoFFE analysis maps the airplane effects of those systems functional failures in order to support the fault tree branches identification.

Then the airplane stopping capabilities are assessed to verify if these lead to the failure condition event. The stopping capability results are determined and substantiated by the S18 airplane performance analyses and simulations data, which takes into account the same environmental and operational conditions as considered in the AFHA.

(Editor’s Note: The S18 airplane takes credit for use of the thrust reverser for the landing distance performance. This assumption may not be supported by the policy or guidance, but it has been used for the sake of brevity to show an example of this process flow.)

For those contributing systems identified in Q.4.3, the functional failures considered are the total loss of system function, partial loss of system function, and also the system malfunction when relevant. These systems functional failures considered here can be associated with the systems failure conditions whenever the associated SFHA is available.

Those considered total loss of systems functions (failed states) and the associated systems failure conditions from the SFHA are listed in Table Q.4-3.

Table Q.4-3 - (PASA)
System functional failures and SFHA failure conditions: Total loss

System Functional Failures	Associated Sys Failure Condition (SFHA)
FF1.1 - Total loss wheel brake sys function (loss of means to decelerate all wheels on ground)	WBS.TL - Total loss of wheel deceleration capability (80% or more)
FF2.1 - Total loss of ground spoiler sys function (loss of means for deploying all spoilers on ground)	GSS.TL - Total loss of ground spoiler deployment
FF3.1 - Total loss of thrust reverser sys function (loss of means for deploying both reversers on ground)	TRS.TL - Loss of thrust reverser deployment
FF4.1 - Total loss of flap sys function (loss of means for extending all flaps)	FLS.TL - Total loss of flap deployment

Those considered partial loss of systems functions (degraded states) and the associated systems failure conditions from the SFHA are listed in Table Q.4-4.

Table Q.4-4 - (PASA)
System functional failures and SFHA failure conditions: Partial loss

System Functional Failures	Associated Sys Failure Condition (SFHA)
FF1.2 - Partial loss wheel brake sys function (loss of half capability means to decelerate wheels on ground)	WBS.PL2.A - Symmetric loss of less than 50% wheel deceleration capability, crew aware
FF2.2 - Partial loss of ground spoiler sys function (loss of half capability means for deploying spoiler on ground)	GSS.PL - Loss of deployment of two or less ground spoiler panels
FF3.2 - Partial loss of thrust reverser sys function (loss of means for deploying one reverser on ground, either the LH or RH side)	TRS.PL - Loss of deployment of one thrust reverser
FF4.2 - Partial loss of flap sys function (loss of half capability means for extending flap)	FLS.PL - Loss of deployment of two or less flap panels

(Editor´s Note: In this example, the degradation of function has been considered useful since it aids in defining fault tree boundary cases. The degraded state considered useful for each particular system has been defined such as 1/2 functional capability.)

(Editor´s Note: An example of Common Resource Analysis is not included here. An example is shown in Table B3.)

The considered system malfunction and the associated system failure condition from the SFHA is shown in Table Q.4-5.

Table Q.4-5 - (PASA)
System functional failures and SFHA failure conditions: malfunction

System Functional Failures	Associated System Failure Condition (SFHA)
FF5.3 - Uncommanded engine high thrust (malfunction)	PRS.MF - Uncommanded high thrust on one or more engines

As FF5.3 system functional failure is already associated to a Catastrophic failure condition from the SFHA PRS.MF, it is not pertinent to identify this functional failure within the CoFFE table since it is allocated to the Propulsion PSSA. The resulting Table Q.4-6 maps combinations of failed and degraded systems, also including the operational states of these systems functions resulting in 81 cases.

The overrun classifications have been assigned for each of these failure cases to help identify those resulting in the top airplane failure condition event. The criteria and terms “high-speed overrun” and “low-speed overrun” is according to the AFHA assumption ASMP 3.2.2-1 and ASMP 3.2.2-6.

(Editor´s Note: It is assumed that the high-speed overrun is above 30 knots and low-speed overrun is below (or equal to) 30 knots.)

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.4-6 - (PASA)
CoFFE table

Case #	Wheel Brake	Ground Spoiler	Thrust Reverser	Flap	Stopping Capability Result
1	F	F	F	F	High-speed overrun
2	F	F	F	D	High-speed overrun
3	F	F	F	O	High-speed overrun
4	F	F	D	F	High-speed overrun
5	F	F	D	D	High-speed overrun
6	F	F	D	O	High-speed overrun
7	F	F	O	F	High-speed overrun
8	F	F	O	D	High-speed overrun
9	F	F	O	O	High-speed overrun
10	F	D	F	F	High-speed overrun
11	F	D	F	D	High-speed overrun
12	F	D	F	O	High-speed overrun
13	F	D	D	F	High-speed overrun
14	F	D	D	D	High-speed overrun
15	F	D	D	O	High-speed overrun
16	F	D	O	F	High-speed overrun
17	F	D	O	D	High-speed overrun
18	F	D	O	O	High-speed overrun
19	F	O	F	F	High-speed overrun
20	F	O	F	D	High-speed overrun
21	F	O	F	O	High-speed overrun
22	F	O	D	F	High-speed overrun
23	F	O	D	D	High-speed overrun
24	F	O	D	O	High-speed overrun
25	F	O	O	F	High-speed overrun
26	F	O	O	D	High-speed overrun
27	F	O	O	O	Low-speed overrun
28	D	F	F	F	Low-speed overrun
29	D	F	F	D	Low-speed overrun
30	D	F	F	O	Low-speed overrun
31	D	F	D	F	Low-speed overrun
32	D	F	D	D	Low-speed overrun
33	D	F	D	O	Low-speed overrun
34	D	F	O	F	Low-speed overrun
35	D	F	O	D	Low-speed overrun

SAENORM.COM : Click to view the full PDF of arp4761a

Case #	Wheel Brake	Ground Spoiler	Thrust Reverser	Flap	Stopping Capability Result
36	D	F	O	O	No overrun
37	D	D	F	F	Low-speed overrun
38	D	D	F	D	Low-speed overrun
39	D	D	F	O	Low-speed overrun
40	D	D	D	F	Low-speed overrun
41	D	D	D	D	Low-speed overrun
42	D	D	D	O	No overrun
43	D	D	O	F	Low-speed overrun
44	D	D	O	D	No overrun
45	D	D	O	O	No overrun
46	D	O	F	F	Low-speed overrun
47	D	O	F	D	Low-speed overrun
48	D	O	F	O	No overrun
49	D	O	D	F	Low-speed overrun
50	D	O	D	D	No overrun
51	D	O	D	O	No overrun
52	D	O	O	F	No overrun
53	D	O	O	D	No overrun
54	D	O	O	O	No overrun
55	O	F	F	F	No overrun
56	O	F	F	D	No overrun
57	O	F	F	O	No overrun
58	O	F	D	F	No overrun
59	O	F	D	D	No overrun
60	O	F	D	O	No overrun
61	O	F	O	F	No overrun
62	O	F	O	D	No overrun
63	O	F	O	O	No overrun
64	O	D	F	F	No overrun
65	O	D	F	D	No overrun
66	O	D	F	O	No overrun
67	O	D	D	F	No overrun
68	O	D	D	D	No overrun
69	O	D	D	O	No overrun
70	O	D	O	F	No overrun
71	O	D	O	D	No overrun
72	O	D	O	O	No overrun

SAENORM.COM : Click to view the full PDF of arp4761a

Case #	Wheel Brake	Ground Spoiler	Thrust Reverser	Flap	Stopping Capability Result
73	O	O	F	F	No overrun
74	O	O	F	D	No overrun
75	O	O	F	O	No overrun
76	O	O	D	F	No overrun
77	O	O	D	D	No overrun
78	O	O	D	O	No overrun
79	O	O	O	F	No overrun
80	O	O	O	D	No overrun
81	O	O	O	O	No overrun

Legend:

F	Failed (total loss of function)
D	Degraded (partial loss of function)
O	Operational (no loss of function)

The failure combinations of Table Q.4-6 are logically reduced to the minimum contributors to the stopping capability results (i.e., CoFFE filter). The resulting CoFFE table summary is presented in Table Q.4-7. The boundaries among “High-speed overrun,” “Low-speed overrun,” and “No overrun” have been captured.

Table Q.4-7 - (PASA)
CoFFE table summary

Wheel Brake	Ground Spoiler	Thrust Reverser	Flap	Stopping Capability Result	Conclusion
F	D	O	O	High-speed overrun	Total loss of wheel brake in addition to partial loss of any ground spoiler or thrust reverser or flap functions resulting in high-speed overrun
F	O	D	O	High-speed overrun	
F	O	O	D	High-speed overrun	
F	O	O	O	Low-speed overrun	Total loss of wheel brake function resulting in low-speed overrun
D	D	D	D	Low-speed overrun	Partial loss of wheel brake in addition to ground spoiler and thrust reverser and flap functions resulting in low-speed overrun
D	O	O	O	No overrun	
O	F	F	F	No overrun	

SAENORM.COM : Click to view the full PDF of arp4761a

The systems functional failures combinations that result in the high-speed overruns, i.e., lead to the AFHA failure condition events are identified in Table Q.4-8.

Table Q.4-8 - (PASA)
CoFFE table result: High-speed overrun

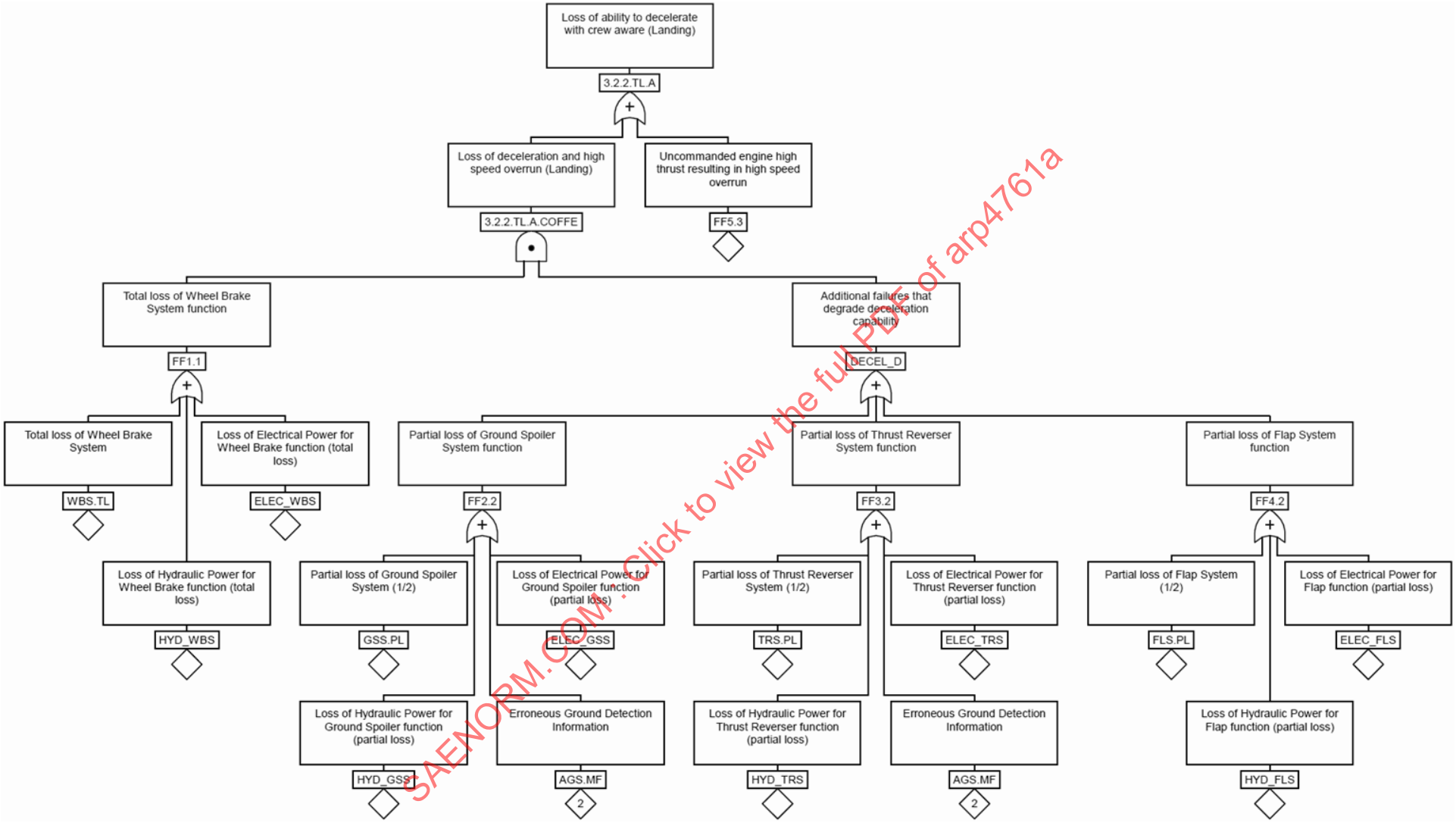
Wheel Brake	Ground Spoiler	Thrust Reverser	Flap	Stopping capability result
F	D	O	O	High-speed overrun
F	O	D	O	High-speed overrun
F	O	O	D	High-speed overrun

Through the CoFFE analysis it can be concluded that “the total loss of wheel brake function in addition to the partial (or total) loss of any ground spoiler or thrust reverser or flap functions” might result in high-speed overruns.

Q.4.4.2 Fault Tree Analysis

Using the CoFFE analysis result, (i.e., the minimal systems functional failures combinations that result in the high-speed overruns), a Fault Tree Analysis (FTA) shown in Figure Q.4-1 is modeled to assess the failure condition identified in the AFHA.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.4-1 - (PASA)
FTA 3.2.2.TL.A

Gates of the FTA 3.2.2.TL.A (Figure Q.4-1) are:

3.2.2.TL.A.CoFFE	Loss of deceleration and high-speed overrun (Landing)
DECEL_D	Additional failures that degrade deceleration capability
FF1.1	Total loss of Wheel Brake System function
FF2.2	Partial loss of Ground Spoiler System function
FF3.2	Partial loss of Thrust Reverser System function
FF4.2	Partial loss of Flap System function

Events of the FTA 3.2.2.TL.A (Figure Q.4-1) are:

FF5.3	Uncommanded engine high thrust resulting in high-speed overrun
WBS.TL	Total loss of Wheel Brake System
GSS.PL	Partial loss of Ground Spoiler System (1/2)
TRS.PL	Partial loss of Thrust Reverser System (1/2)
FLS.PL	Partial loss of Flap System (1/2)
ELEC_WBS	Loss of Electrical Power for Wheel Brake function (total loss)
ELEC_GSS	Loss of Electrical Power for Ground Spoiler function (partial loss)
ELEC_TRS	Loss of Electrical Power for Thrust Reverser function (partial loss)
ELEC_FLS	Loss of Electrical Power for Flap function (partial loss)
HYD_WBS	Loss of Hydraulic Power for Wheel Brake function (total loss)
HYD_GSS	Loss of Hydraulic Power for Ground Spoiler function (partial loss)
HYD_TRS	Loss of hydraulic Power for Thrust Reverser function (partial loss)
HYD_FLS	Loss of Hydraulic Power for Flap function (partial loss)
AGS.MF	Erroneous Ground Detection Information

(Editor´s Note: WBS uses ground detection information together with the wheel speed information. These functions are developed independently so that even if Erroneous Ground Detection Information (AGS.MF) is provided on ground, i.e., with false in-flight status, wheel braking function is available if there is correct wheel speed information.)

(Editor´s Note: The single system branch of the Figure Q.4-1 (FTA), i.e., the FF5.3 "Uncommanded engine high thrust resulting in high-speed overrun" is an undeveloped event in the single system branch of Figure Q.4-1 as already explained for Table Q.4-5 in Q.4.4.1. This event is considered to be a Catastrophic failure condition by itself and is addressed by the propulsion system FHA (Uncommanded high engine thrust).)

The multisystem and multifunction branch of Figure Q.4-1 (3.2.2.TL.A.CoFFE AND-gate of the fault tree, "Loss of deceleration and high-speed overrun during - Landing") shall be extremely improbable and should not result from a single failure [PASA-SO-01].

At an early stage, the PASA determined that the extremely improbable objective of requirement PASA-SO-01 cannot be met with the proposed airplane architecture, where the WBS is supplied by only two hydraulic systems (HYD1 and HYD2) also supplying, even partly, the other systems contributing to the "Decelerate on ground" function (ground spoiler system, thrust reverser system, flap system). With this architecture the loss of two hydraulic systems, which is not extremely improbable, would lead to loss of deceleration and high-speed overrun. The PASA will therefore develop a requirement to address this issue.

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: The PRA in Q.4.4.4.2 identifies a similar need in PRA-UERF-DECEL-01-01-01 that leads to the proposed requirement PASA-SR-12. The development process considered all possible solutions and the design team chose to incorporate a hydraulic accumulator (i.e., emergency accumulator) that is capable of providing sufficient energy to assure safe airplane deceleration by braking the wheels, during all airplane operational modes, including the HYD 1 and HYD 2 loss case.)

The initial probability allocations to these systems functional failures can be made at this stage. Further assessment of all aircraft failure conditions (AFHA) will be required to ensure the final probability allocations to the systems functional failures involved in this PASA example are compatible with allocations made for other AFHA failure cases.

The 3.2.2.TL.A.CoFFE AND-gate is further developed into the FF1.1 and DECEL_D gates. The probabilities are allocated such that the "total loss of wheel brake function in combination with either degraded ground spoilers, degraded thrust reverser or symmetrical partial loss of flap functions" is less than 1.0E-09 for a landing [PASA-FTA-01].

The CoFFE analysis has been performed in the Q.4.4.1 for those correlated functional failures to the failure conditions of the SFHAs. The probability requirements can now be assigned to these systems failure conditions identified in the SFHAs, as follow:

- [FF1.1] Complete loss of wheel brakes shall be less than 1.0E-07 for a landing [PASA-FTA-02]. See CoFFE line 27, where the WBS contributes directly to the Hazardous classification for low-speed overrun.
- [FF2.2] Symmetrical partial loss of ground spoiler (outboard or inboard) shall be less than 1.0E-03 for a landing [PASA-FTA-03].
- [FF3.2] Loss of one thrust reverser (LH or RH) shall be less than 1.0E-03 for a landing [PASA-FTA-04].
- [FF4.2] Symmetrical partial loss of flaps (outboard or inboard) shall be less than 1.0E-03 for a landing [PASA-FTA-05].

The 3.2.2.TL.A.CoFFE AND-gate of the FF1.1 and the DECEL_D covers the failure combination of "total loss of wheel brake function in addition to partial loss of any ground spoiler or thrust reverser or flap functions" resulting in high-speed overrun. The Independence Principles can be established for the following systems functional failures combinations in order to meet no single failure criteria set by safety objective of the AFHA 3.2.2.TL.A failure condition.

- The complete loss of wheel brake function and the partial loss of ground spoiler function does not result from a single failure or event [PASA-INDEP-01].
- The complete loss of wheel brake function and the loss of one thrust reverse function does not result from a single failure or event [PASA-INDEP-02].
- The complete loss of wheel brake function and the partial loss of flap function does not result from single failure or event [PASA-INDEP-03].

These Independence Principles PASA-INDEP-01, PASA-INDEP-02 and PASA-INDEP-03 are inputs to common cause considerations, and also for the Function Development Assurance Level (FDAL) allocation activities.

Q.4.4.3 Common Resource Considerations Analysis

The common resource considerations analysis analyzes the interaction of the common resources within the airplane systems related to decelerate on ground functions, which are identified in the interdependence analysis Table Q.4-2.

These common resources are the hydraulic power, electrical power and ground detection information. The fault tree shown in Figure Q.4-1 includes several undefined events which are common resource system failures. The 3.2.2.TL.A.CoFFE AND-gate shows all combinations of these common resources and other systems failures resulting in high-speed overrun due to loss of declaration capability. Table Q.4-9 shows potential failure combinations, in the format of minimal cut sets.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.4-9 - (PASA)
Potential failures combinations (FT cut set)

Cases	Failure 1	Failure 2
1	HYD_WBS	ELEC_GSS
2	HYD_WBS	ELEC_TRS
3	HYD_WBS	ELEC_FLS
4	HYD_WBS	HYD_GSS
5	HYD_WBS	HYD_TRS
6	HYD_WBS	HYD_FLS
7	HYD_WBS	AGS.MF
8	HYD_WBS	GSS.PL
9	HYD_WBS	TRS.PL
10	HYD_WBS	FLS.PL
11	ELEC_WBS	ELEC_GSS
12	ELEC_WBS	ELEC_TRS
13	ELEC_WBS	ELEC_FLS
14	ELEC_WBS	HYD_GSS
15	ELEC_WBS	HYD_TRS
16	ELEC_WBS	HYD_FLS
17	ELEC_WBS	AGS.MF
18	ELEC_WBS	GSS.PL
19	ELEC_WBS	TRS.PL
20	ELEC_WBS	FLS.PL
21	WBS.TL	ELEC_GSS
22	WBS.TL	ELEC_TRS
23	WBS.TL	ELEC_FLS
24	WBS.TL	HYD_GSS
25	WBS.TL	HYD_TRS
26	WBS.TL	HYD_FLS
27	WBS.TL	AGS.MF
28	WBS.TL	GSS.PL
29	WBS.TL	TRS.PL
30	WBS.TL	FLS.PL

SAENORM.COM : Click to view the full PDF of arp4761a

The airplane architecture for the common resources is proposed in the development process. The PASA process using the Common Cause Methodologies—Common Mode Analysis (CMA), Particular Risk Analysis (PRA), Zonal Safety Analysis (ZSA)—proposes the safety requirements (e.g., independence requirements) to the development process so that the safety objectives can be met.

(Editor´s Note: For the sake of brevity, this example doesn't show the details of this airplane architecture for the common resources, including the common resource mapping to failure conditions.)

Q.4.4.3.1 Hydraulic Common Power Source Analysis

The cases 4 to 6 from Table Q.4-9, address hydraulic common power source failures as listed in Table Q.4-10.

Table Q.4-10 - (PASA)
Hydraulic common power source failures

Cases	Failure 1	Failure 2
4	HYD_WBS	HYD_GSS
5	HYD_WBS	HYD_TRS
6	HYD_WBS	HYD_FLS

Loss of all hydraulic power causes loss of all airplane deceleration capabilities. Trade studies were performed during system development phases and determined that hydraulic drive of all airplane deceleration systems (wheel brake, thrust reverser, ground spoiler and flap) would be more economically feasible with the design requirement identified as S18-ACFT-R-0184 (ARP4754B/ED-79B, Appendix E). This implies that no single failure or event results in the loss of all three hydraulic power systems and it is extremely improbable [PASA-SO-02].

Three redundant hydraulic systems should be distributed to supply the WBS, GSS, TRS, and FLS such that they meet the PASA-SO-02 and also PASA-INDEP-01, PASA-INDEP-02, and PASA-INDEP-03, for each of the cases 4, 5, and 6. These functional independence attributes (Independence Principles PASA-INDEP-01, PASA-INDEP-02, and PASA-INDEP-03) are inputs to the PRA, ZSA, CMA, and Hydraulic System PSSA.

Q.4.4.3.2 Electrical Common Power Source Analysis

The cases 11 to 13 from Table Q.4-9, address electrical common power source failures as listed in Table Q.4-11.

Table Q.4-11 - (PASA)
Electrical common power source failures

Cases	Failure 1	Failure 2
11	ELEC_WBS	ELEC_GSS
12	ELEC_WBS	ELEC_TRS
13	ELEC_WBS	ELEC_FLS

Loss of all electrical power causes loss of all airplane deceleration capabilities. This implies that no single failure or event results in the loss of all electrical power generation and *distribution capabilities and it is extremely improbable [PASA-SO-03]. All electrical power should be distributed to supply the WBS, GSS, TRS and FLS such that they meet PASA-SO-03, and also PASA-INDEP-01, PASA-INDEP-02, and PASA-INDEP-03, for each of the* cases 11, 12, and 13. These functional independence attributes (Independence Principles PASA-INDEP-01, PASA-INDEP-02, and PASA-INDEP-03) are inputs to the PRA, ZSA, CMA, and Electrical System PSSA.

Q.4.4.4 Common Cause Considerations

(Editor´s Note: For the sake of brevity, the cascading effects considerations and external events and survivability considerations are not covered in this PASA example. An example of Cascading Effects Analysis (CEA) is available in Section Q.16, but there is no interface with the scope of this PASA example. Regarding the external events and survivability, no example is provided.)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.4.4.4.1 Common Mode Analysis (CMA)

The cases of Table Q.4-12 are the multisystem and multifunction type combination to be assessed in the CMA as described in Appendix M.

Table Q.4-12 - (PASA)
Multisystem and multifunction type failures combination

Cases	Failure 1	Failure 2
1	HYD_WBS	ELEC_GSS
2	HYD_WBS	ELEC_TRS
3	HYD_WBS	ELEC_FLS
7	HYD_WBS	AGS.MF
8	HYD_WBS	GSS.PL
9	HYD_WBS	TRS.PL
10	HYD_WBS	FLS.PL
14	ELEC_WBS	HYD_GSS
15	ELEC_WBS	HYD_TRS
16	ELEC_WBS	HYD_FLS
17	ELEC_WBS	AGS.MF
18	ELEC_WBS	GSS.PL
19	ELEC_WBS	TRS.PL
20	ELEC_WBS	FLS.PL
21	WBS.TL	ELEC_GSS
22	WBS.TL	ELEC_TRS
23	WBS.TL	ELEC_FLS
24	WBS.TL	HYD_GSS
25	WBS.TL	HYD_TRS
26	WBS.TL	HYD_FLS
27	WBS.TL	AGS.MF
28	WBS.TL	GSS.PL
29	WBS.TL	TRS.PL
30	WBS.TL	FLS.PL

SAENORM.COM : Click to view the full PDF of arp4761a

These cases represent the following Independence Principles:

- The PASA-INDEP-01 implies that the complete loss of wheel brake do not cause partial loss of ground spoiler, and vice versa.
- The PASA-INDEP-02 implies that the complete loss of wheel brake do not cause loss of one thrust reverser, and vice versa.
- The PASA-INDEP-03 implies that the complete loss of wheel brake do not cause partial loss of flap, and vice versa.

For these cases, the CMA questionnaires should be applied for potential common cause failures or error sources. Common cause types assessed for these Independence Principles are: development and design processes, implementation, manufacturing tools and operation to mitigate common specifications (equipment, component, software, hardware, firmware), common requirements, common development process, and common manufacturing (procedure, tools) errors.

(Editor´s Note: There is no aircraft-level CMA example developed in Appendix Q, so there is no reference to it here.)

Q.4.4.4.2 Particular Risk Analysis (PRA)

With those identified Independence Principles PASA-INDEP-01, PASA-INDEP-02 and PASA-INDEP-03, the Particular Risk Analysis (PRA) is performed to examine the proposed airplane design architecture and installation.

Section Q.15 provides a PRA example of Uncontained Engine Rotor Failure (UERF) of the S18 airplane. This analysis is performed with the feedback to the PASA, as described in the Appendix B (PASA) and Appendix L (PRA) processes.

(Editor´s Note: For the sake of brevity, only few proposed safety requirements identified by the PRA of Section Q.15 will be described and discussed herein, just enough to show an example of a clear picture of this process flow among PASA, PRA and development process. There might be other identified proposed safety requirements in the PRA that will not be captured here.)

The proposed airplane architecture for the hydraulic system uses three “redundant” power sources, where only two hydraulic systems HYD1 and HYD2 supply both the WBS (primary deceleration means) and thrust reverser system (secondary deceleration means) for installation convenience.

The UERF PRA analysis shows that the proposed airplane architecture would not satisfy the Independence Principle PASA-INDEP-02 for certain single rotor failure event trajectories causing total loss of wheel braking (due to loss of both HYD1 and HYD2 systems) and thrust reversing capability (due to loss of thrust on failed engine and loss of both HYD1 and HYD2 systems). *(Editor’s Note: The development process considered all possible solutions and the design team chose to incorporate a hydraulic accumulator (i.e., emergency accumulator) that is capable of providing sufficient energy to assure safe airplane deceleration by braking the wheels, during all airplane operational modes, including the HYD 1 and HYD 2 loss case. The PASA confirms that this design solution does not violate the Independence Principle PASA-INDEP-02 since this assures the loss of HYD1 and HYD2 will not result in the complete loss wheel brake function.)*

Considering the design solution chosen, and observing that it had resulted in physical elements common to both the ALTERNATE and EMERGENCY braking modes, the UERF PRA has developed the proposed requirement PRA-UERF-DECEL-01-01-03-01 which specifies that "The Alternate/Emergency Brake System hydraulic equipment and piping shall be installed aft of the Engine 1 UERF trajectory envelope.”

(Editor’s Note: For the sake of simplifying this example, it is assumed that the hydraulic accumulator specified in the WBS provides sufficient energy to permit at least 50% wheel deceleration capability.)

The UERF PRA analysis also shows that the Alternate/Emergency wheel braking modes should have a dual redundant command path (from the pedals to the two metering valves) according to the PRA-UERF-DECEL-01-01-03-02. Also, within the UERF zone, one of the redundant command paths should be routed through the fuselage ceiling area, and the other should be routed such that no Engine 1 UERF trajectory can hit both command paths at same time according to PRA-UERF-DECEL-01-01-03-03.

(Editor’s Note: The development process considered all possible solutions concerning this safety requirement and the design option selected is that the Alternate and Emergency wheel braking modes should have dual redundant command paths (from the pedals to the two metering valves).)

(Editor’s Note: The PRA technique can be used in conjunction with the Multifunction and Multisystem (MF&MS) analysis, with previously identified Independence Principles, to propose safety requirements, i.e., physical installation segregation/separation requirements. This example shows one approach on how proposed safety requirements can be generated in PASA using the PRA techniques. Not all safety requirements from the PRA are described herein but are compiled in Table Q.4-16. Those proposed safety requirements are then used to guide the design implementations which in turn can be used to verify them during the SSA/ASA process.)

Q.4.4.4.3 Zonal Safety Analysis

Many installations analyses were performed during Zonal Safety Analysis (ZSA) of Main Landing Gear Bay for the S18 airplane (Section Q.14), and it has been revealed that flailing shaft of the flap hydraulic motor moving parts could potentially impact the brake pressure valve (Selector Valve), which could violate the Independence Principle [PASA-INDEP-03].

SAENORM.COM : Click to view the full PDF of arp4761a

A safety requirement has been proposed to the development process. Flailing shaft of the flap hydraulic motor moving parts shall not impact on brake pressure valve (Selector Valve), ZSA example (Section Q.14, Table Q.14-17).

Relocation of the flap hydraulic motor to a safe distance from the brake pressure valve was recommended during the interaction between safety and development processes.

(Editor´s Note: For the sake of brevity, only this proposed safety requirement identified by the ZSA of Section Q.14 has been described and discussed herein, just enough to show an example of a clear picture of this process flow among PASA, ZSA and development process. There might be other identified proposed safety requirements in the ZSA that will not be captured here.)

(Editor's Note: The ZSA technique can be used in conjunction with the MF&MS analysis, with previously identified Independence Principles, to propose safety requirements, i.e., physical installation segregation/separation requirements. This example shows one approach on how proposed safety requirements can be generated in PASA using the ZSA techniques. Those proposed safety requirements are then used to guide the design implementation and are used as a basis for verifying the design implementation.)

Q.4.4.5 FDAL Assignment to System Functions

Following the guidance of Appendix P, the airplane functions are assigned development assurance levels that will be applied to the various development processes associated with each function.

Following the steps in Appendix P, the required FDAL for the airplane system function is directly derived from the analysis of the associated AFHA failure condition. Per step a. of Appendix P, the failure condition "Loss of ability to decelerate with crew aware" is selected. This failure condition has been classified as Catastrophic, so that the function "Decelerate on Ground" should be developed as FDAL A as the top-level FDAL per step b.

The Functional Failure Set (FFS) is identified and selected per steps c. and d., and it has multiple members. This FFS is then developed using FT minimal cut sets. The identified minimal equations or terms of the FFSs:

- Wheel Brake System function (F1) and Ground Spoiler System function (F2).
- Wheel Brake System function (F1) and Thrust Reverser System function (F3).
- Wheel Brake System function (F1) and Flap System function (F4).

Per step f., the functional independence claims are validated, which allows the FFS members to be assigned in step h. Since the FFSs are composed of F1 in addition to F2, F3, or F4 functional failures, the F2, F3 and F4 functions can be assigned the same FDAL. Since architectural considerations are planned to be used in the FDAL assignments, the F1 function needs to be functionally independent from the other 3 functions. Based on the assessment of these FFSs and using Figure P3, the FDAL assignment to the systems functions can be developed as shown in Table Q.4-13.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.4-13 - (PASA)
FDAL assignment to system functions

FDAL Assignment to Systems Functions				
Options	**F1 Wheel Brake**	**F2 Ground Spoiler**	**F3 Thrust Reverser**	**F4 Flap**
1	B	B		
2	A	C		
3	C	A		

(*Editor's Note: The option 3 would not be considered for the "Decelerate on Ground" function. This would not be acceptable because the WBS function (F1) is inconsistent with the FDAL C. FDAL A for F1 function to support the Inadvertent Wheel Braking Catastrophic failure condition is required in the WBS PSSA. For the sake of brevity, the inadvertent airplane deceleration failure condition is not analyzed in the PASA.)*

Alternatively, per step g., systems FDAL may also be assigned without taking any architecture consideration credit. Since the top-level FDAL for the function “Decelerate on Ground” should be developed as FDAL A, the affected systems functions should also be assigned as FDAL A as shown in Table Q.4-14.

Table Q.4-14 - (PASA)
FDAL assignment to system functions (option 4)

FDAL Assignment to Systems Functions				
Options	**F1 Wheel Brake**	**F2 Ground Spoiler**	**F3 Thrust Reverser**	**F4 Flap**
4	A	A		

(Editor’s Note: Option 4 would be selected if FDAL A was required for F2, F3, or F4 when assessing any other AFHA failure condition. The option 4 is not selected for this example. Either Options 1 or 2 would be acceptable for this failure condition. Option 2 was selected to assign FDAL A to F1 function to support the Catastrophic Inadvertent Wheel Braking failure condition in the WBS PSSA. For the sake of brevity, the inadvertent airplane deceleration failure condition is not analyzed in the PASA.)

The Option 2 is then selected to make it possible to continue on this example:

- Wheel Brake System function (F1) should be developed FDAL A.
- Ground Spoiler System function (F2) should be developed FDAL C (as minimum).
- Thrust Reverser System function (F3) should be developed FDAL C (as minimum).
- Flap System function (F4) should be developed FDAL C (as minimum).

All other failure conditions (and associated FFS) should be assessed per step i. to confirm a complete review. Once all failure conditions are assessed for the FHA, step j., the FDAL assignments should be reviewed to ensure that all failure conditions are satisfied by the FDAL assignment.

(Editor’s Note: Requirements for functional independence between the wheel brake function and the ground spoiler, thrust reverser and flap functions are not included for brevity.)

Q.4.5 Output

(Editor’s Note: The PASA completion check is then performed to determine that the safety objectives can be satisfied, and any necessary associated system requirements are proposed to the development process. For the sake of brevity, the example does not present all the completion criteria as described in the Appendix B (PASA), Section B.5.)

The output generated by the PASA includes the safety objectives as shown in Table Q.4-15, the proposed requirements as shown in Table Q.4-16, and assumptions as shown in Table Q.4-17.

(Editor’s Note: Any of the output generated within this analysis has to be consistently validated along with other failure condition analysis from the AFHA prior to determine the correct probabilities allocation and FDAL assignments to the systems, so that the most severe condition for a given function should be considered for driving the requirement down to the systems. Also, the PSSA should take the inputs from the PASA and the requirements derived from the SFHA failure condition analysis in order to consider the most severe safety requirements such as FDAL assignment to be allocated to the systems.)

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.4-15 - (PASA)
PASA output (safety objective)

SO#	Safety Objective
PASA-SO-01	3.2.2.TL.A gate “loss of deceleration capability resulting in high-speed overrun” shall be extremely improbable and should not result from a single failure
PASA-SO-02	No single failure or event shall result in the loss of all three hydraulic power systems and it should be extremely improbable
PASA-SO-03	No single failure or event shall result in loss of all electrical power generation and distribution capabilities and it should be extremely improbable

(Editor’s Note: Inadvertent airplane deceleration failure condition from AFHA is not analyzed in this PASA for the sake of brevity. However, this failure condition would normally be assessed in the PASA to support the WBS PSSA. There would be safety objective PASA-SO-XX identified for the “Inadvertent wheel braking” Catastrophic failure condition that should be extremely improbable and should not result from a single failure.)

The following required probabilities, FDAL assignment and the Independence Principles identified in the PASA, become safety requirements after acceptance by the development process, providing early validation of the proposed airplane architecture.

Table Q.4-16 - (PASA)
PASA output (proposed safety requirement)

SR #	Proposed Safety Requirements	Source
PASA-SR-01	[F1] Decelerate wheels function shall be developed FDAL A	PASA-FDAL-01
PASA-SR-02	[F2] Ground spoiler function shall be developed FDAL C (as minimum)	PASA-FDAL-02
PASA-SR-03	[F3] Thrust reverser function shall be developed FDAL C (as minimum)	PASA-FDAL-03
PASA-SR-04	[F4] Flap function shall be developed FDAL C (as minimum)	PASA-FDAL-04
PASA-SR-05	[FF1.1] Complete loss of wheel brake shall be less than 1.0E-07 for a landing.	PASA-FTA-02
PASA-SR-06	[FF2.2] Symmetrical partial loss of ground spoiler shall be less than 1.0E-03 for a landing.	PASA-FTA-03
PASA-SR-07	[FF3.2] Loss of one thrust reverser shall be less than 1.0E-03 for a landing.	PASA-FTA-04
PASA-SR-08	[FF4.2] Symmetrical partial loss of flaps shall be less than 1.0E-03 for a landing.	PASA-FTA-05
PASA-SR-09	No single failure or event shall result in the complete loss of wheel brake and the symmetrical partial loss of ground spoiler.	PASA-INDEP-01
PASA-SR-10	No single failure or event shall result in the complete loss of wheel brake and the loss of one thrust reverser.	PASA-INDEP-02
PASA-SR-11	No single failure or event shall result in the complete loss of wheel brake and the symmetrical partial loss of flap.	PASA-INDEP-03
PASA-SR-12	Loss of power from both hydraulic subsystems powered by the engines shall not lead to complete loss of wheel braking.	PRA-UERF-DECEL-01-01-01
PASA-SR-13	The Alternate/Emergency Brake System hydraulic equipment and piping shall be installed aft of the engine 1 UERF trajectory envelope.	PRA-UERF-DECEL-01-01-03-01
PASA-SR-14	Two redundant control lanes shall be provided between the Electric Brake Unit (EBU) and each of the two Alternate/Emergency Meter Valves.	PRA-UERF-DECEL-01-01-03-02
PASA-SR-15	Two redundant control lanes defined in the proposed requirement [PASA-SR-14] shall use vertically separated routes in the portion of the fuselage crossing the UERF area so that no engine 1 UERF debris can affect both lanes together.	PRA-UERF-DECEL-01-01-03-03
PASA-SR-16	At least one of the two redundant control lanes between the Electric Brake Unit (EBU) and each of the two Alternate/Emergency Meter Valves shall allow control of the corresponding valve until complete stop of the airplane in case of loss of power from both engine driven generators.	PRA-UERF-DECEL-01-01-04-01
PASA-SR-17	The control lane between the Electric Brake Unit (EBU) and each of the two Alternate/Emergency Meter Valves allowing control of the corresponding valve until complete stop of the airplane in case of loss of power from both engine driven generators shall be routed in the cabin ceiling area in the portion of the fuselage crossing the UERF area.	PRA-UERF-DECEL-01-01-03-04
PASA-SR-18	Flailing shaft of the flap hydraulic motor moving parts shall not impact on brake pressure valve.	Appendix Q.14 (ZSA) Table Q.14-17

(Editor´s Note: Further development of the FTA of Figure Q.4-1 should identify interdependencies that lead to a more complete set of safety requirements.)

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.4-17 lists the assumptions output from the PASA process.

Table Q.4-17 - (PASA)
PASA assumption

ASMP #	Assumption
PASA-ASMP-01	It is assumed that the high-speed overrun is above 30 knots and low-speed overrun is below (or equal) 30 knots. This assumption has been derived from the AFHA assumption ASMP 3.2.2-1 and ASMP 3.2.2-6 for the establishment of the criteria and terms of “high-speed overrun” and “low-speed overrun.”
PASA-ASMP-02	The degraded state of systems considered in the CoFFE analysis has been defined such as half functional capability.
PASA-ASMP-03	Wheel Brake System uses ground detection information together with the wheel speed information. These functions are developed independently so that even if Erroneous Ground Detection Information (AGS.MF) is provided on ground, i.e., with false in-flight status, wheel braking function is available if there is correct wheel speed information.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.5 S18 AIRPLANE - WHEEL BRAKE SYSTEM (WBS) SYSTEM FUNCTIONAL HAZARD ASSESSMENT (SFHA) EXAMPLE

SFHA Example

Q.5.1 SFHA Example Introduction

This section contains the system-level functional hazard assessment of the “S18” airplane’s Wheel Brake System (WBS). The WBS system-level functions are considered. The WBS SFHA is developed following the process described in Appendix C.

Q.5.2 Glossary

This section captures specific terms and definitions used within this example.

Term	Definition
Uncommanded	Activation of a function without crew command input or erroneously activated due to equipment failure.
V1	The speed beyond which takeoff should no longer be aborted
VR	The speed at which the pilot begins to apply control inputs to cause the airplane nose to pitch up (rotation), after which the airplane will leave the ground.

Q.5.3 System Description Summary

The primary purpose of the S18 WBS is to control airplane speed through deceleration when on the ground. The S18 airplane WBS performs this function either automatically upon landing or manually upon flight crew activation. In addition to decelerating the airplane, the WBS may be used for controlling direction on the ground through differential braking; stopping the main landing gear wheel rotation upon gear retraction; or prevent airplane motion when parked.

The S18 airplane has two main landing gear struts with four wheels on each strut for a total of eight wheels. Each wheel is equipped with an independent brake.

(Editor’s Note: Other features defining this airplane system would normally be included in this paragraph, but are not described for the sake of brevity.)

Q.5.4 WBS SFHA Development

Q.5.4.1 SFHA Inputs

The S18 system development process identifies the system-level functions presented in Table Q.5-1 for the S18 airplane wheel brake.

Table Q.5-1 - (SFHA - WBS)
WBS function list

1. Decelerate the wheels on the ground
   - 1.1. Decelerate the wheels on command (manual or automatic)
   - 1.2. Automatically command wheel deceleration on landing and Rejected Takeoff (RTO)
   - 1.3. Prevent tire skidding during wheel deceleration
   - 1.4. Provide Wheel Brake System annunciation
2. Decelerate the wheels on gear retraction
3. Decelerate the wheels differentially for directional control
4. Prevent airplane motion when parked
5. Provide wheel speed data to the airplane

SAENORM.COM : Click to view the full PDF of arp4761a

Q.5.4.2 Review and Confirm System-Level Functions

These functions and their breakdown have been reviewed and confirmed to be complete. The review has also confirmed that the functions are described at a consistent level of abstraction, avoiding reference to particular design solutions. Where functional breakdown was provided, the lower-level functions have been confirmed to be necessary and sufficient to accomplish the higher-level function. This list of functions is, therefore, found appropriate for development of the SFHA.

Q.5.4.3 Determine Failure Conditions

(Editor's Note: Failure conditions for the lower-level functions under the "Decelerate the wheels on the ground" function are assessed in this example. Failure conditions for all other WBS functions at the lowest level of the functional breakdown would be assessed in similar fashion.)

Q.5.4.3.1 Failure Condition Identification Matrix

A failure condition identification matrix was constructed for the "Decelerate the wheels on the ground" function. This initial matrix is presented in Table Q.5-2. Postulated failure condition descriptions are captured for total loss of function, automatic command of wheel deceleration function and prevent wheel skid function.

Table Q.5-2 - (SFHA - WBS)
"Decelerate the wheels on the ground" failure condition identification matrix

ID #	System Function	Total Loss	Partial Loss	Malfunction
1	Decelerate the wheels on the ground			
1.1	Decelerate the wheels on command (manual or automatic)	**1.1.TL** Total loss of wheel deceleration (80% or more)	**1.1.PL1** Symmetric loss of 50% to 80% wheel deceleration capability **1.1.PL2** Symmetric loss of less than 50% wheel deceleration capability **1.1.PL3** Asymmetric loss of 50% wheel deceleration capability	**1.1.MF1** Uncommanded full symmetric wheel deceleration **1.1.MF2** Uncommanded partial symmetric wheel deceleration **1.1.MF3** Uncommanded asymmetric wheel deceleration
1.2	Automatically command wheel deceleration	**1.2.TL** Total loss of automatic deceleration command	**1.2.PL1** Symmetric partial loss of automatic deceleration command	**1.2.MF1** Erroneous Early activation of the automatic deceleration command **1.2.MF2** Erroneous Late activation of the automatic deceleration command
1.3	Prevent tire skidding during deceleration	**1.3.TL** All wheels locked	**1.3.PL1** Symmetric partial set of wheels locked **1.3.PL2** Asymmetric partial set of wheels locked **1.3.PL3** Loss of skid protection on all wheels (wheels not locked)	**1.3 MF1** Erroneous early activation of skid prevention **1.3 MF2** Erroneous late activation of skid prevention

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: The unique numbering scheme used in the example has been established to enable readability as well as traceability to later assessment examples. Suffixes for total loss (TL), partial loss (PL), and malfunction (MF) have been appended to differentiate the different function failure condition mechanisms. Other numbering mechanisms may also be used.)

The following rationale was used when populating the Table Q.5-2 failure condition identification matrix:

(Editor's Note: A link to PASA is made to assure that the decomposition from airplane-level failure conditions to system-level failure condition(s) is complete.)

1.1.TL: Total loss of wheel deceleration

This condition describes the total loss of the primary function of the WBS. On the S18 airplane, ground performance simulations have determined that loss of 80% or more of the brake capacity effectively results in total loss of wheel braking.

1.1.PL1: Symmetric loss of 50% to 80% wheel deceleration capability

The applicability of certain regulatory requirements (14 CFR Part 25/CS-25) is based on whether the airplane can be stopped within a distance that is two times the landing distance in normal operating conditions. For this reason, loss of 50% wheel deceleration capability was selected as a reference point for partial loss of deceleration capability.

1.1.PL2: Symmetric loss of less than 50% wheel deceleration capability

Same as noted for 1.1.PL1.

1.1.PL3: Asymmetric loss of 50% wheel deceleration capability

Asymmetric loss of deceleration capability causes a directional control disturbance to be introduced whenever the brakes are applied. The control disturbance may be significant when applying maximum braking.

1.1.MF1: Uncommanded full symmetric wheel deceleration

The "Decelerate the wheels on the ground" function is understood to have time and intensity as relevant parameters. The "Uncommanded full symmetric wheel deceleration" malfunction addresses full activation of the function at an incorrect time. Excessive intensity when commanded is not a significant failure condition. Reduced intensity is addressed in the partial loss of function failure conditions.

1.1.MF2: Uncommanded partial symmetric wheel deceleration

The "Uncommanded partial symmetric wheel deceleration" malfunction addresses partial activation of the function at an incorrect time. Partial symmetric wheel deceleration application occurs when 50% wheel deceleration capability is applied.

1.1.MF3: Uncommanded asymmetric wheel deceleration

Asymmetric deceleration causes a directional control disturbance. The control disturbance may be significant. Asymmetric wheel deceleration occurs when a braking intensity commanded on the left and right struts differs by 50% or more.

(Editor's Note: Only failure conditions associated with system function ID 1.1 of Table Q.5-2 were developed as part of this example for brevity. Development of the other failure conditions would follow the same process and be captured in the FHA failure condition classification tables (Table Q.5-4).)

Q.5.4.3.2 Crew Awareness

The effect of crew awareness on the severity of the failure conditions (FC) has been reviewed. Crew awareness has been determined to be significant to the effects of multiple failure conditions. These conditions have, therefore, been separated into conditions with or without crew awareness as shown in Table Q.5-3.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.5-3 - (SFHA - WBS)
Revised failure conditions considering crew awareness

Revised FC ID	Revised Failure Condition Description
1.1.TL1.A	Total loss of wheel deceleration capability with crew aware
1.1.TL1.U	Total loss of wheel deceleration capability with crew unaware
1.1.PL1.A	Symmetric loss of 50% to 80% wheel deceleration capability with crew aware
1.1.PL1.U	Symmetric loss of 50% to 80% wheel deceleration capability with crew unaware
1.1.PL2.A	Symmetric loss of less than 50% wheel deceleration capability with crew aware
1.1.PL2.U	Symmetric loss of less than 50% wheel deceleration capability with crew unaware
1.1.PL3.A	Asymmetric loss of 50% wheel deceleration capability with crew aware
1.1.PL3.U	Asymmetric loss of 50% wheel deceleration capability with crew unaware
1.2.PL1.A	Symmetric partial loss of automatic deceleration command with crew aware
1.2.PL1.U	Symmetric partial loss of automatic deceleration command with crew unaware
1.3.PL3.A	Loss of skid protection on all wheels (wheels not locked) with crew aware
1.3.PL3.U	Loss of skid protection on all wheels (wheels not locked) with crew unaware

Q.5.4.4 Assess Failure Condition Effects

(Editor's Note: The effects of the failure conditions for the "Decelerate the wheels on command (manual or automatic)" function are partially developed in this example. All other failure conditions would be developed in similar fashion.)

The effects of each of the identified failure conditions on the airplane, flight crew, and occupants other than the flight crew have been assessed. The effects are captured based on their immediate effect on airplane, flight crew, and occupants during the phase of flight being analyzed. This includes immediate effects as well as effects that would occur during subsequent flight phases.

The effects of each failure condition are shown in Column 5 of Table Q.5-4.

Q.5.4.4.1 Flight Phases

Failure condition effects are described for each flight phase. The flight phase indicates the moment when the failure condition occurs. For this assessment, the 5-hour average duration flight has been divided into the following anticipated flight phases:

- Taxi.
- Takeoff.
- Climb.
- Cruise.
- Descent.
- Approach.
- Landing.

(Editor's Note: Operational flight phase divisions (e.g., takeoff before V1, takeoff after V1) are typically included in the flight phase list but have been omitted here for brevity.)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.5.4.4.2 Operational Events

Potential operational events that could independently occur and increase the severity of the failure condition have been reviewed. The following event(s) have been identified as relevant: Rejected Takeoff (RTO).

An RTO, occurring independently and concurrently with the failure condition, can increase the severity of the effects of loss of function and partial loss of function by creating the potential for a runway overrun during the takeoff flight phase. Therefore, the following failure conditions have been added to the SFHA:

Symmetric loss of 50% to 80% wheel deceleration capability in combination with RTO (1.1.PL1.RTO)

Symmetric loss of less than 50% wheel deceleration capability in combination with RTO (1.1.PL2.RTO)

(Editor's Note: These loss combination failure conditions would normally be developed but are omitted in this example for brevity.)

Q.5.4.4.3 Environmental Events

Potential environmental events that could independently occur and increase the severity of the failure condition have been reviewed.

Runway icing was identified as a relevant environmental event. However, icing drastically reduces the expected effectiveness of wheel braking, thus making both the loss and malfunction of wheel braking less significant to the ground performance and controllability of the airplane. For this reason, no new failure conditions were created combining runway icing with the existing failure conditions.

It should be noted that a wet runway is considered a normal operating condition. Therefore, all failure conditions identified in the SFHA were assessed considering the possibility of a wet runway.

Q.5.4.5 Classify Based on Effect Severity

Each failure condition has been classified based on the severity of its effects by applying the qualitative classification criteria provided in AC 25.1309 draft ARSENAL revised/AMC 25.1309, as applicable to this type of airplane.

The classification of each failure condition for each flight phase is shown in Column 5 of Table Q.5-4.

Q.5.4.6 SFHA Assumptions

The following assumptions have been made during the development of this SFHA:

a. Loss of 80% or more of deceleration capability is considered a total loss of the deceleration means (SASP 1.1-1).

b. Failure conditions are assessed on wet runway conditions (SASP 1.1-2).

c. RTO is considered an operational condition caused either by an external event or by a system failure (annunciated or perceived by the flight crew) during takeoff run (SASP 1.1-3).

d. The flight crew will not initiate an RTO due to an annunciated failure of the deceleration function after V1 (SASP 1.1-4).

e. Taxi is performed at groundspeeds below 30 knots (SASP 1.1-5).

f. Overrunning the runway length at or above "XYZ" knots is considered a high-speed overrun (SASP 1.1-6).

g. Overrunning the runway length below "XYZ" knots is considered a low-speed overrun (SASP 1.1-7).

h. Failures of deceleration capability will be detected and annunciated by on-board systems (SASP 1.1-8).

(Editor's Note: "XYZ" speed values would be defined in a normal assessment.)

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: The systems development process will evaluate the validity of the assumptions as part of normal activities.)

(Editor's Note: For brevity, only the SFHA Assumptions for system function ID 1.1 of Table Q.5-2 are developed. An arbitrary naming convention (SASP) is used in this example to identify SFHA assumptions.)

Q.5.4.7 SFHA Outputs

In addition to the list of assumptions, the SFHA output includes the full worksheet with functions, failure conditions, effects, and classifications.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.5-4 - (SFHA - WBS)
S18 wheel brake SFHA (partial; "Decelerate wheels on the ground" function only)

(Editor's Note: The effects for each airplane flight phase (Q.5.4.4.1) have been captured in the example S18 Airplane FHA worksheets in order to present a comprehensive FHA concept. This may not be normal practice in all organizations. The specific effects and classifications shown here are for illustrations purposes and may not reflect real-world situations.)

1	2	3	4	5	6
Function/ ID No.	**Failure Condition**	**Flight Phase**	**Effects**	**Classification**	**References/ Notes**
1.1 Decelerate the wheels on command (manual or automatic)					
1.1.TL1.A	Total loss of wheel deceleration capability (≥80%) with crew aware	Taxi	**Aircraft:** Severely reduced/loss of deceleration capability. **Flight crew:** Aware of the condition, will abort flight operation. Slight increase in workload to avoid collision. **Other occupants:** Inconvenience due to delayed flight.	Minor	SASP 1.1-1 SASP 1.1-2 SASP 1.1-5 SASP 1.1-8
		Takeoff Climb Cruise Descent Approach	**Aircraft:** No immediate effect. Large reduction/loss in deceleration capability. May be unable to land safely at originally planned destination. **Flight crew:** Aware of the condition, crew will execute emergency procedures (e.g., divert to a suitable landing location, minimize landing speed and minimize airplane weight for landing). Excessive crew workload increase due to emergency procedures and performance of an abnormal landing. **Other occupants:** Inconvenience due to diversion. Potential serious or fatal injuries during landing.	Hazardous	SASP 1.1-4
		Landing	**Aircraft:** Severe reduction/loss of deceleration capability. Severely reduced deceleration capability results in overrun below "XYZ" knots when maximum reverse thrust is applied. **Flight crew:** Aware of the condition prior to landing, crew will alter landing profile for minimum speed and use maximum thrust reverse capabilities to slow the airplane. If condition awareness occurs during landing, may slightly reduce time to application of maximum reverse thrust in attempt to avoid obstacle collision during runway length overrun. Excessive workload to attempt to avoid obstacle collision during a potential low-speed overrun. **Other occupants:** Potential serious or fatal injuries to small number of passengers or cabin crew in the event of low-speed collision with obstacles or terrain.	Hazardous	SASP 1.1-1 SASP 1.1-2 SASP 1.1-7

SAENORM.COM : Click to view the full PDF of arp4761a

1 Function/ ID No.	2 Failure Condition	3 Flight Phase	4 Effects	5 Classification	6 References/ Notes
1.1 Decelerate the wheels on command (manual or automatic)					
1.1.TL1.U	Total loss of wheel deceleration capability (≥80%) with crew unaware	Taxi	**Aircraft:** Severe reduction/loss deceleration capability. Reduction of functional capability during taxi. **Flight crew:** Crew is unaware of the condition until attempting to decelerate. Crew may be unable to fully stop the airplane resulting in low taxi speed collision or taxiway overrun. Slight increase in crew workload to avoid these conditions. **Other occupants:** Potential injury to unrestrained cabin crew in case of collision.	Major	SASP 1.1-1 SASP 1.1-2 SASP 1.1-5
		Takeoff Climb Cruise Descent Approach	**Aircraft:** Severe reduction/loss of deceleration capability when needed in landing phase. **Flight Crew:** No immediate effect. Crew is unaware of the condition and will proceed with normal flight operation until landing. **Other occupants:** No immediate effect. Potential serious or fatal injuries upon landing	Hazardous	
		Landing	**Aircraft:** Severe reduction/loss of deceleration capability. Severely reduced deceleration capability results in overrun below “XYZ” knots when maximum reverse thrust is applied. **Flight crew:** Crew is unaware of the condition and will proceed with normal flight operation until landing. Excessive crew workload to apply maximum reverse thrust in attempt to avoid obstacle collision during low-speed runway length overrun. **Other occupants:** Potential serious or fatal injuries to small number of passengers or cabin crew in the event of low-speed collision with obstacles or terrain.	Hazardous	SASP 1.1-1 SASP 1.1-2 SASP 1.1-7

SAENORM.COM : Click to view the full PDF of arp4761a

1 Function/ ID No.	2 Failure Condition	3 Flight Phase	4 Effects	5 Classification	6 References/ Notes
1.1 Decelerate the wheels on command (manual or automatic)					
1.1.MF1	Uncommanded full (≥ 80%) symmetric wheel deceleration	Taxi	**Aircraft:** Partial or total application of uncommanded deceleration may cause the airplane to be incapable of continuing taxi. **Flight crew:** Crew will abort taxi operation. **Other occupants:** Inconvenience due to missed flight.	Minor	SASP 1.1-2 SASP 1.1-5
		Takeoff	**Aircraft:** Total deceleration capability applied. Uncommanded deceleration above V1 may prevent successful takeoff and result in overrun above “XYZ” knots. **Flight crew:** Crew may be unaware of uncommanded brake application. Uncommanded deceleration application prior to airplane achieving V1 will be observed by crew and successful rejected takeoff will be achieved. Uncommanded deceleration application after airplane achieves V1 will result in airplane not achieving VR. Crew unable to takeoff and will be unable to stop with runway length resulting in an overrun. **Other occupants:** Potential multiple fatal injuries in the event of collision with obstacles or terrain.	Catastrophic	SASP 1.1-6
		Climb Cruise Descent Approach	**Aircraft:** No immediate effect. Partial or total uncommanded deceleration is latent until landing phase. **Flight Crew:** No immediate effect. Crew will observe condition upon landing. **Other occupants:** No immediate effect. Discomfort upon landing.	Minor	
		Landing	**Aircraft:** Partial or total uncommanded deceleration on touch down or during the landing roll. Landing roll may be abbreviated. Airplane may be incapable of taxi-in. Tire burst may occur. **Flight crew:** Crew will observe the condition and continue the landing rollout normally. **Other occupants:** Discomfort due to sudden deceleration characteristics.		SASP 1.1-2

SAENORM.COM : Click to view the full PDF of arp4761a

Q.6 S18 AIRPLANE - WBS PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA) EXAMPLE

PSSA Example

Q.6.1 PSSA Example Introduction

This section provides an example of how to accomplish the PSSA process objectives, not the development of a PSSA document.

The example contains references to documentation that a company may use to assure itself of the safety of its products. Some of these documents are submitted to the regulatory agencies for the purpose of certification (e.g., the Wheel Brake System FHA). Other documents are internal to the company and not required for certification. No implication is made that these documents should all be submitted to a regulatory agency and none should be implied. This example shows the systems engineering process as applied to the development on an airplane, including those processes that go beyond certification requirements.

(Editor's Note: For the sake of brevity, only one failure condition from the SFHA example has been selected to be developed in detail for this Wheel Brake System (WBS) PSSA example. This provides enough complexity to allow use of all methodologies, yet it is simple enough to present a clear picture of the process. An additional failure condition is partially developed to highlight particular aspects of Fault Tree Analysis (FTA) development. Other failure conditions would be assessed by the same method shown here.)

(Editor's Note: To facilitate the interaction between the system development process example in ARP4754B/ED-79B, Appendix E and the safety process example in this appendix, the safety and system development teams are considered separate teams for illustrative purposes only. However, this example is not intended to imply that these activities are independent or a specific organizational structure.)

Q.6.2 WBS PSSA Activities - Initial

(Editor's Note: After the hand-off of the initial architecture to the safety process, the safety team evaluates the architecture against the SFHA and requirements resulting from the PASA. This initial evaluation is generally not formally documented but the results are passed to the design process if architectural changes are necessary for safety. Each of these process steps would be completed for each iteration of architecture evaluation.)

The safety team works with the system development team to evaluate the initial proposed architecture against the WBS safety requirements and to further define the WBS architecture.

Q.6.2.1 PSSA Inputs

The first step in the WBS example PSSA process is to gather the inputs necessary to support the PSSA process.

(Editor's Note: The inputs captured in the following sub-sections are not intended to be documented in a PSSA document but are provided here to ensure proper context for the PSSA process activities shown in this example.)

Q.6.2.1.1 SFHA Failure Conditions

The following failure conditions (FC) and classifications from the WBS SFHA are provided as inputs to the WBS PSSA process.

(Editor's Note: Due to the size of the WBS SFHA, not all of the SFHA is included here. The PSSA example only lists a sample of the failure conditions included in Section Q.5. Table Q.6-1 is not intended to prescribe the format of capturing the information in an actual PSSA document.)

(Editor's Note: For the sake of simplifying the PSSA example, since both SFHA ID No. 1.1.TL1.A and 1.1.TL1.U (excluding taxi phase) have the same classifications [see Table Q.5-4], this example will only refer to one FC ID number and it will be 1.1.TL [and it should be considered as the "superset" of SFHA ID No. 1.1.TL1.A and 1.1.TL1.U].)

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.6-1 - (PSSA - WBS)
SFHA failure conditions and classifications

FC ID Number	Failure Condition	Flight Phase	Classification
1.1.TL	Total loss of wheel deceleration (80% or more) [independent of “crew aware” or “crew unaware”]	Taxi	
		Takeoff	
		Climb	
		Cruise	
		Descent	
		Approach	Hazardous
		Landing	Hazardous
1.1.MF1	Uncommanded full symmetric wheel deceleration	Taxi	
		Takeoff	Catastrophic
		Climb	
		Cruise	
		Descent	
		Approach	
		Landing	
….			

Q.6.2.1.2 Requirements

Q.6.2.1.2.1 Allocated Safety Requirements from Development Process

The set of safety requirements in Table Q.6-2 are provided as inputs to the PSSA from the development process. These requirements, specific to the WBS, originate from the PASA, but are passed to the PSSA process via the development process as described in ARP4754B/ED-79B, Appendix E.

Table Q.6-2 - (PSSA - WBS)
Allocated requirements from safety process

ID	Output Description	App E Source
S18-WBS-R-0150	Complete loss of the decelerate the wheels on the ground function shall be less probable than 1.0E-07 for a landing.	Table E11
S18-WBS-R-0100	The Wheel Brake System decelerate the wheels on the ground function shall be developed as FDAL A.	Table E11

Q.6.2.1.2.2 Architecture Requirements

Some architectural elements are input to the WBS based on initial program specification of the S18 airplane.

Architectural elements include:

a. Two hydraulic systems.

b. Two electrical power sources.

c. Two sets of pilot brake pedals.

d. Braking applied to eight wheels.

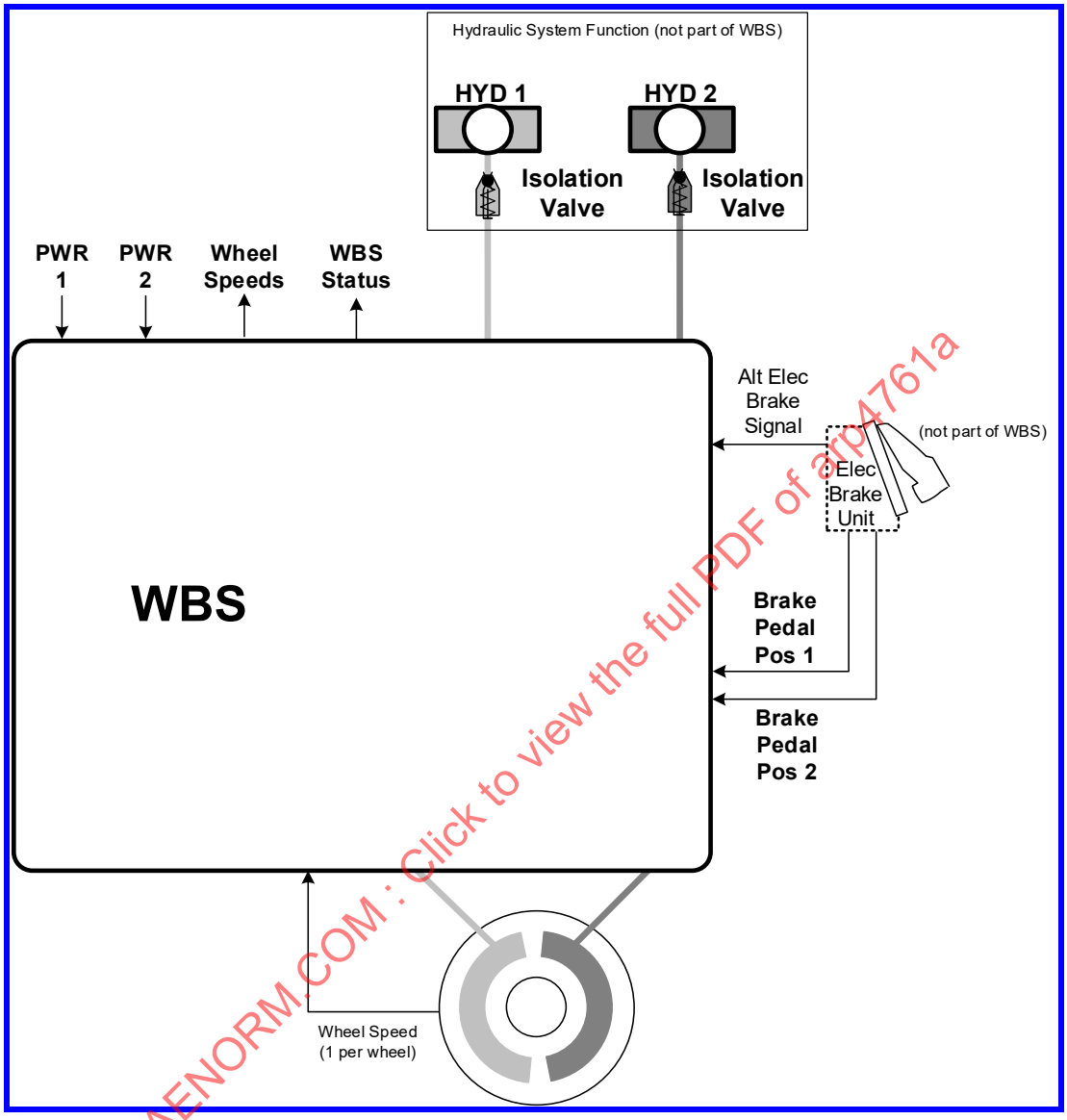
e. Accumulator to provide pressure in event of loss of the hydraulic system.

f. Parking brake (not shown in diagram since not used in the example).

g. System status output.

SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-1 shows the conceptual representation of the WBS. The WBS is further developed in Figure Q.6-3 and represents the initial architecture to be evaluated in the PSSA. This architecture reflects some initial system development activity such as a control unit called a Brake System Control Unit (BSCU).



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-1 - (PSSA - WBS)
WBS initial architecture

(Editor's Note: The descriptions in Figure Q.6-2 apply to the hydraulic control portions of the diagrams shown in this example. Open/Closed defined as valve allows flow when Open.)

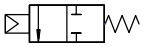
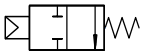
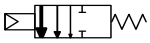
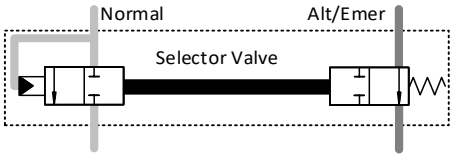
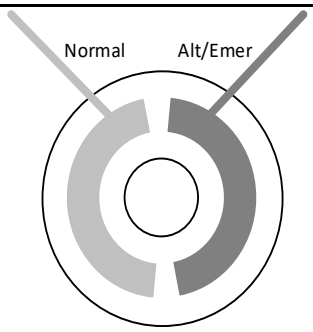
Legend	
Electro-Hydraulic Component	**Description**
	Normally closed valve; open when signal drives input.
	Normally open valve; closed when signal drives input.
	Normally closed valve; open when signal drives input. Opens with increasing flow rate with increasing signal.
	Selector Valve normally closed for Normal, open for Alt/Emer; opens for Normal, closes for Alt/Emer when pressure is applied from Normal side. In the example, the spring-loaded Selector Valve automatically opens Alt/Emer if Normal pressure falls below a threshold or is shut off via the Shutoff Valve.
	Wheel brakes, either input (Normal or Alt/Emer) provides hydraulic pressure to apply 100% of braking.

Figure Q.6-2 - (PSSA - WBS)
Electro-hydraulic equipment descriptions

Q.6.2.1.2.3 Operational Requirements

The S18 airplane program has established some operating characteristics based on customer interface during the initial market research. This information was used to create an operational profile for the airplane and is passed from the airplane level to all systems for use in safety assessments.

The operational profile for the WBS safety assessment includes:

a. An average flight duration of 5 hours.

b. An airplane life of 100000 flight hours.

c. A power on time of 100 operating hours.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.6.2.1.3 Proposed WBS Architecture

(Editor's Note: The system development process (ARP4754B/ED-79B) has provided the following system description information. More details on the system architecture would be contained in systems documentation and in this example, some are presented in ARP4754B/ED-79B.)

The S18 Wheel Brake System (WBS) is comprised of the pedal brake control system, brake hydraulic system, anti-skid and autobrake systems, brakes/wheels/tires, brake temperature monitor system, brake cooling fans, tire pressure indication system, and tire and brake monitoring system.

(Editor's Note: For brevity, the example will only show certain aspects of the systems architecture in detail.)

The airplane has two main landing gear attached to the wings and a nose gear. The Wheel Brake System is installed on the two main landing gear. The nose gear wheels are unbraked. The eight main gear wheels have multi-disc carbon brakes.

Braking on the main gear wheels is used to provide safe retardation of the airplane during taxiing and landing phases, and in the event of a rejected takeoff. The wheel brakes also prevent unintended airplane motion when parked, and may be used to provide differential braking for airplane directional control. A secondary function of the WBS is to stop main gear wheel rotation upon gear retraction.

Braking on ground is commanded manually via brake pedals, or automatically (autobrake) without the need for pedal application. The Autobrake functionality allows the pilot to pre-arm the decelerate function prior to takeoff or landing and is only available in the NORMAL Mode.

Brake application is controlled by left and right meter valves located in the wheel wells. The meter valves are operated via electrical signals, through the Electric Brake Unit, from toe pedals integral to the rudder pedal assembly. Differential control of the left and right brakes is available to both the captain and first officer. The parking brake handle is used to set the parking brake. To set the parking brake, the brake pedals must be fully depressed. The parking brake handle can be pulled up and will latch when the pedals are released. The WBS maintains brake clamping force without further flight crew action once the parking brake has been set. The brake pedals must be depressed to unlatch the parking brake handle.

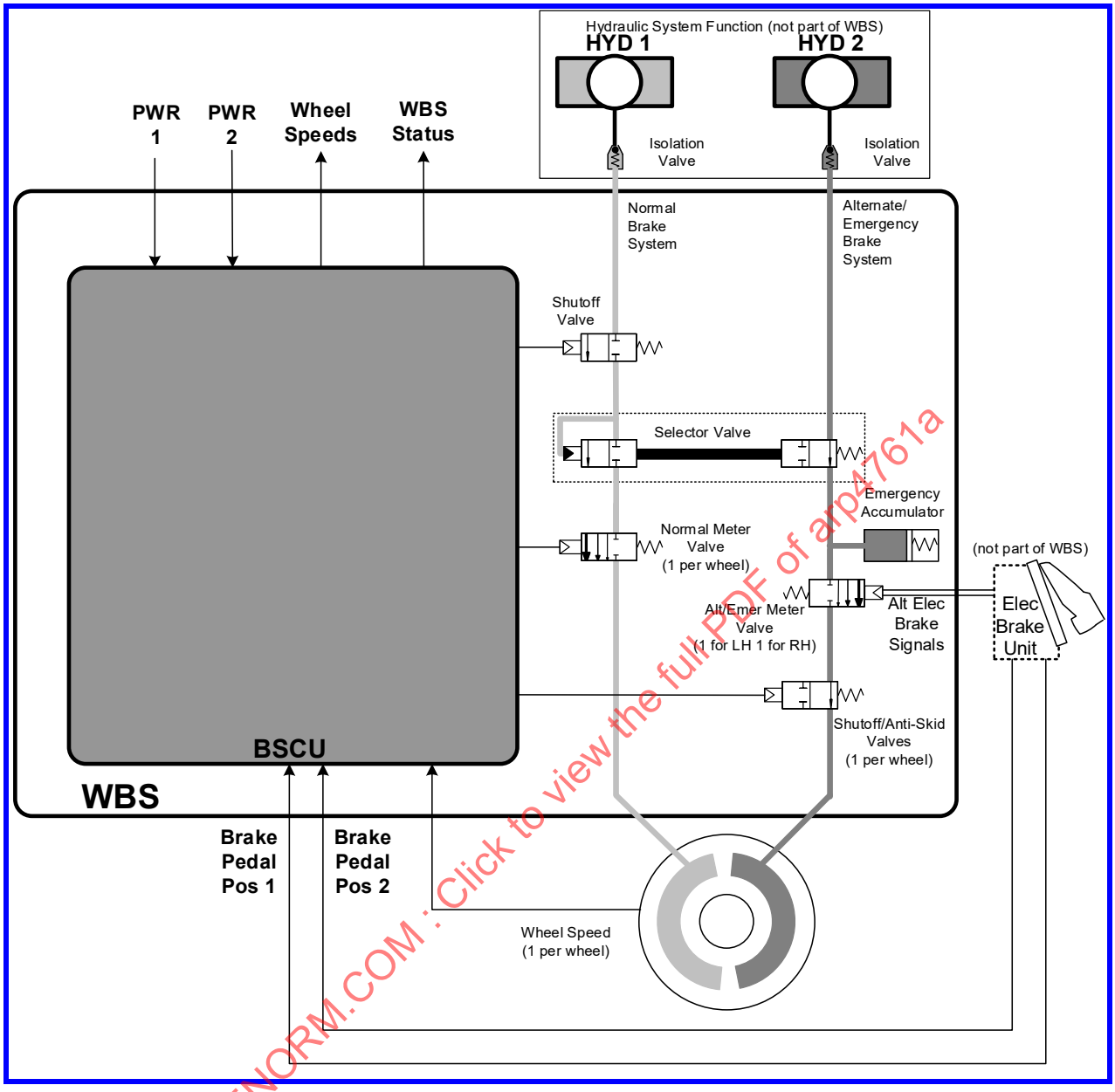
The brake pedal position is also electrically fed to a brake computer. This in turn produces corresponding control signals to the brakes. In addition, this computer monitors various signals which denote certain critical airplane and system states, to provide correct brake functions and improve system fault tolerance, and generate warnings, indications and maintenance information to other systems. This computer is accordingly named the Brake System Control Unit.

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: This WBS PSSA example only focuses on the function "Decelerate the wheels on the ground", failure condition "Total loss of wheel deceleration capability.")

Initial architectural discussions between Systems Development and Systems Safety determined that the proposed architecture would require two command functions. This determination was due to the qualitative understanding that a single processing channel cannot meet the probability requirements associated with a Hazardous failure condition, assuming no numerical safety credit is taken for EMERGENCY Mode within the PSSA fault tree.

A design decision was made at the airplane level with input from the WBS supplier to provide one BSCU containing two command channels. In support of the trade study, the safety process confirmed that a single BSCU implementation was expected to meet safety objectives and requirements. This WBS Architecture is shown in Figure Q.6-3, where the only change to the architecture occurred at the BSCU level, and this figure was used throughout the WBS PSSA process/activities.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-3 - (PSSA - WBS)
WBS revised architecture

The system interfaces are as follows (not all are shown in Figure Q.6-3 for clarity):

- Electrical power system.
- Hydraulics.
- Pilot flight deck controls.
- Flight deck displays.
- Landing Gear Actuator System
- Proximity Sensing (WOW).

- Propulsion.
- Earth Reference System (ground speed).
- Health management system

The WBS includes a Normal Brake System and Alternate/Emergency Brake System which operate in NORMAL, ALTERNATE, and EMERGENCY Mode.

a. NORMAL Mode is operated with BSCU and HYD 1 hydraulic system. NORMAL Mode includes either autobrake or manual braking. Autobrake is only available in the NORMAL Mode.

b. ALTERNATE Mode is on standby and is selected automatically when the Normal Brake System fails, it is operated with HYD 2 hydraulic system.

c. EMERGENCY Mode is selected when the Normal Brake System has failed and HYD 2 hydraulic system is lost. It is operated with an emergency hydraulic accumulator.

The mode transitions for the WBS are shown in Figure Q.6-4.

SAENORM.COM : Click to view the full PDF of arp4761a

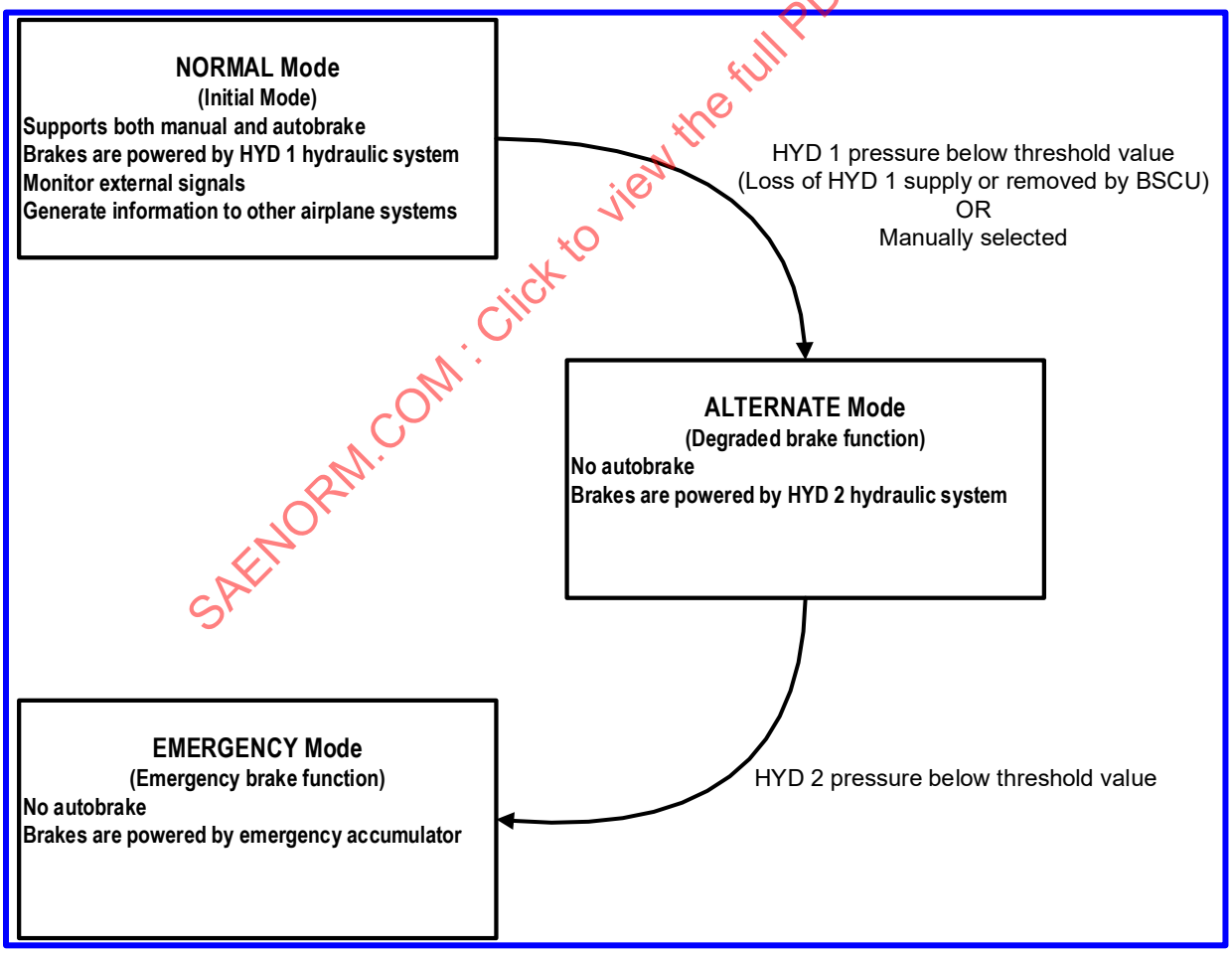


Figure Q.6-4 - (PSSA - WBS)
WBS mode transitions

Now that a proposed high-level architecture has been established, it is analyzed against the system-level functions, operational and safety requirements, and any design constraints that have been identified thus far.

Q.6.2.2 Functional Mapping

The list of functions from the SFHA includes:

1. Decelerate the wheels on the ground.

    1.1. Decelerate the wheels on command (manual or automatic).

    1.2. Automatically command wheel deceleration on landing and RTO.

    1.3. Prevent tire skidding during wheel deceleration.

    1.4. Provide WBS annunciation.

2. Decelerate the wheels on gear retraction.

3. Decelerate the wheels differentially for directional control.

4. Prevent airplane motion when parked.

5. Provide wheel speed data to the airplane.

(Editor's Note: This example will evaluate the functional mapping for the "1.1 Decelerate the wheels on command (manual or automatic)" to support the evaluation of the failure condition: "1.1.TL Total loss of wheel deceleration (80% or more)" shown in Figure Q.6-5. The functional mapping diagram forms the basis for the PSSA fault tree structure. In a complete PSSA process, the contributors to all functions would be evaluated.)

(Editor's Note: This example will evaluate only certain aspects of the system architecture in detail. For simplicity of this example, NORMAL Mode will be analyzed only from the "manual" perspective, thus assuming that manual mode is the recommended braking mode. The autobrake portion of the NORMAL Mode architecture will not be examined and thus this example will not address the following proposed design features: (a) the ability of the flight crew to pre-arm the decelerate function prior to takeoff or landing via inputs pilot controls, (b) the ability of the flight crew to override the autobrake when commanded by the flight crew.)

SAENORM.COM : Click to view the full PDF of arp4761a

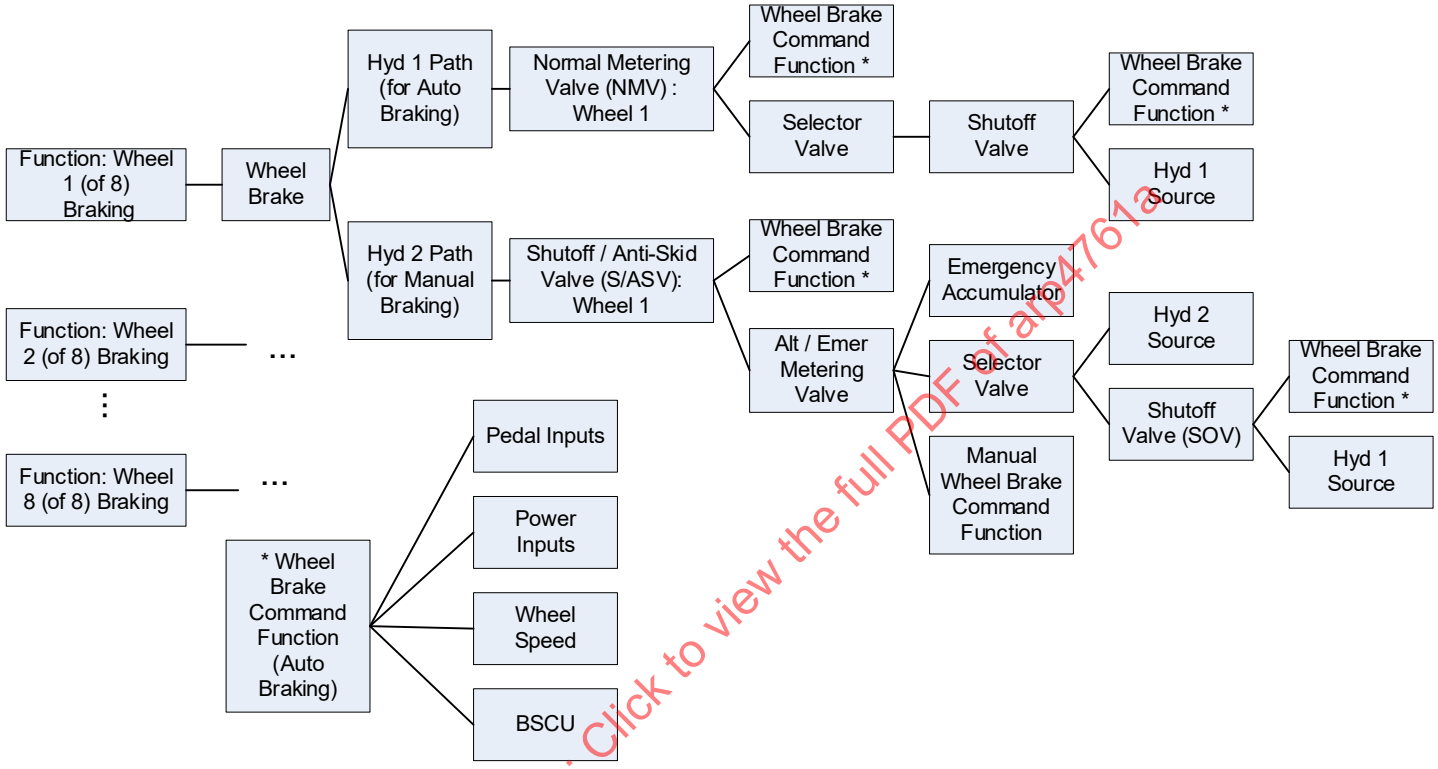
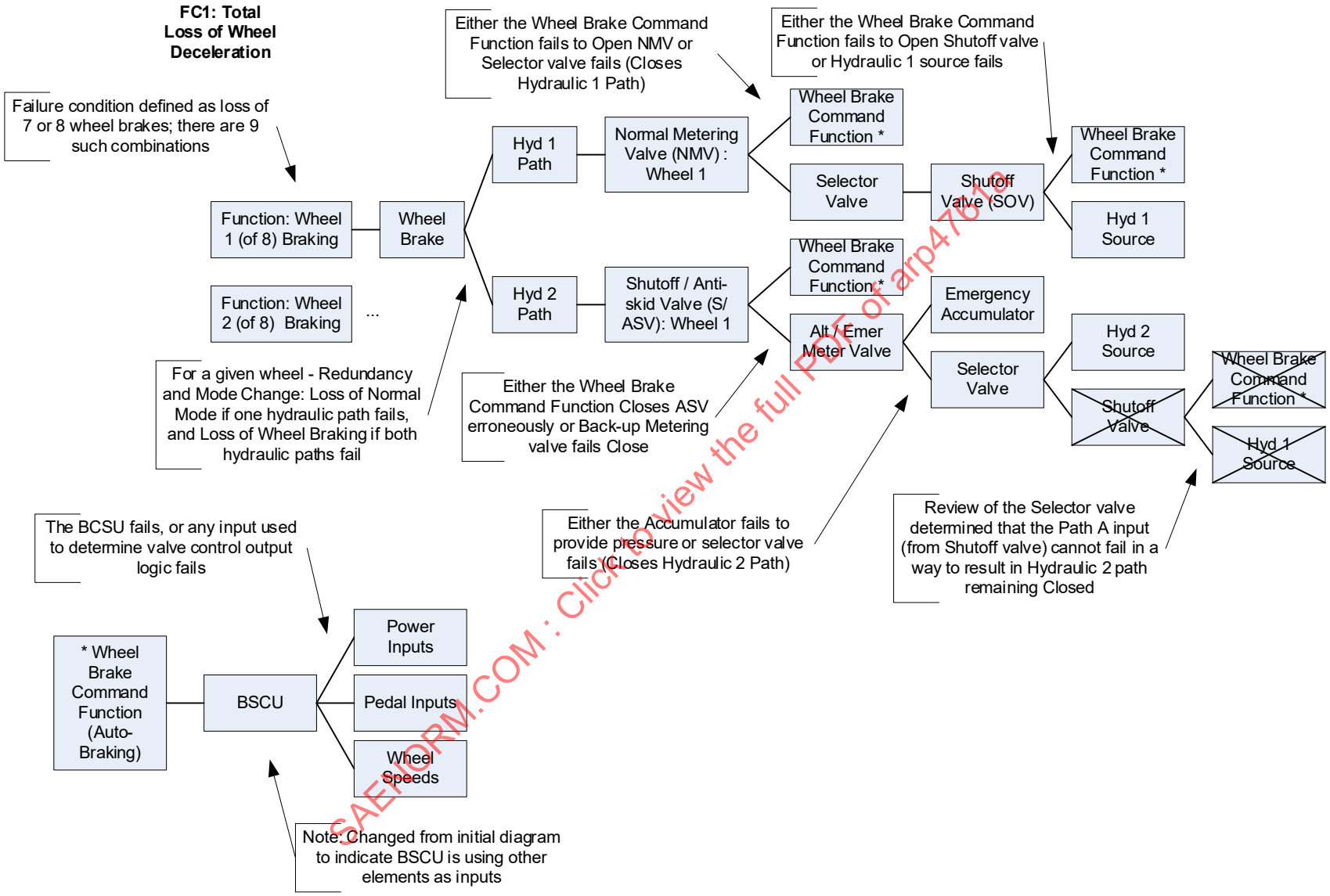


Figure Q.6-5 - (PSSA - WBS)
Conceptual representation of thought process for Failure Condition Functional Mapping

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-6 - (PSSA - WBS)
Detailed Functional Failure Condition Mapping for "Loss of wheel braking"

The following description details the mitigation strategies related to the proposed architecture such as redundancy and monitoring.

Braking on ground is commanded manually, via brake pedals, or automatically (autobrake) without the need for pedal application. The autobrake functionality allows the pilot to pre-arm the deceleration function prior to takeoff or landing and is only available in NORMAL Mode.

Based on the requirement (S18-ACFT-R-1385) that loss of all wheel braking is less probable than 1.0E-07 for a landing, a design decision was made that each wheel has a brake assembly operated by two independent sets of hydraulic pistons. One set is operated from the HYD 1 hydraulic supply and is used in the NORMAL Mode. The Alternate/Emergency system is on standby and is selected automatically when the Normal Brake System fails. It is operated independently using the HYD 2 hydraulic power supply and is backed by an emergency accumulator which is also used to drive the parking brake. The emergency accumulator supplies the Alternate/Emergency Brake System in the EMERGENCY Mode, when the HYD 2 supply is lost and the NORMAL Mode is not available. Switch-over is automatic under various failure conditions, or can be manually selected. Reduction of HYD 1 pressure below a threshold value, either from loss of HYD 1 supply itself or from its removal by the BSCU due to the presence of faults, causes an automatic selector valve to connect the HYD 2 supply to the Alternate/Emergency Brake System. An anti-skid function is available in both the Normal and Alternate/Emergency Brake Systems, and operates at all speeds greater than 2 meters per second.

In the Normal Brake System, all eight wheels are individually braked from their own servo valves, which are also used to apply anti-skid. In the Alternate/Emergency Brake System, a dual meter valve provides a low pressure hydraulic braking input via four servo valves which provide the anti-skid function to four pairs of wheels. Operation of the Alternate/Emergency Brake System is precluded when the Normal Brake System is in use to maintain independence between the two systems.

In the NORMAL Mode, the brake pedal position is electrically fed to the BSCU. This in turn produces corresponding control signals to the brakes. In addition, the BSCU monitors various signals which denote certain critical airplane and system states, to provide proper brake system functionality and improve fault tolerance, and generates warnings, indications, and maintenance information to other systems.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.6.2.3 PSSA Failure Condition Evaluation

The WBS PSSA process begins as soon as the systems development team has an initial architecture concept. This initial evaluation of the architecture against the system FHA (repeated in Table Q.6-3), and requirements passed from the development process will help in determining if the selected architecture can be expected to meet the safety objectives.

Table Q.6-3 - (PSSA - WBS)
Evaluated SFHA Failure Conditions

FC ID Number	Failure Condition	Flight Phase	Classification	Planned Analysis Method
1.1.TL	Total loss of wheel deceleration (80% or more)	Landing	Hazardous	FTA and qualitative
1.1.MF1	Uncommanded full symmetric wheel deceleration	Takeoff	Catastrophic	FTA and qualitative
…	…	…	…	

(Editor's Note: During planning stages, it is useful to consider the planned methods to be used to analyze the failure conditions as recommended in D.3.c. For convenience, this is shown in Table Q.6-3.)

(Editor's Note: Failure conditions that are not being evaluated in this example were not included in Table Q.6-3 for clarity. The full list is in the SFHA.)

A proposed high-level architecture has been established as shown in Figure Q.6-3. This architecture (including system description, interfaces and system requirements) is analyzed to determine if it can reasonably be expected to meet the safety objectives.

Once the architecture is selected the requirements development process may initiate additional safety requirements that could potentially result in further iteration of the architecture to meet the safety objectives. This architecture will continue to be analyzed and has the potential to change until the requirements are validated.

Q.6.2.3.1 Function Development Assurance Level Assignment

The Function Development Assurance Level (FDAL) is passed from the development process as follows:

S18-WBS-R-0100 - The Wheel Brake System decelerate the wheels on the ground function shall be developed as FDAL A.

The WBS FDAL is allocated to the functions of the WBS by analyzing the functional decomposition (see Q.6.2.2) and the system architecture. All failure conditions associated with each WBS function are addressed when assigning the FDAL to the function.

(Editor's Note: FDAL is only assigned to the WBS Control function in this example. If a complete PSSA were to be developed then each sub-function of the WBS would have an FDAL assigned.)

Q.6.2.3.1.1 FDAL Assignment for Braking System Control Function

The WBS braking command function is allocated to a single BSCU within the WBS architecture. Development errors within the WBS Control function could lead to failure conditions classified as Catastrophic. There are no functionally independent means outside of the WBS braking command function that would prevent the allocated Catastrophic failure conditions, therefore, the WBS braking command function is assigned an FDAL of A.

Q.6.2.3.1.2 Item Development Assurance Level (IDAL) Assignment

There are no software or complex hardware items defined at this level. IDAL assignment will be shown at the BSCU level of the PSSA.

Q.6.2.3.2 WBS Fault Tree Analysis

(Editor's Note: Alternative methods of analysis to FTA exist that could be used here. These include Dependence Diagrams, Markov Analysis, and Model-Based Safety Analysis.)

(Editor's Note: All FTAs shown in Appendix Q use the Unavailability method as this is the more widely known and applied method. Alternatively, the Failure Frequency method could have been used, as described in Appendix G.)

The FTA shown in Figure Q.6-7 reflects the top-level requirement of the WBS and depicts the braking subsystems and budgets for the loss of function of each subsystem. The FTA evaluates the failure condition on a "per flight" basis, while the probability for a Hazardous failure condition in the FHA (1.0E-07) is on a "per hour of flight" basis. So, in the FTA the "per flight" probability requirement for a Hazardous failure condition is 5.0E-07 per flight. Since the FTA determines a probability of 2.72E-07 per flight, the requirement is expected to be met.

The NORMAL Mode braking system is composed of both Manual and Automatic modes. No credit is taken for the Automatic mode as to do so would yield negligible quantitative benefit due to the similarity with Normal Manual Mode. This is represented by setting P=1. Similarly, no credit is taken for EMERGENCY Mode. ALTERNATE Mode is modeled within the FTA.

(Editor's Note: Though no credit is taken for Automatic and EMERGENCY Modes, a PSSA would normally develop these branches in order to develop safety requirements unique to these modes of operation.)

SAENORM.COM : Click to view the full PDF of arp4761a

Manual Normal Model is developed under sub tree [WBS-NML-MANUAL-LOSS] using architecture drawing Figure Q.6-3 and functional mapping Figure Q.6-6 as a guide for how to assemble the fault tree structure. Allocated probabilities are assigned to failures of the hydraulic system [WBS-HYD1-LOSS], a Shutoff Valve [WBS-SOV-LOSS], and to the Selector Valve [WBS-SELVALVE-HYD1-LOSS]. Failures of any of these would result in loss of NORMAL Mode braking.

If the SOV were to fail in the closed position [WBS-SOV-LOSS], it would prevent the application of hydraulic pressure represented by the next higher-level gate [WBS-SOV-CLOSURE]. Failure of the actual valve is assigned a probability of 5.0E-06, but the BSCU could also fail to command the SOV to open when required. The BSCU [WBS-BSCU-SOV-LOSS] is assigned a probability of 2.0E-04 for this failure mode. The loss of both electrical power inputs to the BSCU would also result in loss of output from the BSCU. At this point it is not fully understood how power inputs to the BSCU will be managed, so the FTA models loss of both power inputs, assuming independence.

(Editor's Note: It is important that the FTA model for power inputs be revisited to account for any potential common cause failures between the power sources. It may not be possible to have a common cause failure between power buses that would allow the Hazardous numerical objective to be met.)

The application of hydraulic pressure to a given wheel brake is controlled through one additional valve—a Normal Meter Valve (NMV). For an 80% loss of braking at least seven of the eight NMVs would have to fail [WBS-MULTNMV-LOSS], or the associated wheel caliper assemblies. For simplicity, the FTA models the failure of multiple NMVs as a single undeveloped basic event [WBS-GT7NMV-LOSS]. The NMVs are dependent upon a valid braking command from the BSCU [WBS-BSCU-NMV-CMDOUT-LOSS].

There are two different failure modes represented for the BSCU output. The first is the loss of the braking command function from the BSCU. The second failure mode is the output of an erroneous (insufficient) braking command to the NMV, which would effectively also result in a loss of function. Each of these basic events is assigned a probability of 2.0E-04, a maximum allocated budget for the BSCU that still enables the top-level probability to be met. Inputs required for the BSCU are the pedal position inputs, for metering valve position and power supply. The individual wheel speed sensors are also a required input to the BSCU. As with the NMVs, at least seven sensors are required to fail in order to facilitate losing > 80% normal braking. These are modeled within a single basic event.

ALTERNATE Mode is modeled in the FTA in a similar manner to NORMAL Mode. Allocated probabilities are assigned to failures of the hydraulic system (HYD 2), to the Selector Valve and to each of the Alternate/Emergency Meter Valves. In ALTERNATE Mode, the Shutoff/Anti-Skid Valve (S/ASV) should be in the normally open state unless there exists a skid condition. However, failure of the S/ASV, wheel speed sensors, or an erroneous command from the BSCU could result in the loss of ALTERNATE Mode [WBS-BSCU-ASVCLOSE-LOSS].

(Editor's Note: ALTERNATE Mode and NORMAL Mode share common cause failures as both are dependent upon the BSCU and the Selector Valve. The BSCU could fail in such a manner that it prevents hydraulic flow from HYD 1 via the SOV, and prevents hydraulic flow of HYD 2 via the S/ASV. This would result in loss of all braking. Similarly, the Selector Valve may have a common cause that results in failure of both HYD1 and HYD2. These common causes are not developed, but this example illustrates other common cause considerations.)

(Editor's Note: The failure rates are assumed to be constant in fault trees. Should a component/piece-part be subject to a wear out failure mode within its useful life, a CCMR task would be identified to drive a maintenance action allowing the constant failure rate assumption to remain valid. A Weibull Analysis is one method to define the required maintenance interval for wear out failures.)

(Editor's Note: The normal FTA modeling of wire failures or hydraulic piping failures has been intentionally omitted to reduce the size of the example FTAs.)

(Editor's Note: The FTA basic event convention used in this example use the "worst-case" calculation as shown in Figure G23.)

(Editor's Note: Failure rates shown for loss of function are the full hardware failure rates. This is conservative by incorporating the contributions for all failure modes, including erroneous operation.)

SAENORM.COM : Click to view the full PDF of arp4761a

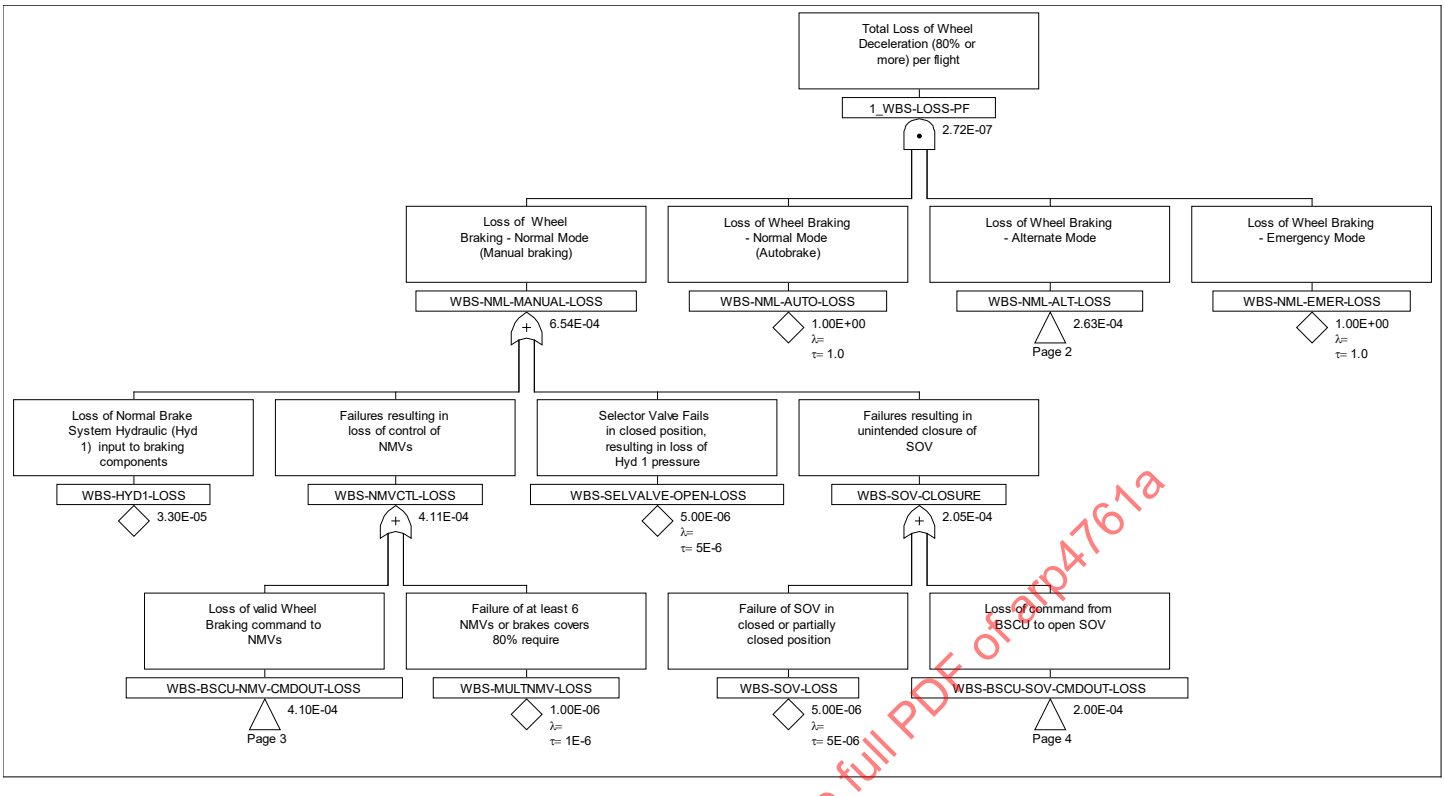
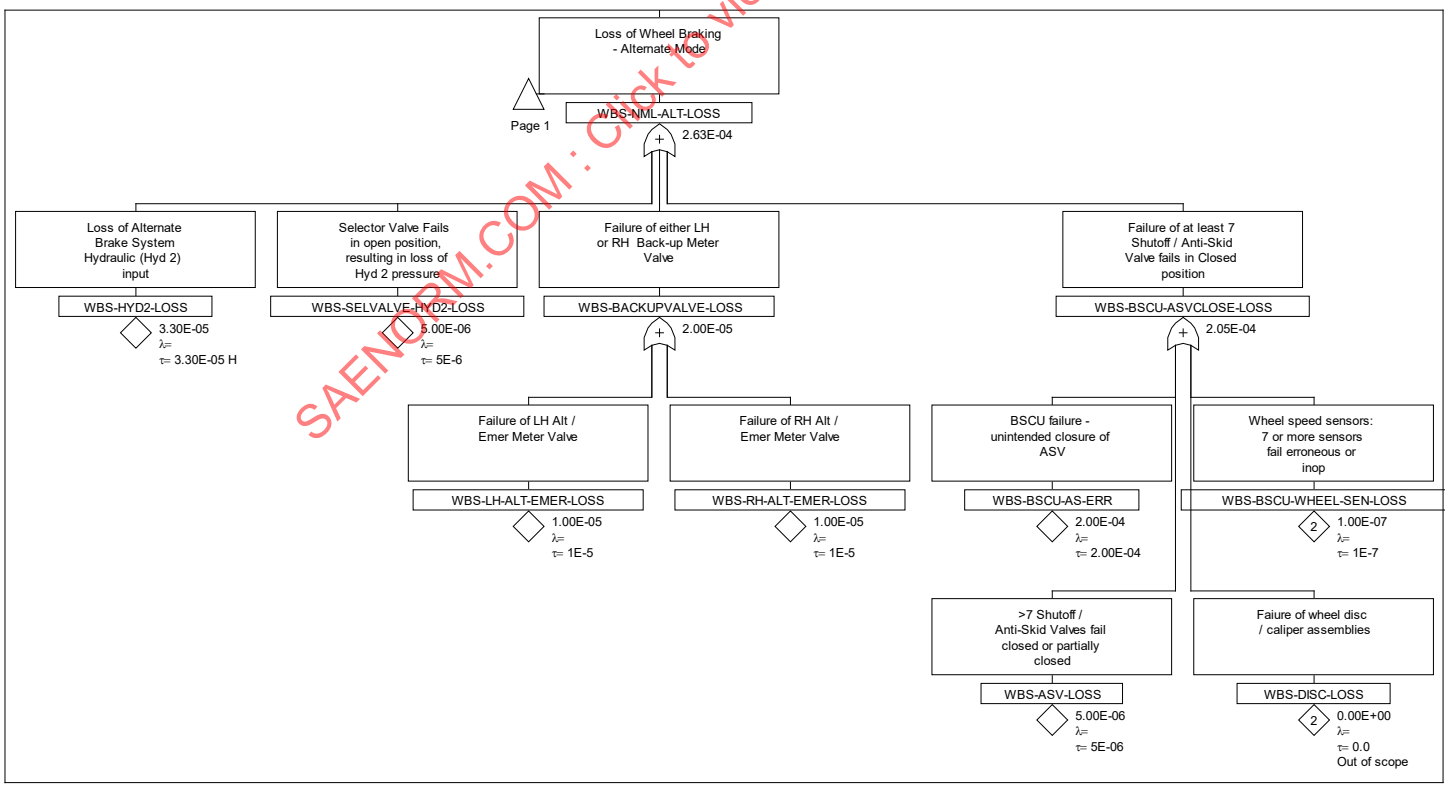


Figure Q.6-7 - (PSSA - WBS FTA)
Total loss of wheel deceleration on command FTA (page 1)



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-8 - (PSSA - WBS FTA)
Total loss of wheel deceleration on command FTA (page 2)

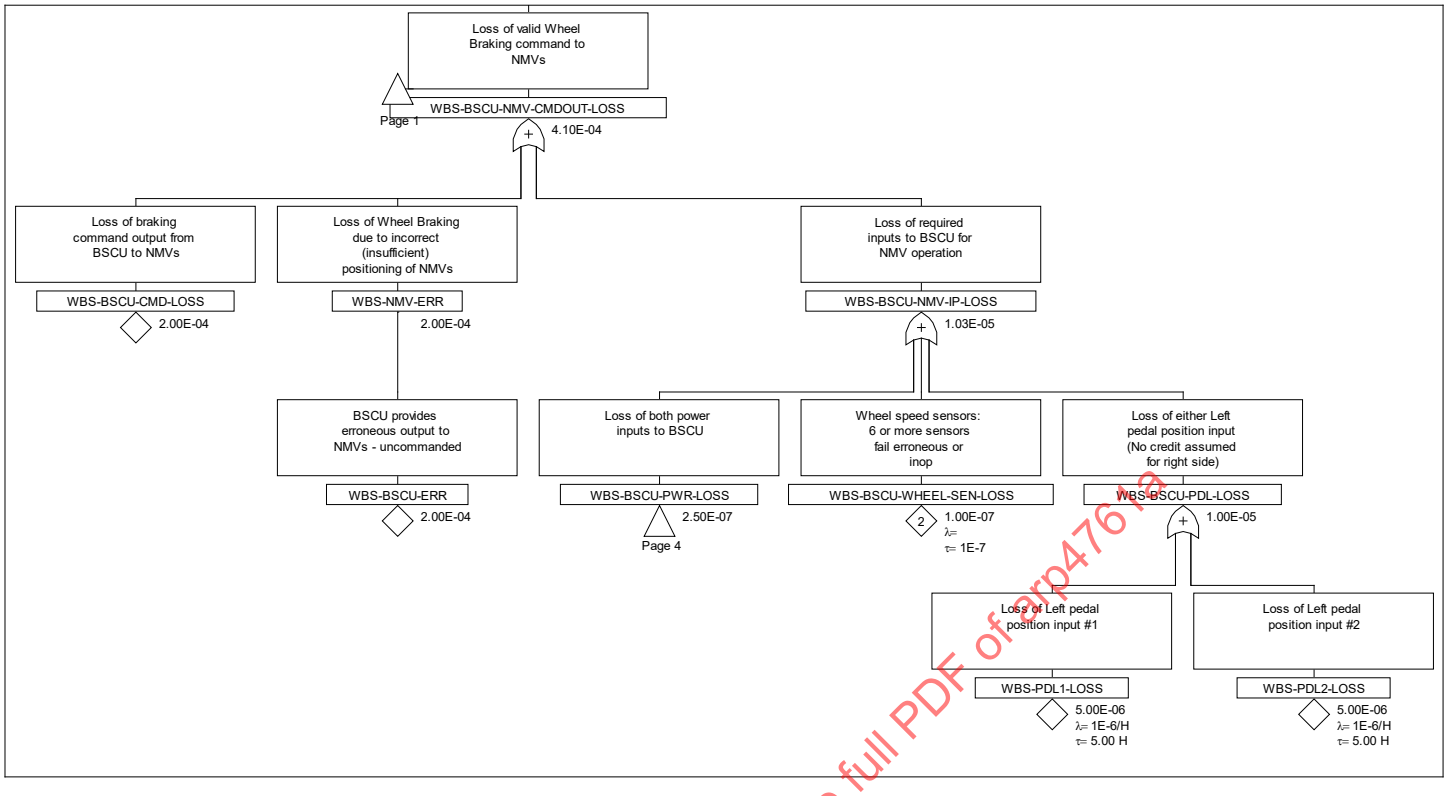


Figure Q.6-9 - (PSSA - WBS FTA)
Total loss of wheel deceleration on command FTA (page 3)

SAENORM.COM : Click to view the full PDF of arp4761a

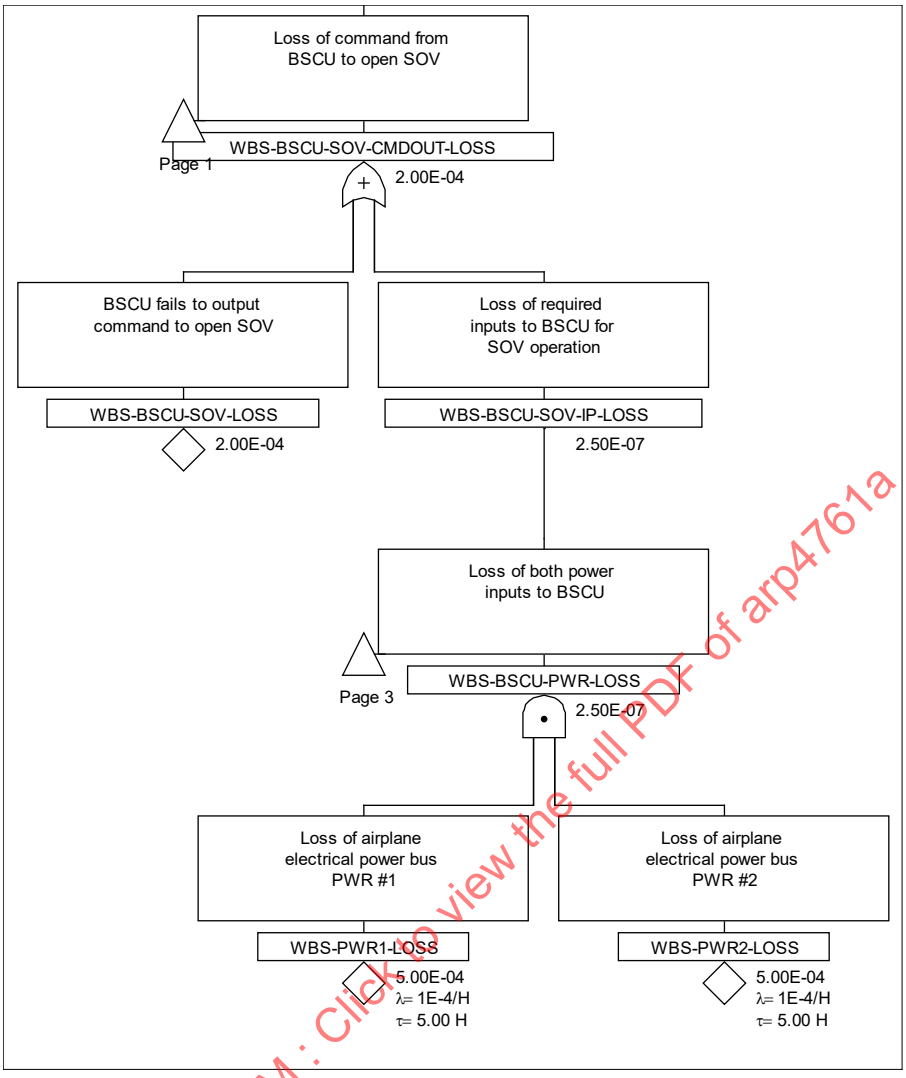


Figure Q.6-10 - (PSSA - WBS FTA)
Total loss of wheel deceleration on command FTA (page 4)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.6.2.3.3 Identify Latent Failures

(Editor's Note: No latent failures were identified for the fault tree as far as it was developed in this example. However, had the fault trees been completely developed, latent events may have been identified. The concept of latent events is discussed in Q.6.4.3.3.)

Q.6.2.3.4 Identify Where Independence is Necessary

As stated by D.4.2.2 the Independence Principles may be identified using various methods; two commonly used methods are described in the following sub-sections.

Since all FDALs are assigned to the level indicated by the failure condition classification, there are no Independence Principles needed to support FDAL assignment.

(Editor's Note: In Q.6.2.3.4.1, FTA is used to identify the Independence Principles to support the "Total loss of wheel deceleration" failure condition. In Q.6.2.3.4.2, design analysis is used to illustrate the identification of Independence Principles to support the "Uncommanded full symmetric wheel deceleration" failure condition.)

Q.6.2.3.4.1 Identification of Independence Principles by Fault Tree Analysis

The fault tree AND-gates are qualitatively evaluated to determine the Independence Principles (i.e., identify where independence is necessary). After evaluating the AND-gates in the FTA for failures, the following design elements were identified as Independence Principles:

- NORMAL Mode braking function independent from ALTERNATE Mode braking function, for total loss failure condition (Figure Q.6-7).

- Airplane electrical power bus 1 independent from airplane electrical power bus 2 (Figure Q.6-9).

For example, the need for airplane electrical power bus 1 and airplane electrical power bus 2 to be independent assures that in the event of either bus failing, the SOV and NMV commands will continue to be provided. The FTA inherently takes credit for this, which can be verified through review of its structure.

(Editor's Note: The following requirements were determined from evaluation of the SFHA failure conditions 1.1.MF1 and 1.1.MF3 for which fault trees are not shown in this example. These requirements are provided in accordance with ARP4754B/ED-79B to the BSCU and result from the "no single point failure" associated with Catastrophic failure conditions. They are included here to illustrate Independence Principles in the BSCU PSSA.

- *Uncommanded wheel braking of all wheels during takeoff roll shall not result from a single command or event.*

- *Uncommanded wheel braking on one wheel w/o locking during takeoff shall not result from a single command or event).*

(Editor's Note: Some single failures covered by 14 CFR/CS §25.735(b)(1) are excepted, as identified in the requirements of 14 CFR/CS §25.1309(b). However, for illustration purposes single failures are considered as part of this example.)

Q.6.2.3.4.2 Identification of Independence Principles by Design Analysis

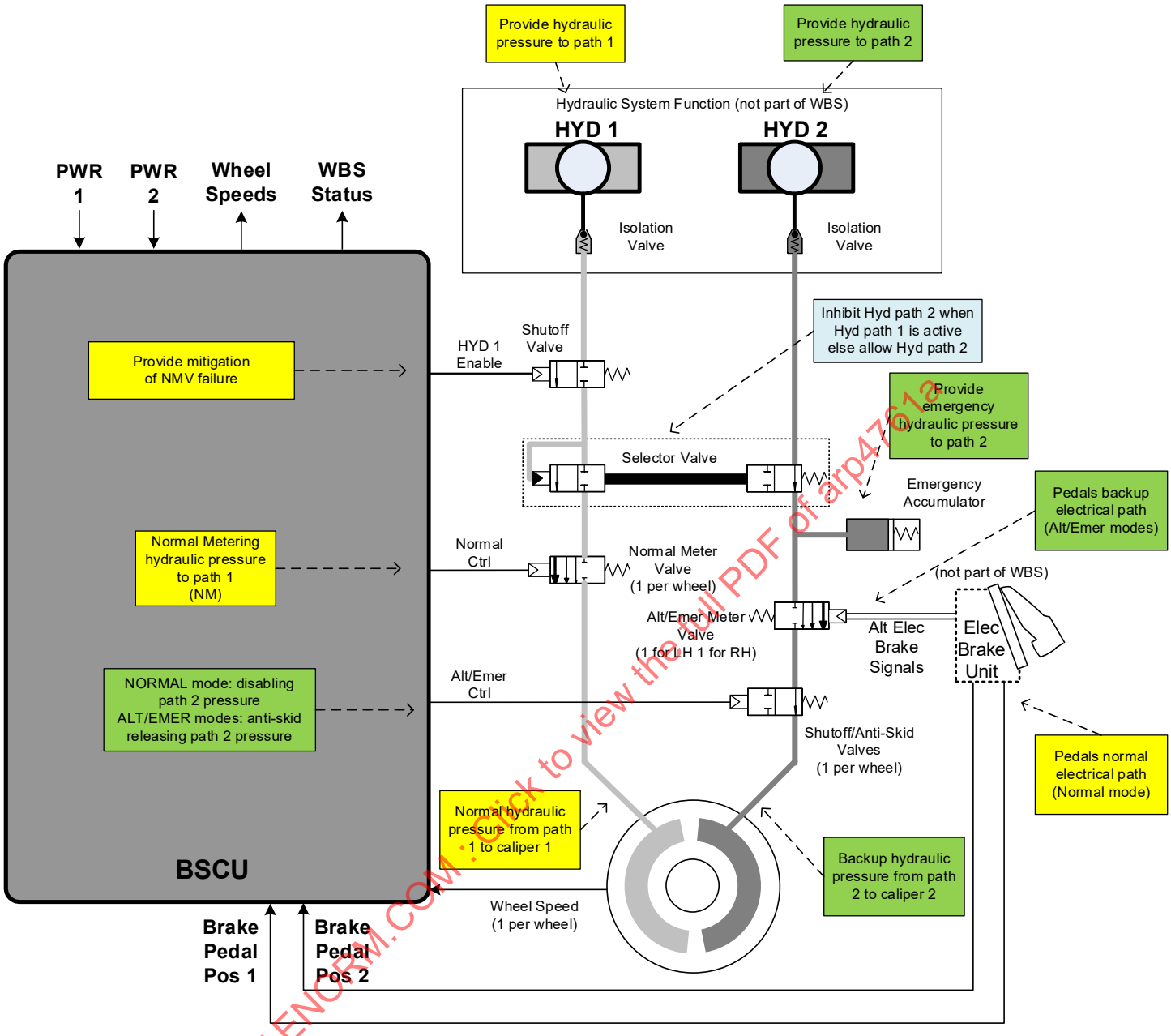
(Editor's Note: This section is showing an example of how to identify Independence Principles by design analysis. The failure condition chosen for this section is "Uncommanded full symmetric wheel deceleration" (classified as Catastrophic). Since some architectural features specifically to address the "Uncommanded full symmetric wheel deceleration" failure condition were not shown in detail previously in this example, some architecture discussion appears here that doesn't appear in ARP4754B/ED-79B, Appendix E example.)

(Editor's Note: This example shows the identification of Independence Principles for failures only and does not include FDAL/IDAL assignment for "Uncommanded full symmetric wheel deceleration.")

(Editor's Note: The figures in this section are a conceptual representation of the thought process for identification of Independence Principles by design analysis.)

The starting point for this discussion is the proposed architecture shown in Figure Q.6-3. This representation is adapted in Figure Q.6-11 to illustrate the design analysis concept.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-11 - (PSSA - WBS)
WBS - architecture: identify the main function of the equipment

The examination of the design shown in Figure Q.6-11 shows that:

a. To brake the wheel there are two braking mechanisms (calipers) on each wheel which are actuated by a separate hydraulic path.

b. There are two separate hydraulic paths:

   1. The “NORMAL Mode” path (HYD1) named “path 1.”

   2. The “ALTERNATE Mode” path (HYD2), named “path 2,” having two modes: ALTERNATE and EMERGENCY.

Using Figure Q.6-11, the functional failures that may result in “Uncommanded full symmetric wheel deceleration” can be identified along with mitigations for those failures.

(Editor's Note: For the sake of brevity, since each hydraulic path has the capability to apply an "Uncommanded full symmetric wheel deceleration," specific independence needs will only be developed for path 1.)

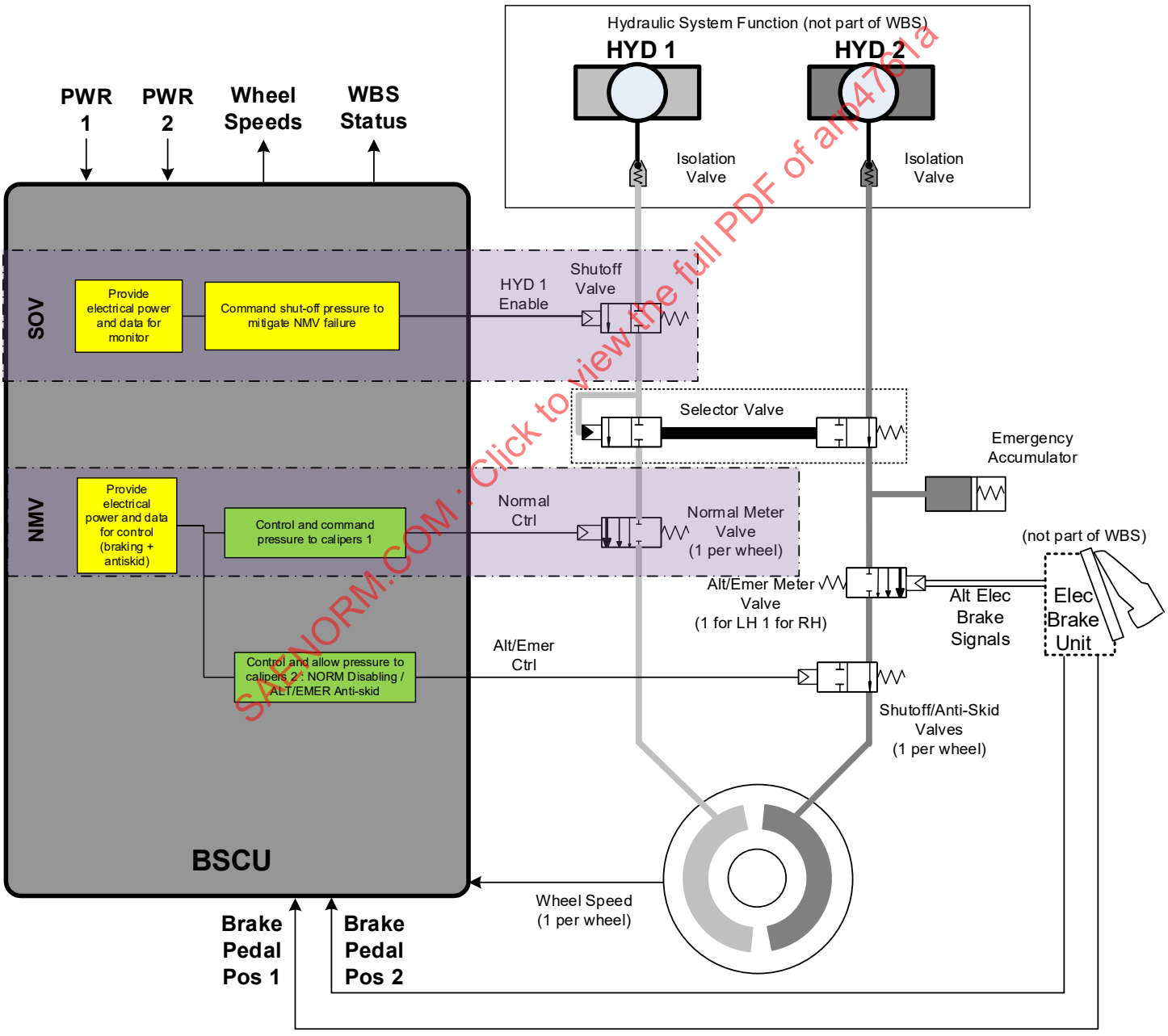
For path 1, uncommanded full symmetric wheel deceleration would result if both of the following events occurred:

a. The Normal Meter Valves (NMV) inadvertently open, increasing hydraulic pressure.

b. The Shutoff Valve (SOV) does not open, preventing fluid flow (which would cause the system to revert to path 2).

Functional representations of the failures that result in (a) "NMV," and (b) "SOV" are shown in Figure Q.6-12. Based on analysis of this functional representation we generate the following Independence Principle:

The NMVs and their control shall be independent from the SOV and its control.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-12 - (PSSA - WBS)
Independence Principle mapped on WBS architecture drawing

Q.6.2.3.5 Identify Proposed Safety Requirements

(Editor's Note: From this point forward, no further consideration of the Independence Principles for Uncommanded Full Symmetric Wheel Deceleration is shown.)

(Editor's Note: The PSSA would normally use a CMA checklist against which to evaluate each of the Independence Principles and generate independence requirements. An example of this process is shown at the BSCU level of this example, but is omitted here for brevity.)

Table Q.6-4 shows how the independence needs from the WBS FTA are correlated to requirements within the development process, along with the resulting proposed independence requirements that should be passed to the BSCU. The safety independence needs are passed to the development process, where they are reviewed with safety and WBS requirements are generated. These requirements are used by the safety process to generate proposed requirements for the BSCU.

(Editor's Note: Requirements shown are only those specific to the failure conditions discussed within this example.)

Table Q.6-4 - (PSSA - WBS)
Proposed independence requirements

Independence Need	Development Process Correlation	Resulting Proposed Requirement for BSCU
Airplane electrical power 1 independent from airplane electrical power 2 (from WBS FTA).	S18-WBS-R-0130 (No single failure or event shall cause the complete loss of electric power for both the Wheel Brake System Normal and Alternate systems).	The SOV and NMV commands shall be provided by the BSCU upon loss of either airplane electrical power input.
NORMAL Mode braking function independent from ALTERNATE Mode braking function, for total loss failure condition (from WBS FTA).	S18-WBS-R-0120 (No single failure or event shall cause the complete loss of hydraulic power for both the Wheel Brake System Normal and Alternate systems).	When "HYD1 Enable" output is enabled, then "Alt/Emer Ctrl" output shall be disabled. When "HYD1 Enable" output is disabled, then "Alt/Emer Ctrl" output shall be enabled.
The NMVs and their control are independent from the SOV and its control such that no single failure results in uncommanded braking (from design analysis).	S18-WBS-R-0326 (No single failure shall result in inadvertent wheel braking of all wheels during takeoff roll).	No single failure shall cause erroneous NMV command and inhibit the SOV function.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.6-5 shows additional proposed safety requirements that were identified during the WBS PSSA process

(Editor's Note: Proposed requirements 2, 3, 4 and 5 are sourced from the associated fault tree. Other requirements would result from other fault trees and these might also result in changes to these proposed requirements.)

Table Q.6-5 - (PSSA - WBS)
Proposed safety requirements, not related to independence

Ref #	Resulting Proposed Requirement	Rationale
1	The wheel brake command function of the BSCU shall be developed to FDAL A	See Section Q.6.2.3.1
2	The probability of BSCU failure resulting in loss of a valid braking command output to the NMV shall not exceed 2.0E-04 per flight.	Fault tree for FC 1.1.TL, U.E. WBS-BSCU-CMD-LOSS
3	The probability of BSCU failure resulting in unannunciated erroneous braking command to the NMV shall not exceed 2.0E-04 per flight.	Fault tree for FC 1.1.TL, U.E. WBS-BSCU-ERR
4	The probability of BSCU failure resulting in the loss of command to open the SOV shall not exceed 2.0E-04 per flight.	Fault tree for FC 1.1.TL, U.E. WBS-BSCU-SOV-LOSS
5	The probability of BSCU failure resulting in unintended closure of the S/ASV shall not exceed 2.0E-04 per flight.	Fault tree for FC 1.1.TL, U.E. WBS-BSCU-AS-ERR

(Editor's Note: In this example a probability requirement is passed from the WBS to the BSCU. The requirement could also have been passed as a failure rate, though if this method is chosen, it should be clear what exposure time is associated with the failure event.)

(Editor's Note: The rationale with specific safety analysis need were captured in the safety assessment data to support the proposed safety requirement.)

Q.6.2.4 PSSA Completion

(Editor's Note: The WBS is integrated with other systems and subsystems. These other subsystems can be at lower levels, in which case the requirements will be passed up to the WBS as assumptions. A thorough assessment of the associated functional failure conditions is performed during the PSSA process to gain an accurate understanding of the contribution each subsystem function lends to the WBS functional failures assessed during the WBS FHA, and resultant failure condition classifications. These details (such as classifications and FDAL/IDAL) are passed back through their respective subsystem-level safety assessment processes. The WBS PSSA process is not complete until all sub-level PSSA processes are complete and evaluated for impact to the overall WBS PSSA.)

(Editor's Note: The following questions are stated in Appendix D, and together determine if the architecture can be reasonably expected to meet the safety objectives. These questions and answers are stated here to illustrate the associated thought process, but do not need to be captured in PSSA documentation.)

The proposed WBS architecture is evaluated using the following PSSA completion checks. The analysis attributes considered are discussed in Section D.5.

a. The quantitative analyses in Q.6.2.3.2 show that the proposed system implementation architecture can reasonably be expected to satisfy the numerical requirements and safety objectives in Q.6.2.1.1 and Q.6.2.1.2.

b. The FDALs for the functions implementing the system were assigned including a rationale to substantiate the assignment in Q.6.2.3.1.

c. Independence requirements between the functions were identified and captured in Q.6.2.3.4.

d. The proposed safety requirements were identified in Q.6.2.3.5.

e. The development team has accepted all proposed requirements identified by safety engineering.

f. The proposed architecture did not introduce additional failure conditions not included in the SFHA.

g. The proposed safety requirements rationale ties the requirements to the safety assessment in Q.6.2.3.5.

h. Assumptions were captured and provided to the airplane level as described in Q.6.2.5.

i. Derived requirements identified in ARP4754B/ED-79B, Appendix E have been reviewed for safety impact.

Q.6.2.5 PSSA Outputs

Once accepted by the development process, proposed safety requirements generated from the PSSA are captured in the WBS's requirement set and identified as safety requirements.

The WBS allocates the WBS requirements including safety requirements (e.g., probability, FDAL/IDAL, independence) to the subsystem (BSCU) supplier based on the proposed WBS architecture.

(Editor's Note: iteration may be required between the architecture and the allocation, based on feedback received from the BSCU supplier.)

SAENORM.COM : Click to view the full PDF of arp4761a

These outputs, which are a summary of information derived in Q.6.2.3.5, are provided to the BSCU supplier who then begins their PSSA activities.

a. The probability of BSCU failure resulting in loss of a valid braking command output to the NMV shall not exceed 2.0E-04 per flight.

b. The probability of BSCU failure resulting in unannunciated erroneous braking command to the NMV shall not exceed 2.0E-04 per flight.

c. The probability of BSCU failure resulting in the loss of command to open the SOV shall not exceed 2.0E-04 per flight.

d. The probability of BSCU failure resulting in unintended closure of the S/ASV shall not exceed 2.0E-04 per flight.

e. The SOV and NMV commands shall be provided by the BSCU upon loss of either airplane electrical power input.

f. When “HYD1 Enable” output is enabled, then “Alt/Emer Ctrl” output shall be disabled.

g. When “HYD1 Enable” output is disabled, then “Alt/Emer Ctrl” output shall be enabled.

h. No single failure shall cause erroneous NMV command and inhibit the SOV function.

i. The wheel brake command function of the BSCU shall be developed to FDAL A.

Assumptions provided to system development for communication to the airplane level:

a. The probability of “Loss of Normal Braking System Hydraulic Equipment” will be less than 3.3E-05 per flight.

b. The probability of “Loss of Alternate Braking System Hydraulic Equipment” will be less than 3.3E-05 per flight.

c. The probability of seven or more wheel speed sensors erroneous or inoperative will be less than 1.0E-07 per flight.

d. The failure rate for loss of an airplane electrical power bus will be less than 1.0E-04 per hour of flight.

e. The failure rate for loss of a left brake pedal position input will be less than 1.0E-06 per hour of flight.

f. Airplane electrical power bus 1 is independent from airplane electrical power bus 2.

g. HYD 1 hydraulic system is independent from HYD 2 hydraulic system.

(Editor’s Note: As f. and g. are PASA requirements it is not necessary to pass them as assumptions, though it is a good practice to do so for confirmation.)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.6.3 BSCU PSSA Activities - BSCU First Iteration

This section presents an example of completing the PSSA activities at a Line Replaceable Unit (LRU) level, i.e., BSCU.

Q.6.3.1 PSSA BSCU Inputs

(Editor’s Note: The BSCU safety requirements are received from the development process. These would be the same as those output from the WBS PSSA and are not repeated here.)

(Editor’s Note: Part of the BSCU inputs passed down to the BSCU supplier could be a statement that the BSCU FTA does not have to model airplane power, as this is modeled at the WBS level.)

(Editor’s Note: The failure condition for uncommanded wheel braking is re-introduced for the BSCU portion of the PSSA because it provides a better example for demonstrating the BSCU CMA and FMEA during the SSA process.)

Q.6.3.1.1 Allocated Safety Requirements (From Other PSSA Levels)

Other than the requirements from the WBS, there are currently no safety requirements from other PSSAs identified that need to be evaluated by the BSCU Analysis.

Q.6.3.1.2 Architecture Summary/Description

The requirements imposed on the BSCU for availability and integrity led to the proposal that the BSCU consist of two independent systems to meet the availability requirements and the proposal that each system contain a command channel capable of meeting the integrity requirements. The WBS specified that these channels are housed in a single LRU. A block diagram of the proposed BSCU architecture is shown in Figure Q.6-13.

Each BSCU channel receives input power from a single power source (PWR 1 or PWR 2). Each BSCU channel generates the necessary voltages within its own power supply (not shown in Figure Q.6-13). Brake pedal inputs are provided to the command channels, which compute the necessary braking commands. The HYD 1 Enable signal is output from both command blocks and provides a control signal for the SOV. Channel 1 also provides a control signal to the command source select switch, which outputs the “Normal Ctrl” signal.

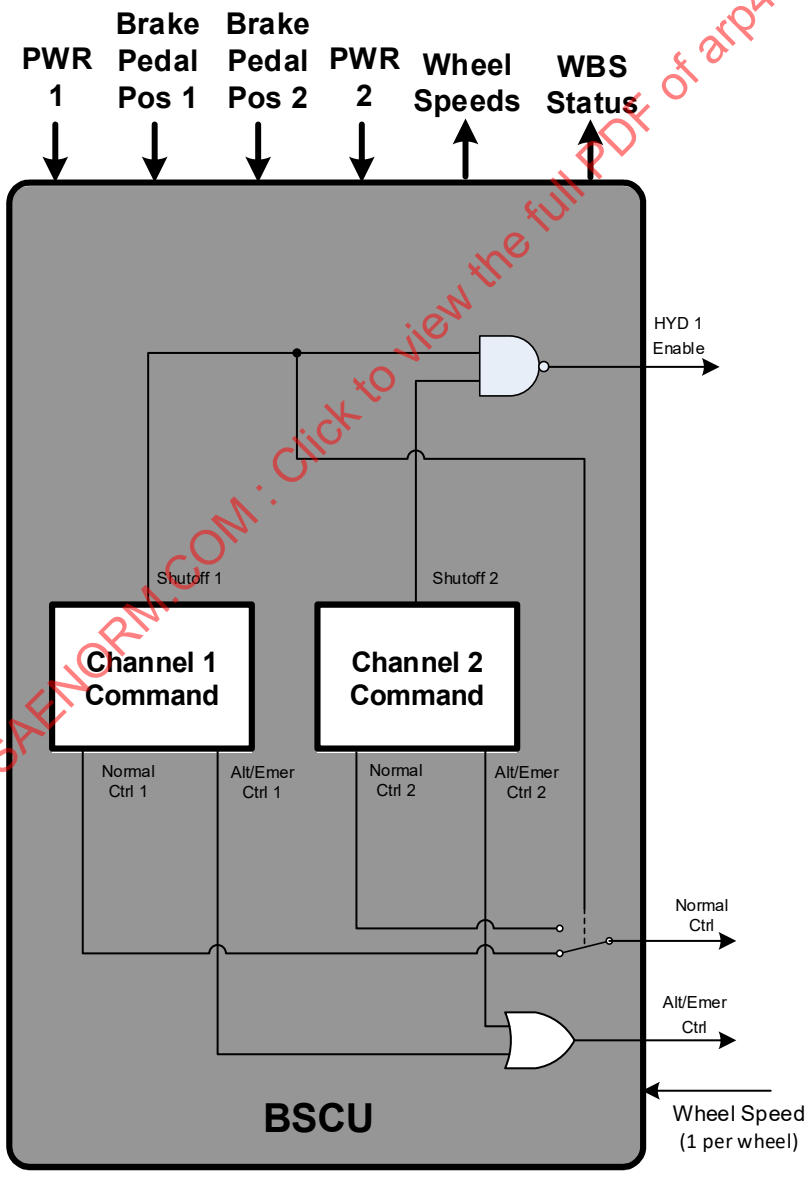


Figure Q.6-13 - (PSSA - BSCU) BSCU iteration 1

SAENORM.COM : Click to view the full PDF of arp4761a

In normal operation, BSCU Channel 1 provides the braking commands (including anti-skid commands) to the wheel brakes. In the event of a malfunction of Channel 1, Channel 2 assumes control. In the event that Channel 2 subsequently fails, all BSCU outputs are disabled, the SOV is closed (preventing flow) and the WBS Status is set to invalid.

Q.6.3.1.2.1 Architecture Requirements

(Editor's Note: Some architectural requirements were input to the WBS and passed to the BSCU based on initial program specification of the S18 airplane. New architecture requirements were also created as part of the design evaluation based on the WBS safety assessment.)

(Editor's Note: The architecture requirements in Table Q.6-6 were received from the WBS development process.)

(Editor's Note: Requirements that were designated as "Safety" may or may not have been developed as part of the safety assessment process but were identified as necessary to achieve the safety objectives.)

Table Q.6-6 - (PSSA - BSCU)
Safety requirements from WBS PSSA

Requirement Number	Safety	Requirement
S18-WBS-R-0047	No	The Wheel Brake System shall meet safety requirements while operating in an average atmospheric radiation environment per the IEC 62396 standard with an altitude of 40000 feet and a latitude of 45 degrees.
S18-WBS-R-0509	No	The Wheel Brake System shall have dual BSCU command functions.
S18-WBS-R-1613	No	Hydraulic pressure shall be controlled for weight, autobrake mode, ground speed, wheel rotation, brake temperature and deceleration rate in accordance with graphs given in S18 Brake Force Analysis AAS18-XXX.
S18-WBS-R-2986	Yes	The wheel brake command function of the BSCU shall be developed as FDAL A.
S18-WBS-R-2997	Yes	The BSCU shall have two independent command channels.
S18-WBS-R-6104	Yes	The probability of BSCU failure resulting in loss of a valid braking command output to the NMV shall not exceed 2.0E-04 per flight.
S18-WBS-R-6105	Yes	The probability of BSCU failure resulting in unannunciated erroneous braking command to the NMV shall not exceed 2.0E-04 per flight.
S18-WBS-R-6106	Yes	The probability of BSCU failure resulting in the loss of command to open the SOV shall not exceed 2.0E-04 per flight.
S18-WBS-R-6107	Yes	The probability of BSCU failure resulting in unintended closure of the S/ASV shall not exceed 2.0E-04 per flight.
S18-WBS-R-6108	Yes	The SOV and NMV commands shall be provided by the BSCU upon loss of either airplane power input.
S18-WBS-R-6109	Yes	When "HYD 1 Enable" output is enabled, then "Alt/Emer Ctrl" output shall be disabled.
S18-WBS-R-6110	Yes	No single failure shall cause erroneous NMV command and inhibit the SOV function.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.6.3.1.3 Operational Requirements

(Editor's Note: The S18 program has established some expected operating characteristics based on customer interface during the initial market research. This information was used to create an operational profile for the airplane.)

There are no changes to the operational requirements, the operational requirements are shown in Q.6.2.1.2.3 and are output from the WBS to the BSCU supplier.

Q.6.3.2 BSCU Functional Mapping - BSCU First Iteration

The BSCU functional block diagram in Figure Q.6-13 was used to identify the elements within the BSCU that contribute to the safety requirements identified in Q.6.3.1.

Q.6.3.3 PSSA Failure Condition Evaluation - BSCU First Iteration

(Editor's Note: For simplicity of this part of the example, only the uncommanded braking requirement FTA is included. The results for other requirements are not included.)

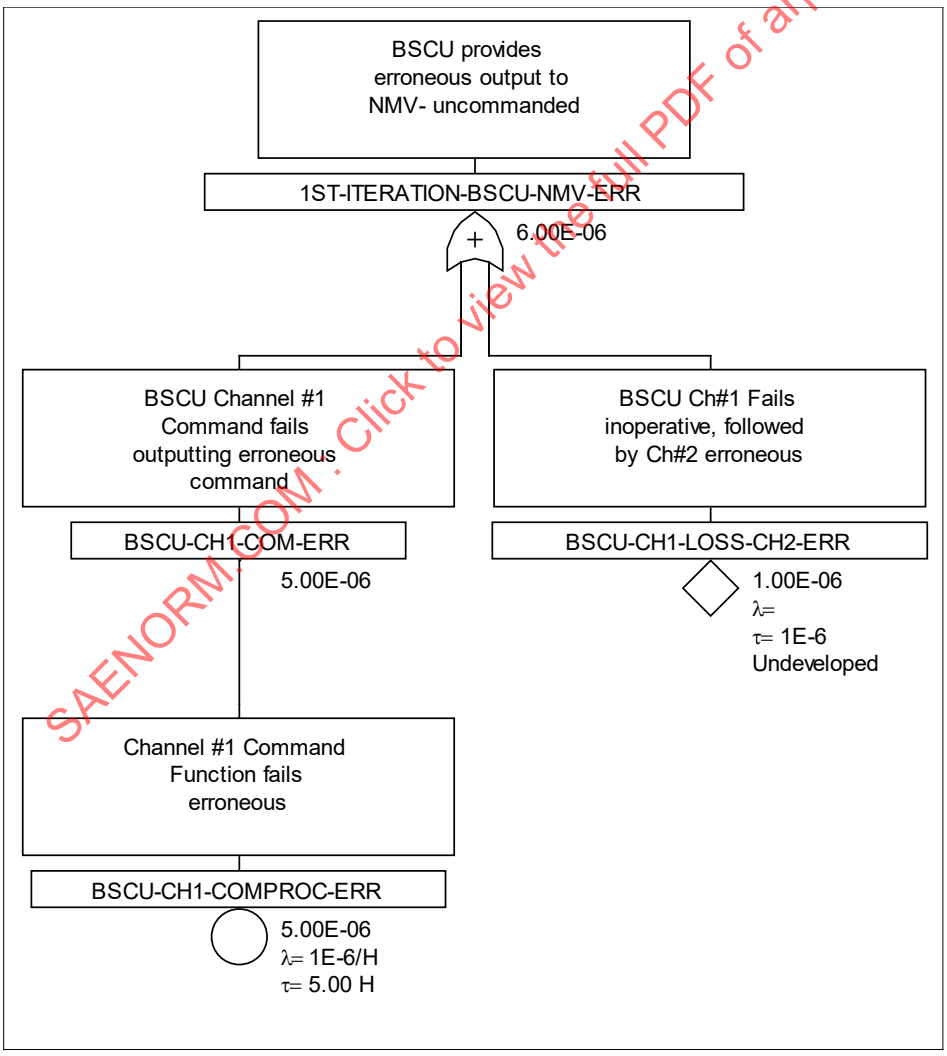
An FTA assessment of the architecture shown in Figure Q.6-13 is the basis of the first iteration.

Q.6.3.3.1 Fault Tree for Failures

(Editor's Note: This section contains the fault trees for the significant failure conditions associated with the BSCU only.)

(Editor's Note: Alternative methods of analysis to FTA exist that could be used here. These include Dependence Diagrams, Markov Analysis, and Model-Based Safety Analysis.)

The FTA associated with S18-WBS-R-6105 (unannunciated erroneous braking command to the NMV) models the normal condition whereby Channel #1 is in control of the NMV and fails erroneous resulting in the BSCU commanding the NMV to an open position. Also modeled (undeveloped) is the case where Channel #1 fails inoperative followed by erroneous operation of Channel #2.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-14 - (PSSA - BSCU - FTA)
BSCU first Iteration

(Editor's Note: Even though the first iteration FTA shows compliance with its numerical requirement, the failure condition evaluation was stopped once it was recognized that the proposed architecture could not meet the requirements associated with the uncommanded full symmetric wheel deceleration Catastrophic failure condition (1.1.MF1), which is not shown here. It is clear from the simple FTA (Figure Q.6-14) that a single command function without a monitor cannot meet the associated safety requirements.)

Q.6.3.4 PSSA BSCU Completion - BSCU First Iteration

When it was recognized that the initial architecture could not meet the safety requirements, no further analysis of that architecture was performed. So FDAL and IDAL requirements were not generated, nor independence or detailed quantitative requirements. No safety assumptions or requirements were identified based on the proposed architecture.

Q.6.3.5 PSSA BSCU Outputs - BSCU First Iteration

The primary output generated was that the proposed architecture will not meet the safety requirements imposed on the BSCU. Conversations ensued between the safety analyst and the development team to clarify that a command channel without an appropriate level of monitoring cannot meet the safety requirements. The development process was then tasked with producing another proposed architecture to be evaluated by the PSSA process. The subsequent evaluation constitutes the "Update Iteration" sections which follow.

(Editor's Note: The level of formality of the way this information is communicated will vary by organization. In this example, the safety team sent an email to the development team containing the information in the preceding paragraph. No formal documentation was created since the proposed design cannot meet the safety requirements.)

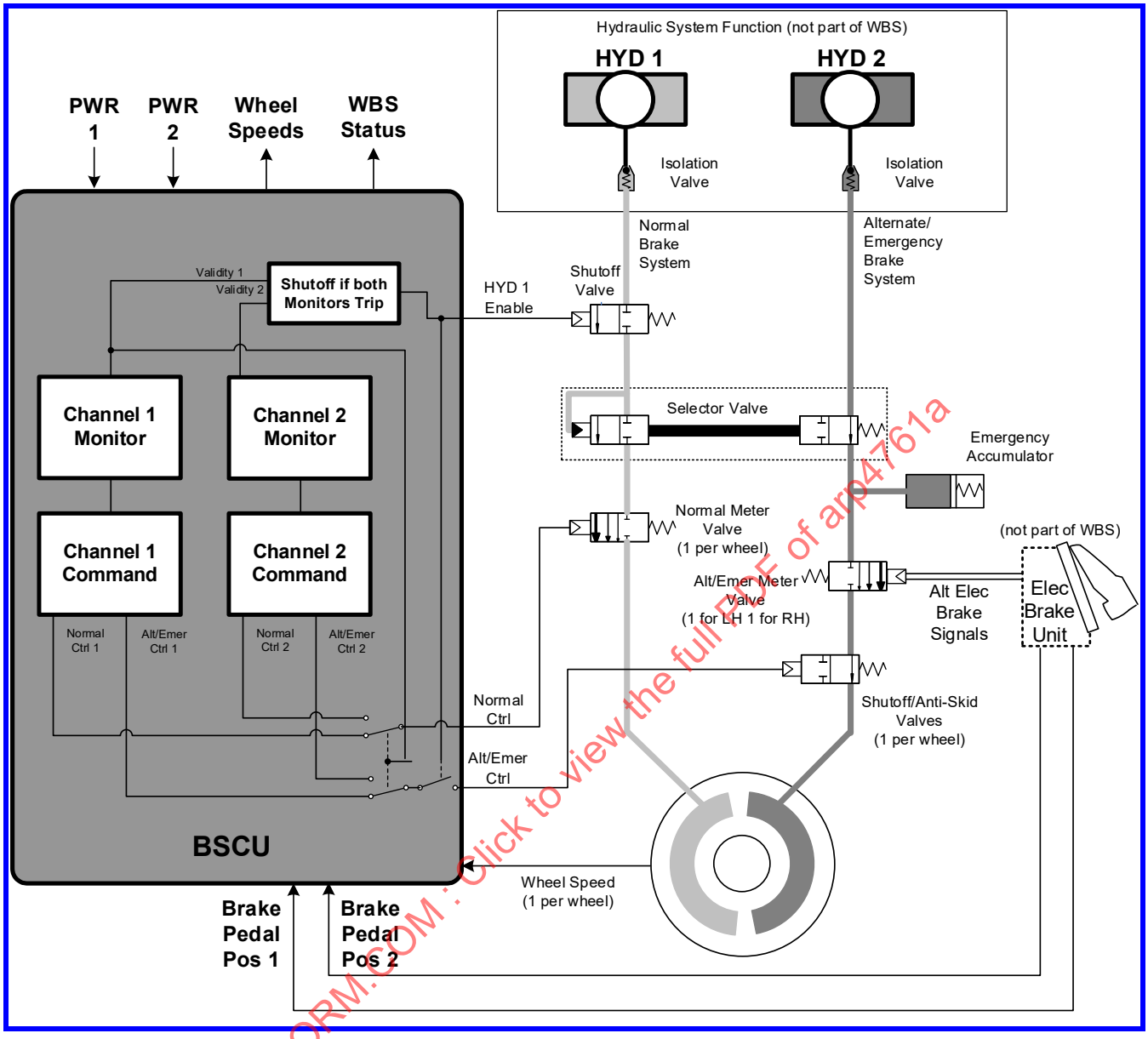
Q.6.4 PSSA BSCU Activities - BSCU Update Iteration

Safety worked with the development team to define monitoring that would allow the system to meet the safety requirements. During this definition phase, informal fault trees were generated to evaluate various proposed architectures. These informal fault trees were not archived since the architectures involved were not selected. Once an architecture is selected, the PSSA process is applied to the new architecture including more formal fault trees.

Q.6.4.1 PSSA BSCU Inputs

The safety requirements are unchanged from the BSCU Iteration 1 evaluation. Evaluation of the updated architecture (update iteration) follows:

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-15 - (PSSA - BSCU)
BSCU update iteration

Q.6.4.1.1 Allocated Safety Requirements (From Other PSSA Levels)

Other than those passed from the WBS (listed in Q.6.3.1.2.1), currently no safety requirements from other PSSAs have been identified that need to be evaluated by the BSCU Analysis.

Q.6.4.1.2 Architecture Summary/Description

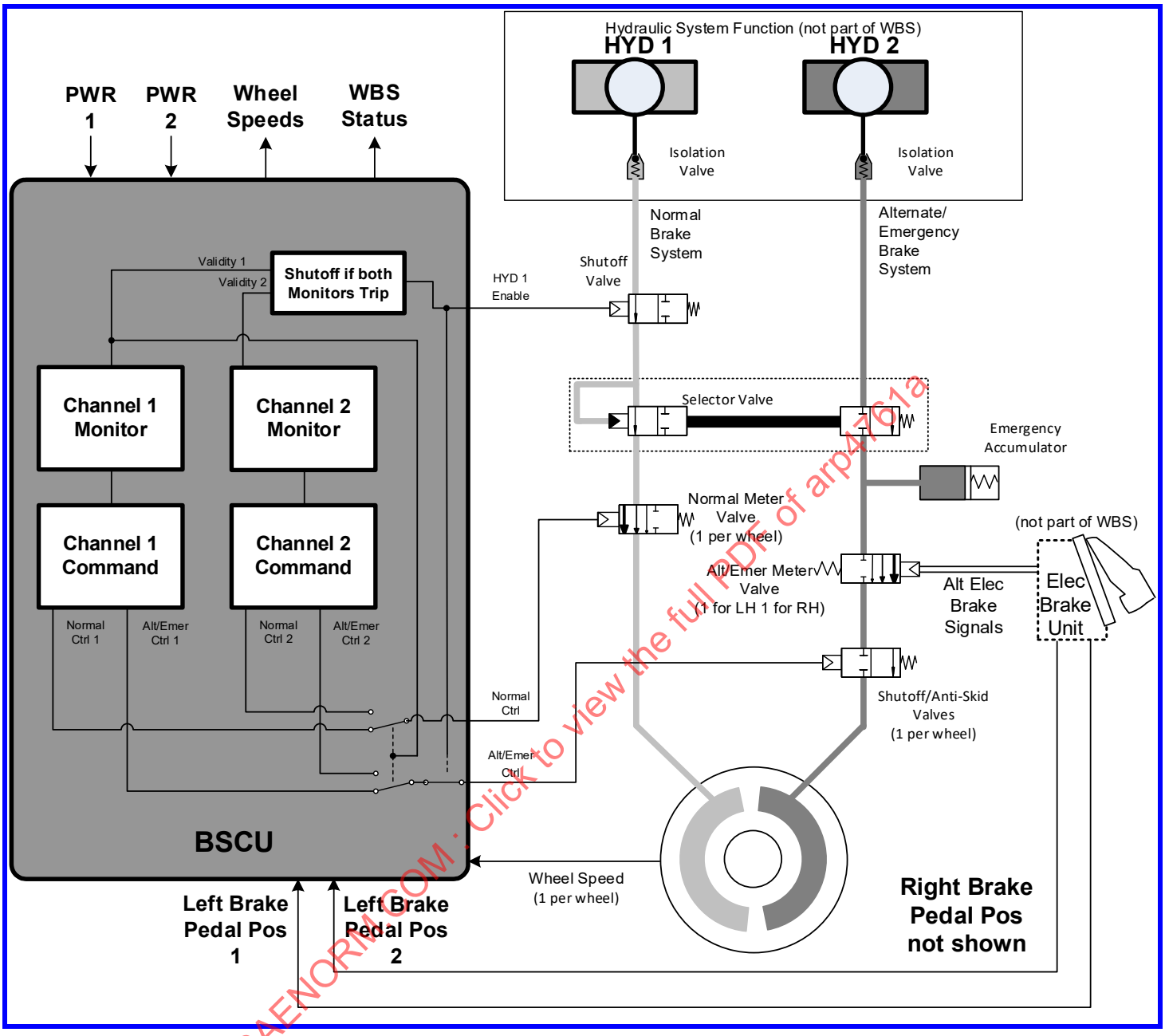
The requirements imposed on the BSCU for availability and integrity led to the proposal that the BSCU consist of two independent channels to meet the availability requirements and the proposal that each channel contain a command and monitor to meet the integrity requirements. A block diagram of the proposed BSCU architecture is shown in Figure Q.6-15. At this point in the development process, the power design and routing for pedal position inputs within the BSCU have not been defined. Therefore, the diagram does not contain details associated with these inputs, so the safety analyst inferred an appropriate design for how the inputs are handled inside the BSCU.

Brake pedal inputs are provided to each of the command and monitor channels (Pedal Pos 1 to Channel 1, Pedal Pos 2 to Channel 2) which compute the necessary braking commands. Each command output is compared with the corresponding monitor, a mis-match results in an invalid command. As part of meeting the integrity requirement, a detected command/monitor mis-match failure reported by an individual channel in a BSCU will cause that channel of the BSCU to disable its outputs. It also sets the individual System Validity Monitor to invalid allowing the second channel to become active within the BSCU to meet the availability requirements. Each BSCU System Validity Monitor is provided to an overall BSCU Validity Monitor (shown as WBS Status). Failure of both Channel 1 and Channel 2 will cause the opening of the SOV (HYD 1 Enable) on the primary/HYD 1 Pump which results in the Selector Valve selecting the Alternate Braking Mode provided by HYD 2, by opening the switch on the Alt/Emer control signal.

In normal operation, BSCU Channel 1 provides the braking and anti-skid commands to the wheel brakes. When Channel 1 reports a failure via its System Validity Monitor, the output of Channel 2, is switched in to provide the commands. In the event that Channel 2 subsequently fails or is already failed, all BSCU outputs are disabled and the BSCU Validity Monitor is set to invalid.

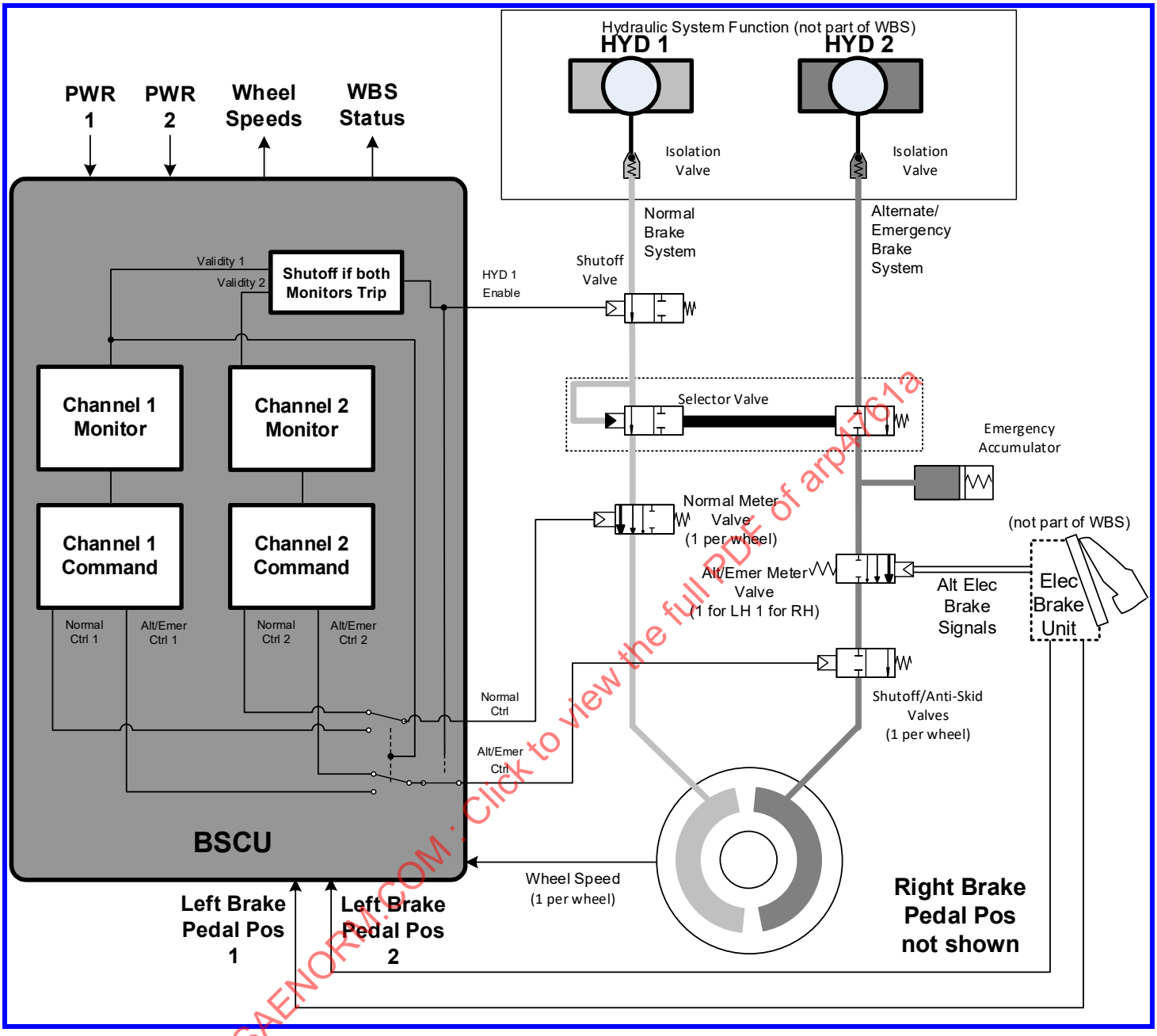
Figure Q.6-16, Figure Q.6-17, and Figure Q.6-18 illustrate the different operational states of the proposed architecture.

SAENORM.COM : Click to view the full PDF of arp4761a



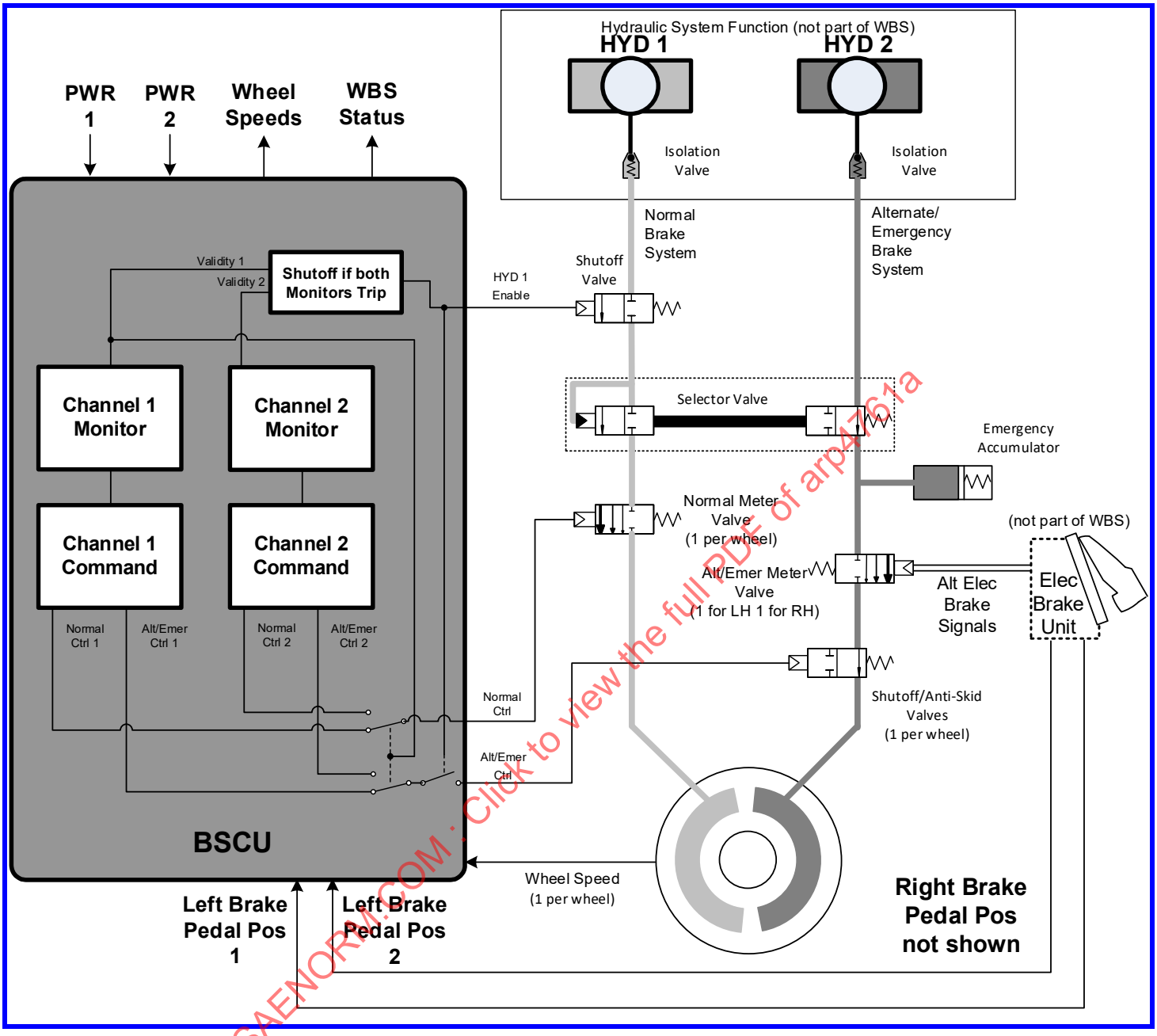
SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-16 - (PSSA - BSCU)
BSCU update iteration (NORMAL Mode: Channel 1 in control)



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-17 - (PSSA - BSCU)
BSCU update iteration (NORMAL Mode: Channel 2 in control)



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-18 - (PSSA - BSCU)
BSCU update iteration: ALTERNATE Mode
(when HYD 2 working)/Emergency Mode (when HYD 2 not working)

Q.6.4.1.3 Architecture Requirements

There are no changes to the architecture requirements, the architecture requirements are shown in Q.6.3.1.2.1.

Q.6.4.1.4 Operational Requirements

The S18 airplane program has established some expected operating characteristics based on customer interface during the initial market research. This information was used to create an operational profile for the airplane.

The operational profile for the WBS safety assessment is provided to the BSCU supplier and includes:

a. An average flight duration of 5 hours.

b. An airplane life of 100000 flight hours.

c. A power on time of 100 hours.

There are no changes to the operational requirements, the operational requirements are shown in Q.6.2.1.2.3.

Q.6.4.2 BSCU Functional Mapping - BSCU Update Iteration

The BSCU functions include, but are not limited to:

a. Provide NORMAL Mode commands.

b. Provide Shutoff Valve commands.

(Editor's Note: Figure Q.6-19 is an alternate method to Figure Q.6-6 as a conceptual thought process for evaluating how each portion of the architecture could contribute to the failure condition under evaluation, including protection provided by monitoring. Each function is annotated on the diagram to group the elements of the BSCU architecture that provide each function.)

SAENORM.COM : Click to view the full PDF of arp4761a

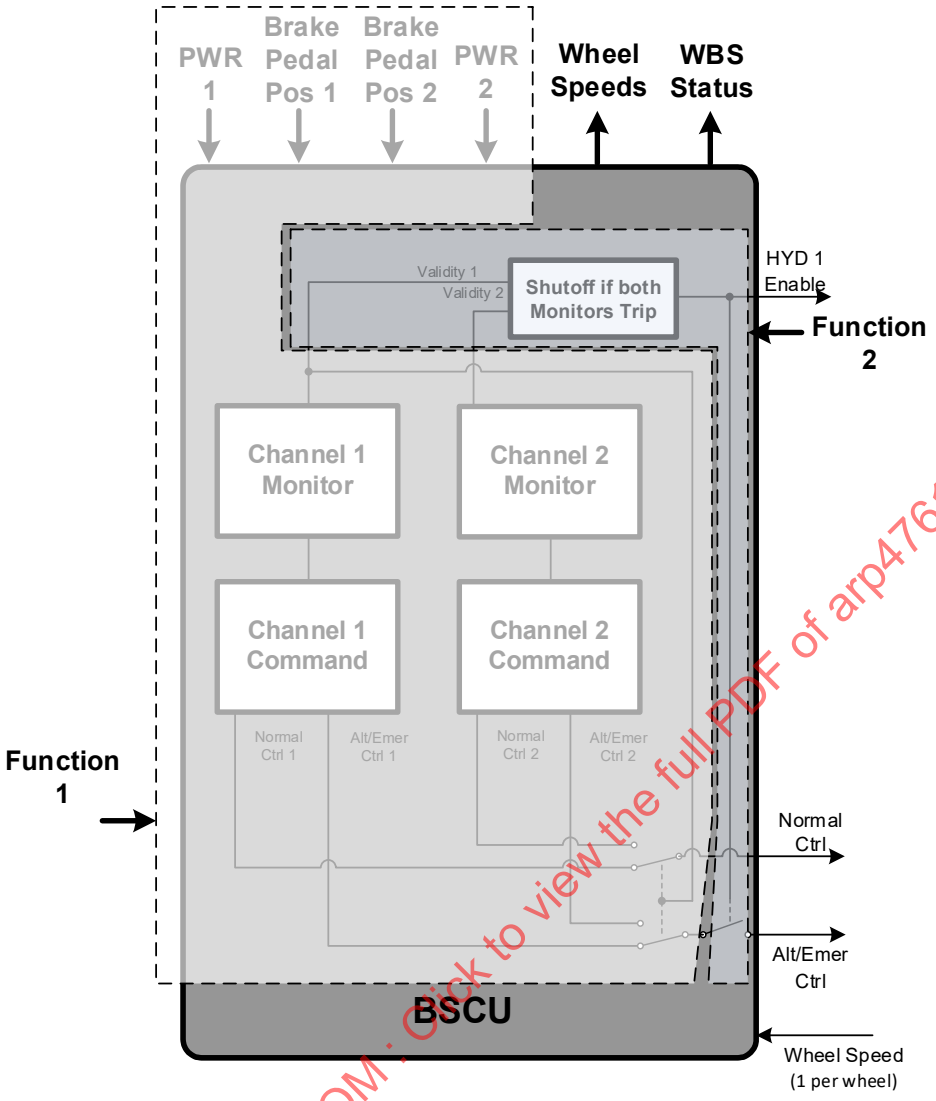


Figure Q.6-19 - (PSSA - BSCU)
BSCU functional mapping

SAENORM.COM : Click to view the full PDF of arp4761a

Using the described functional mapping, Table Q.6-7 shows the specific failure modes, and their mitigations, that result in the failure effects of interest to this analysis. The Functions illustrated are defined as follows:

Function 1 performs the necessary computations to calculate the required metering for the NMV and ASV. This is output through the Normal Ctrl and Alt/Emer Ctrl signals. Function 1 also generates a validity status for each computational channel, Validity 1 and Validity 2.

Function 2 controls the opening of the SOV through the HYD 1 Enable signal based on the validity status outputs from Function 1.

Table Q.6-7 - (PSSA - BSCU)
BSCU contributions to Failure Conditions

Failure Effect	Functional Failure	Failure Modes	Mitigation Features
Uncommanded braking due to BSCU	Function 1 erroneous “Normal Ctrl” and Function 2 fails to disable HYD 1 Enable signal	Function 1 erroneous: - Channel 1 command or Channel 2 command erroneous behavior - BSCU power erroneous	Function 2
		Function 2 fails: - BSCU fails to disable HYD 1 Enable signal - BSCU power erroneous - Monitor 1 or Monitor 2 fails	None
Loss of wheel braking command from BSCU	Function 1 fails to provide “Normal Ctrl” or Function 2 erroneously disables HYD 1 Enable signal	Function 1 fails: - Channel 1 command and Channel 2 command fails - Loss of BSCU power	Existing redundancy
		Function 2 erroneous: - Monitor 1 and Monitor 2 output erroneous validity signal - BSCU outputs erroneous HYD 1 Enable signal	Existing redundancy

Q.6.4.3 PSSA Failure Condition Evaluation - BSCU Update Iteration

The individual requirements for which verification is required to be shown by the BSCU are reproduced in Table Q.6-8:

Table Q.6-8 - (PSSA - BSCU)
Safety requirements from WBS PSSA

Requirement #	Description
S18-BSCU-R-0001	The wheel brake command function of the BSCU shall be developed to FDAL A *(Editor’s Note: Based on the Catastrophic classification of “Uncommanded braking due to BSCU”)*
S18-BSCU-R-0002	The probability of BSCU failure resulting in loss of a valid braking command output to the NMV shall not exceed 2.0E-04 per flight
S18-BSCU-R-0003	The probability of BSCU failure resulting in unannunciated erroneous braking command to the NMV shall not exceed 2.0E-04 per flight
S18-BSCU-R-0004	The probability of BSCU failure resulting in the loss of command to open the SOV shall not exceed 2.0E-04 per flight
S18-BSCU-R-0005	The probability of BSCU failure resulting in unintended closure of the S/ASV shall not exceed 2.0E-04 per flight
S18-BSCU-R-0006	The SOV and NMV commands shall be provided by the BSCU upon loss of either airplane electrical power input
S18-BSCU-R-0007	When “HYD 1 Enable” output is enabled, then “Alt/Emer Ctrl” output shall be disabled
S18-BSCU-R-0008	No single failure shall cause erroneous NMV command and inhibit the SOV function

(Editor’s Note: Once the architecture is selected the requirements development process may initiate additional safety requirements that could potentially result in further iteration of the architecture to meet the safety objectives.)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.6.4.3.1 FDAL and IDAL Assignment

(Editor's Note: This example shows FDAL and IDAL assignment using fault trees to determine the Functional Failure Sets. Other methods of determining the assignment may be used.)

(Editor's Note: The FDAL and IDAL assignment were coordinated with the development team to ensure the assigned levels aligned with program needs.)

Q.6.4.3.1.1 FDAL Assignment for Braking System Control Function

The following FDALs were considered relevant to the BSCU functions by the WBS PSSA process:

a. Provide NORMAL Mode commands: FDAL A (per requirement S18-BSCU-R-0001).

b. Provide Shutoff Valve commands: FDAL B (per Hazardous classification for 1.1.TL (Total Loss of Wheel Deceleration)).

However, FDAL A was allocated/assigned by the WBS PSSA process, given a single set of requirements for the BSCU.

(Editor's Note: The SOV commands cannot independently fail such that uncommanded braking occurs. However, the SOV commands are a protection mechanism against the uncommanded failure condition. The most severe failure condition it directly contributes to is 1.1.TL "Total loss of wheel deceleration (80% or more)," which is classified as Hazardous.)

(Editor's Note: It would be possible to have identified command and monitor as functions and assigned FDALs to these. This would necessitate maintaining development independence. For this reason, the decision was made to not pursue this.)

Q.6.4.3.1.2 IDAL Assignment for Braking System Control Function

The following items require IDAL assignment for the wheel braking function of the BSCU:

- Command hardware.
- Command software.
- Monitor hardware.
- Monitor software.

(Editor's Note: Other hardware such as logic gates and switches are simple and can be considered equivalent to IDAL A in this example. They do not need to have an IDAL assignment identified.)

A consideration in the IDAL assignment process is the specifications and requirements traceability for the command and monitor functions. As shown in Figure Q.6-20 the command and monitor functions have independent software specifications. Thus, if desired the IDAL assignment process can leverage this difference in accordance with the DAL assignment table (Appendix P, Table P2).

The S18 BSCU requirements traceability followed the specification tree as shown in Figure Q.6-20. The traceability was bidirectional with the higher-level requirements being parent to the requirements below.

SAENORM.COM : Click to view the full PDF of arp4761a

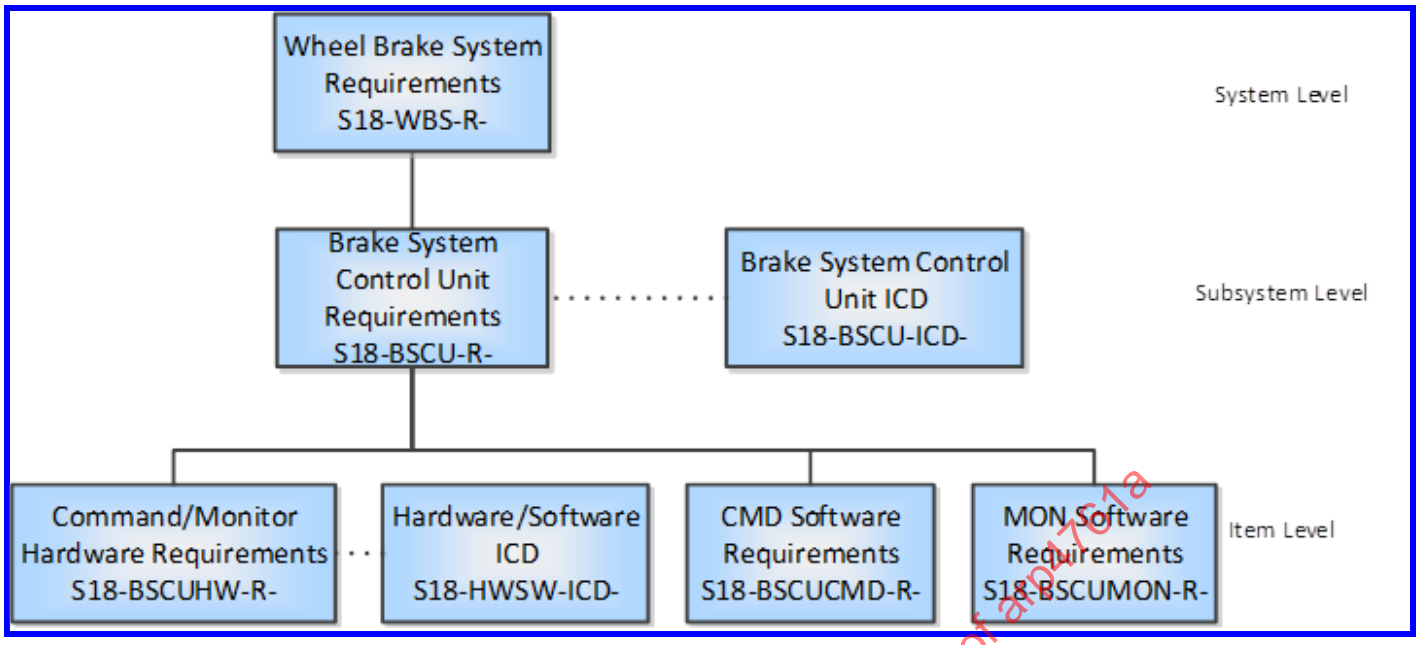


Figure Q.6-20 - (PSSA - BSCU) BSCU requirements traceability

The allocation of IDALs requires understanding how BSCU software and hardware items might cause or contribute to the failure condition 1.1.MF1 - Uncommanded full symmetric wheel deceleration. The choice of IDALs is constrained by FDAL A assigned to the function “Provide NORMAL Mode commands.” This FDAL allocated from the WBS PSSA process is driven by the failure condition 1.1.MF1 - Uncommanded full symmetric wheel deceleration.

(Editor’s Note: “_COMX_HW”, “_MONX_HW”, “_COMX_SW”, and “_MONX_SW” naming convention was used for this effort, for convenience where “X” designates either Channel 1 or Channel 2. Either channel could be represented by the same branch, because either channel is capable of uncommanded braking. Figure Q.6-21 could have represented both channels 1 and 2 separately by duplicating Channel “X.”)

(Editor’s Note: The FDALs and IDALs shown in the figure are the result of analyzing the Functional Failure Sets (FFS) shown in Table Q.6-9. The BSCU safety team’s preference is to depict FDALs in the location they are shown below. Other ways including labeling on the gates could have been used.)

SAENORM.COM : Click to view the full PDF of arp4761a

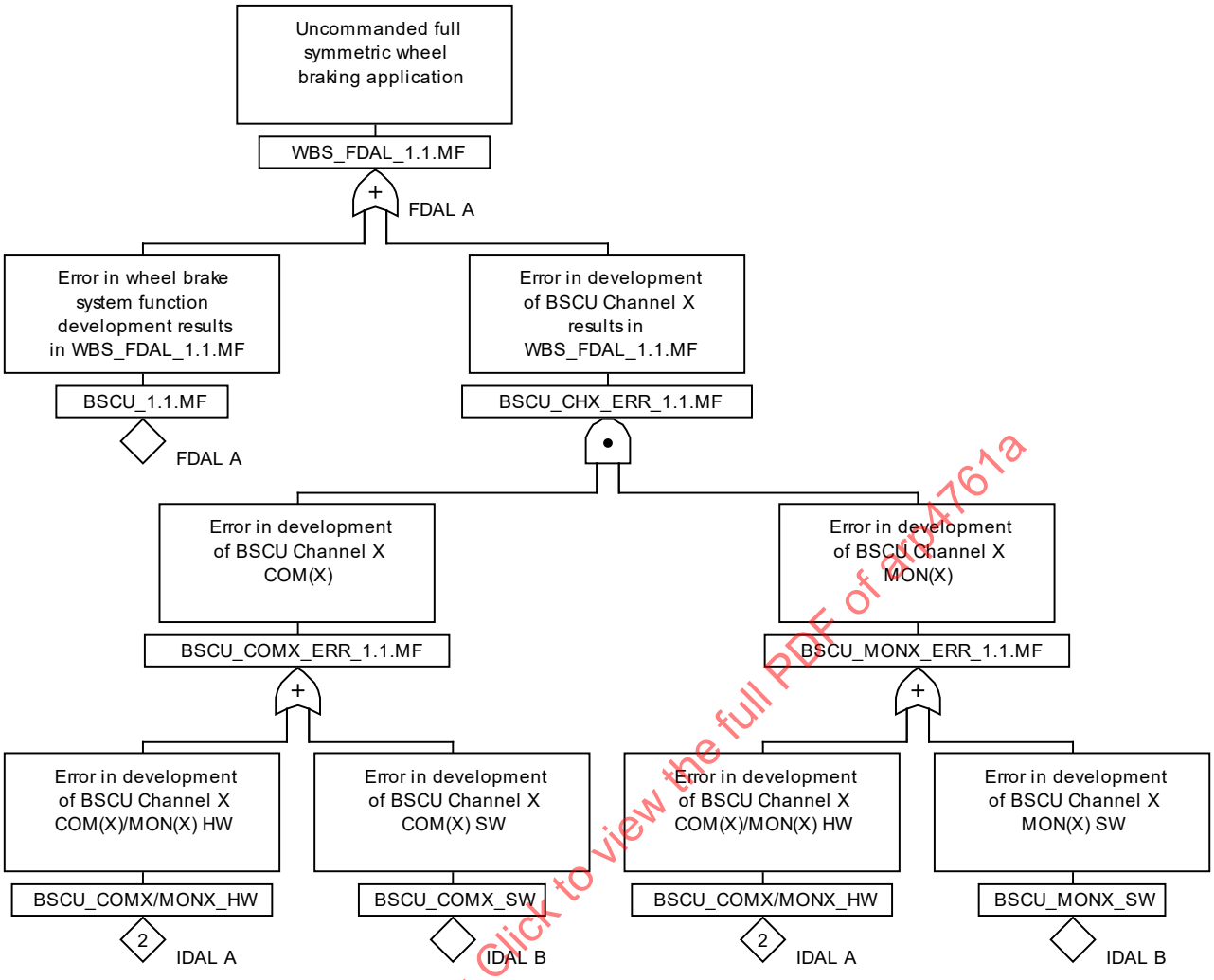


Figure Q.6-21 - (PSSA - BSCU)
BSCU update iteration: IDAL assignment

Table Q.6-9 summarizes the minimal FFSs that were identified from the fault free in Figure Q.6-21.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.6-9 - (PSSA - BSCU)
Functional failure set summary

Functional Failure Sets		Remarks
BSCU_1.1.MF=FDAL A		
BSCU_COMX/MONX_HW=IDAL A		A single Hardware Requirements Specification is envisaged for COMX/MONX hardware. So, P.7.1, Case 1: Neither functional nor item development independence is applicable. The FDAL and IDAL are the same and are equal to the FDAL of the top-level function, in this case, A.
BSCU_COMX_SW=IDAL B	BSCU_MONX_SW=IDAL B	Different/separate Software Requirement Specifications are envisaged for COMX software and MONX software respectively. Hence, P.7.4 Case 4 is applicable: No functional independence but item development independence. The item IDALs are assigned using either Option 1 or Option 2 in the decision in Table P2 corresponding to the top-level failure condition classification. In this case, only Option 2 is valid, resulting in an allocation of IDAL B for two of the members). *(Editor's Note: An allocation of IDAL A for one member, and IDAL C for the other member wouldn't have worked for BSCU_1.1.TL (any FFS member can result in loss (BSCU_1.1.TL), hence any FFS member must as a minimum be IDAL B).)*

The resulting IDAL assignments are summarized in Table Q.6-10

Table Q.6-10 - (PSSA - BSCU)
BSCU update iteration: IDAL assignment

Item	IDAL Assignment	Rationale
Command 1 HW	A	See Table Q.6-9
Command 1 SW	B	
Command 2 HW	A	
Command 2 SW	B	
Monitor 1 HW	A	
Monitor 1 SW	B	
Monitor 2 HW	A	
Monitor 2 SW	B	

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: Other IDALs would be assigned for evaluation of other requirements (and associated functions) but these are not shown here for clarity.)

(Editor's Note: This is one way but not the only way that the IDALs could have been allocated, recognizing that there are logistical issues/constraints around item development independence with this approach (i.e., allocating IDAL B to COM and MON S/W). This approach was chosen for illustrative purposes. COM and MON S/W could have been allocated IDAL A, employing the same Software Requirements Specification to simplify logistical issues/constraints.)

Q.6.4.3.2 FTAs for Failures

(Editor's Note: Alternative methods of analysis to FTA exist that could be used here. These include Dependence Diagrams, Markov Analysis, and Model-Based Safety Analysis.)

Q.6.4.3.2.1 FTA: Loss of a Valid Braking Command Output to the NMV

The fault tree for S18-BSCU-R-0002 “BSCU failure resulting in loss of a valid braking command output to the NMV” is modeled as failure of Channel #2, combined with failure of Channel #1. Each of the respective channels is composed of a command and monitor function and its associated power supply and pedal inputs, so basic events are included in the FTA to model loss of these functions.

(Editor’s Note: Though the architecture diagram doesn’t contain details related to power inputs or connectors, the safety analyst models one power supply in each channel in order to support the independence requirement S18-WBS-R-2997, for two independent channels.)

The FTA is made up of three elements. The first subtree [BSCU-CH2LAT_CH1-LOSS] models the latent failure of Channel #2 followed by the active failure of Channel #1. Since Channel #2 is not normally used it could fail in an inoperative state without detection for some failure modes. The exposure time for each of the Channel #2 basic events is conservatively assigned airplane life. Each channel contains basic events for loss of the command function, power supply, pedal inputs and models failure of the switch responsible for switching between Channel #1 and Channel #2.

The second subtree [BSCU-CH2CH1-LOSS] models the active failure of both Channel #1 and Channel #2 during the same flight. Channel #2 contains an additional basic event representing a false trip of the power supply monitor [BSCU-CH2-PSM-ERR]. The addition of the power supply monitor was determined during the development of the FTA for erroneous operation, and also accounting for common cause considerations in the CMA.

The third subtree is a single basic event representing a common cause to both Channel #1 and Channel #2. The switch that selects the channel could fail [BSCU-CMD-SW-TOTAL-ERR] such that neither Channel #1 nor Channel #2 is selected. This failure would be detectable via WBS Status upon landing, and therefore has an exposure time of one flight. The resulting FTA, shown in Figure Q.6-22 through Figure Q.6-24, does not meet the 2.0E-04 per flight requirement.

SAENORM.COM : Click to view the full PDF of arp4761a

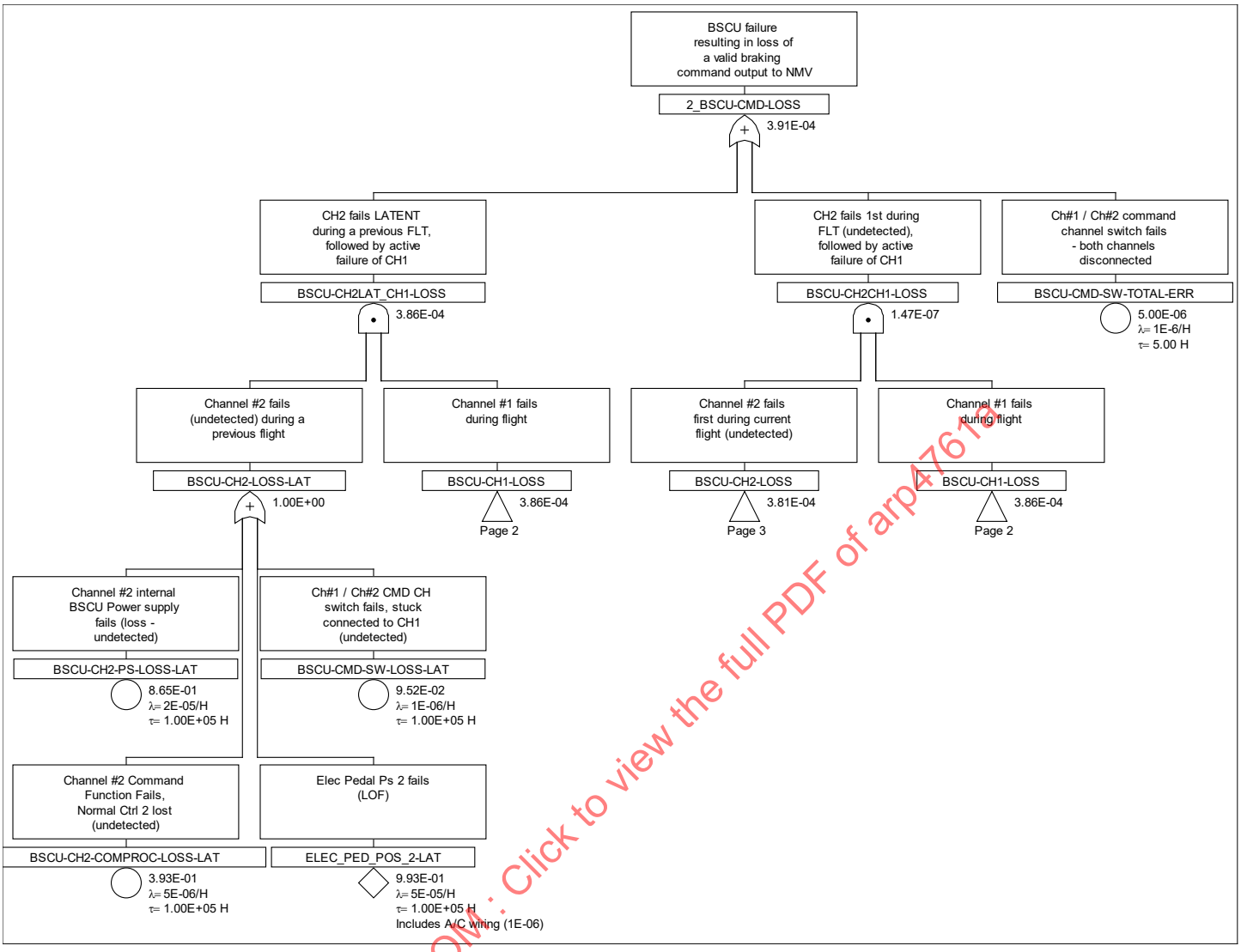


Figure Q.6-22 - (PSSA - BSCU - FTA)
BSCU update iteration: loss of a valid braking command output to the NMV lifetime latency (page 1 of 3)

SAENORM.COM : Click to view the full PDF of arp4761a

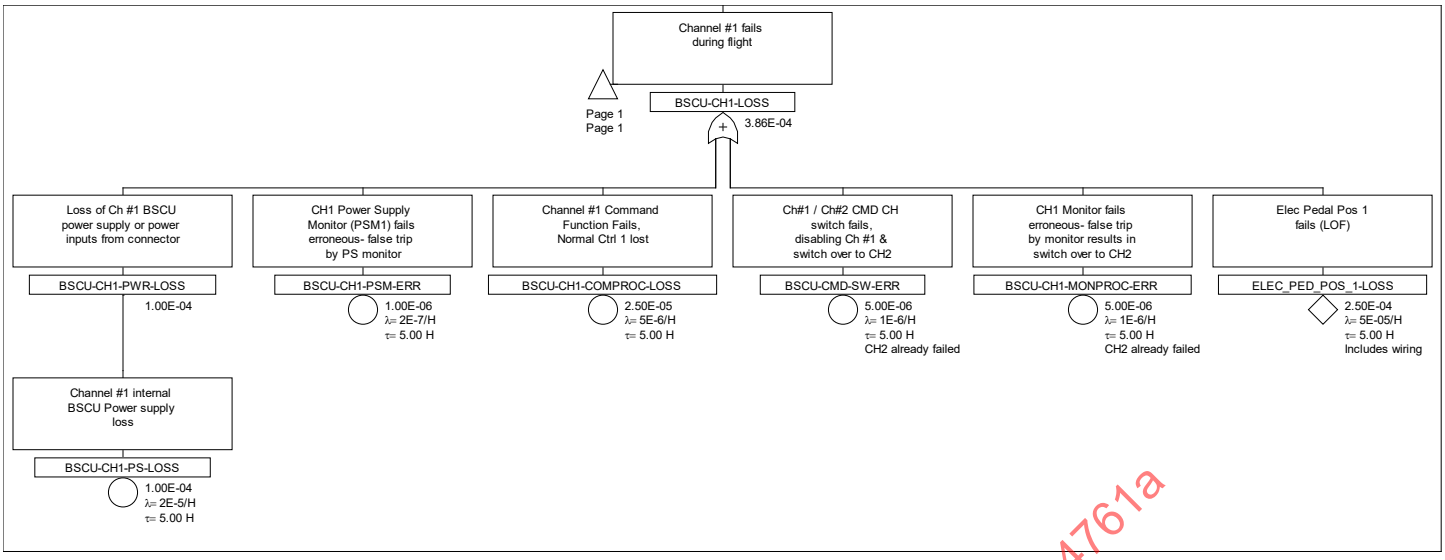
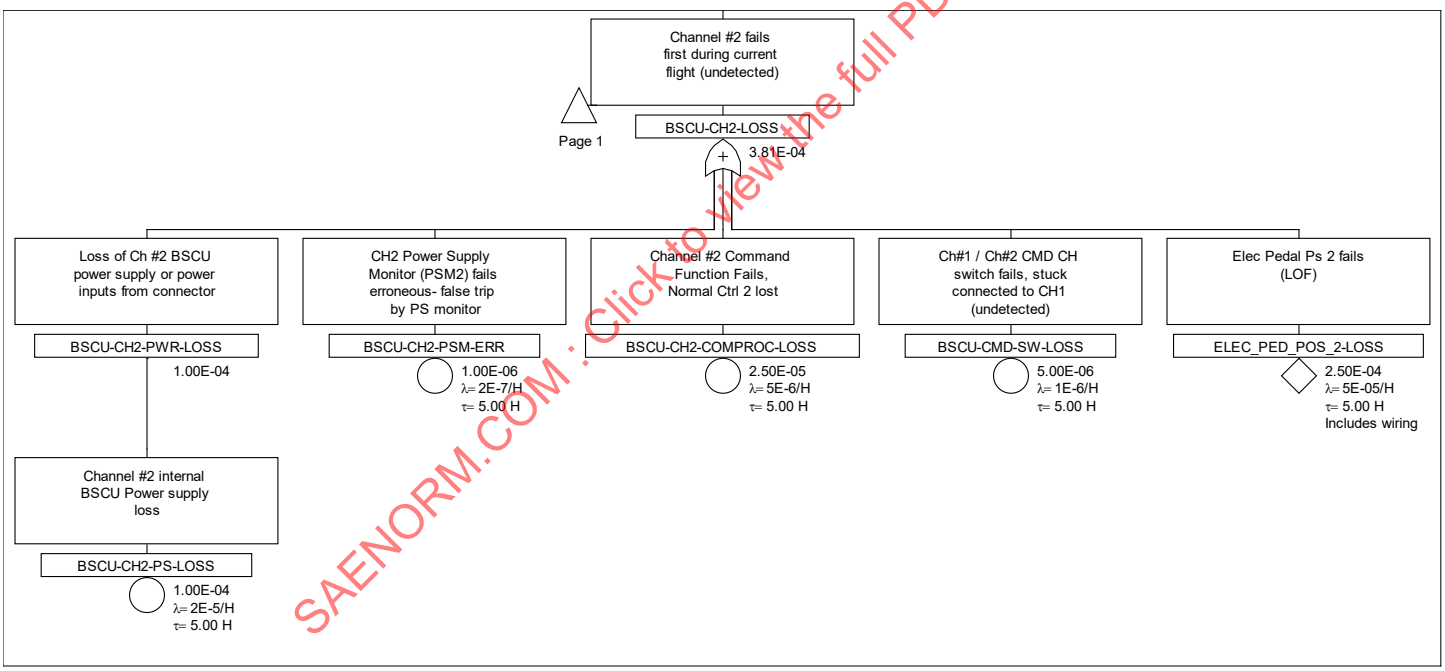


Figure Q.6-23 - (PSSA - BSCU - FTA)
BSCU update iteration: loss of a valid braking command output to the NMV lifetime latency (page 2 of 3)



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-24 - (PSSA - BSCU - FTA)
BSCU update iteration: loss of a valid braking command output to the NMV lifetime latency (page 3 of 3)

Since the requirement is not met (exceeding 2.0E-04 per flight), the decision was made to create a requirement for a power-up test of both channels and the switch every 100 hours, limiting the latent exposure (BSCU-009). In the event of a failure, an annunciation is output by the WBS Status. It is assumed that a maintenance action is performed upon the WBS status indicating a failure, as captured in the assumptions to WBS.

The resulting FTA is shown in Figure Q.6-25, which meets the requirement.

(Editor's Note: Only the first page of the FTA is shown for brevity, as pages 2 and 3 are unchanged.)

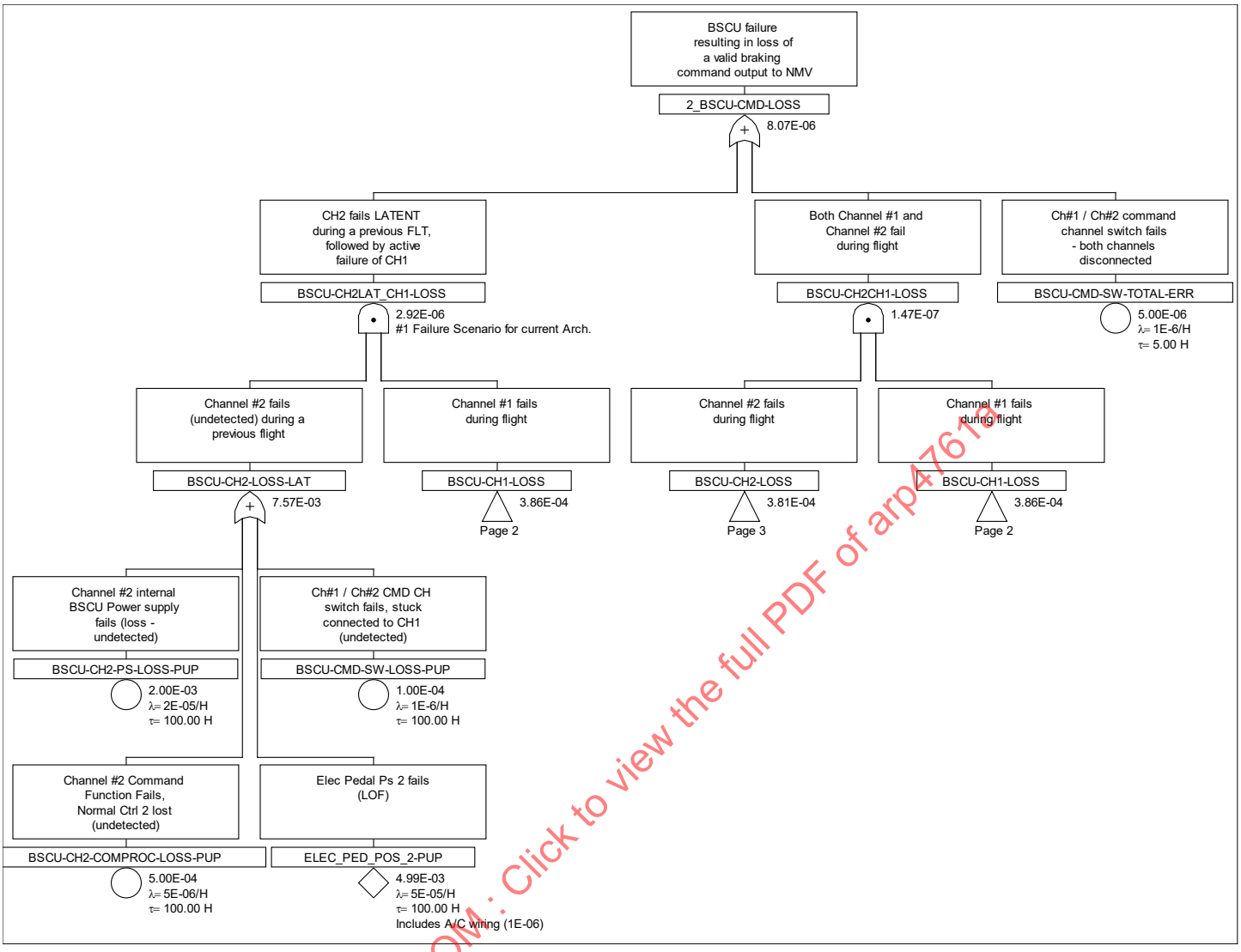


Figure Q.6-25 - (PSSA - BSCU - FTA)
BSCU update with 100-hour check (only first page shown)

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: Since the FTA indicates the need for proposed safety requirement to limit the exposure time, this requirement is identified in Q.6.4.3.5.)

Q.6.4.3.2.2 FTA: BSCU Provides Erroneous Output To NMV

The FTA for an erroneous output command from the BSCU is shown in Figure Q.6-26 through Figure Q.6-29. The FTA models two failure scenarios that could result in erroneous operation of the NMV. The first is erroneous operation of Channel #1, while the second is erroneous operation of Channel #2, after loss of operation of Channel #1.

Channel #1 could fail erroneous due to power supply operation outside its specified limits [BSCU-CH1-PS-ERR]. Channel #1 could also fail erroneous [BSCU-CH1-UND-ERR] if the command function failed erroneous and the monitor function failed to mitigate the failure. The exposure time of the monitor function is limited to power-up time (as a requirement has now been created limiting this exposure).

Channel #2 could fail in a similar manner if it were to become the channel controlling the NMV [BSCU-NMV-CH2-ERR]. Channel #2 would assume control in the event of a Channel #1 failure [BSCU-CH1TOCH2-CH1-FAIL] or the switch fails to the Channel #2 position [BSCU-CMD-SW-ERR]. The subtree for Channel #2 failing erroneous [BSCU2BADCM] is modeled similarly to Channel #1.

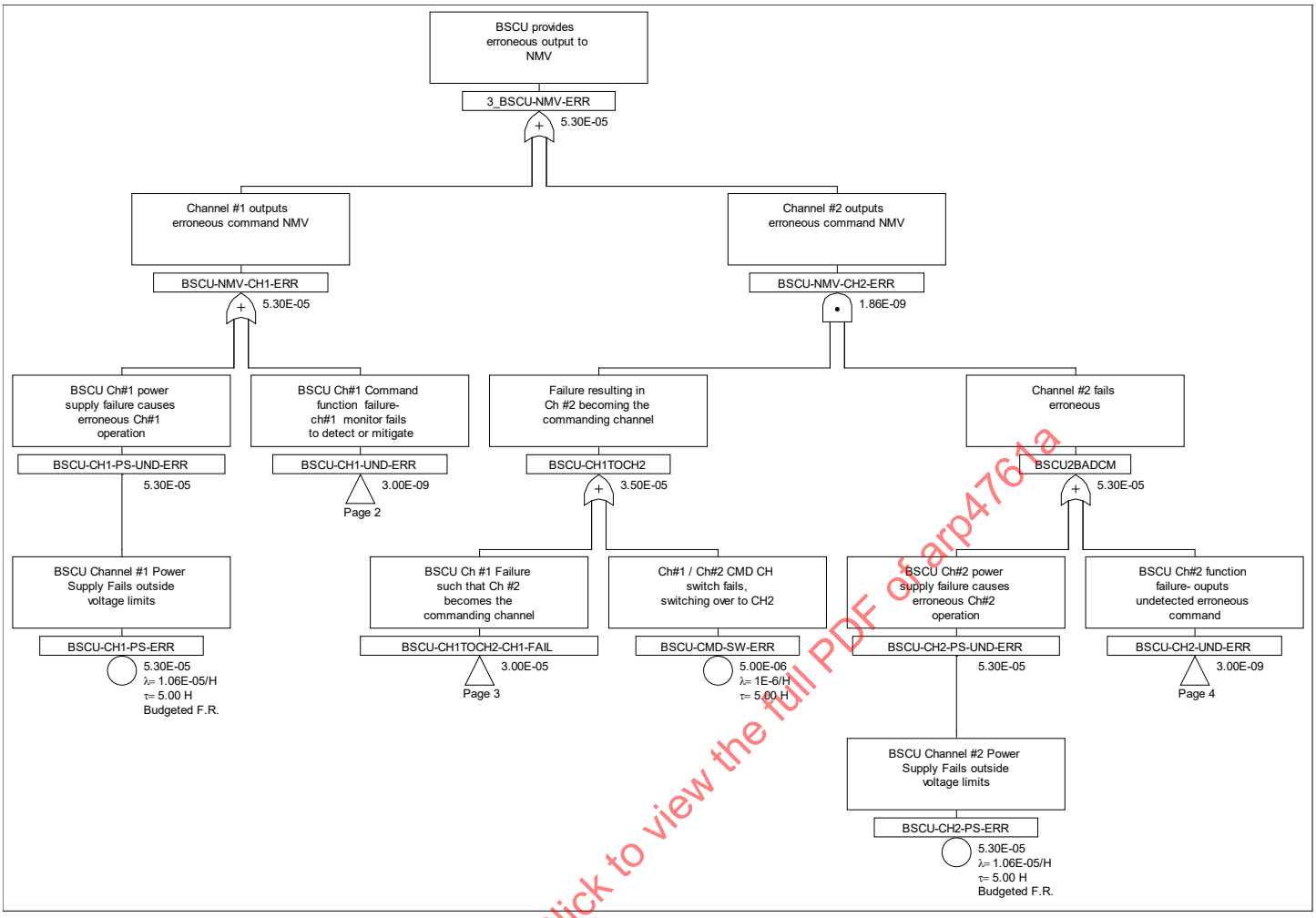


Figure Q.6-26 - (PSSA - BSCU - FTA)
BSCU update iteration: unannunciated erroneous braking command to the NMV (page 1 of 4)

SAENORM.COM : Click to view the full PDF of arp4761a

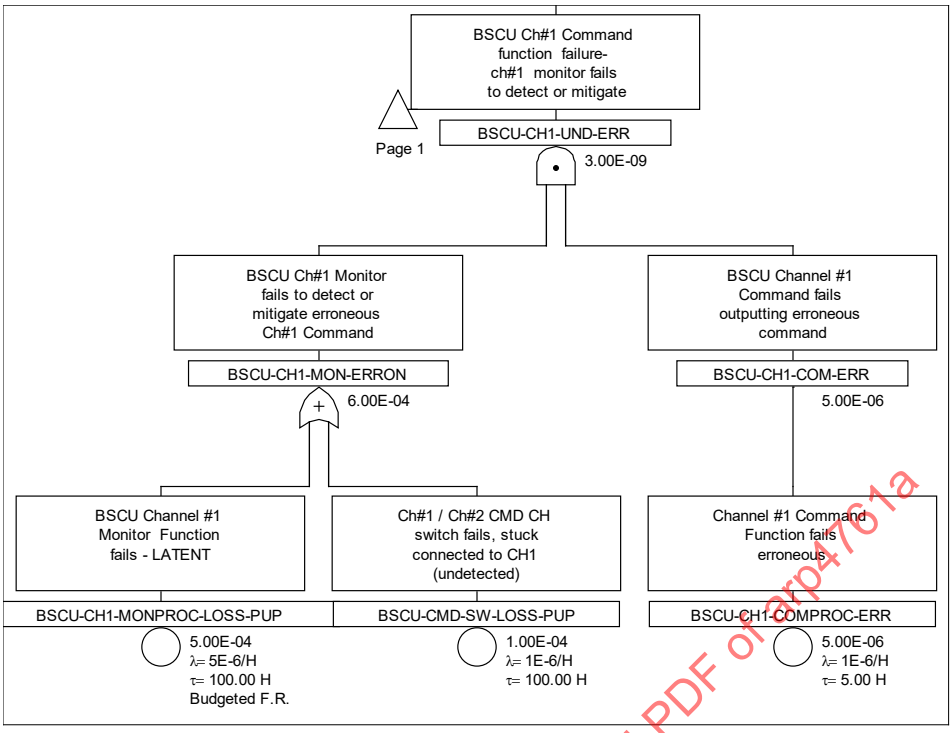
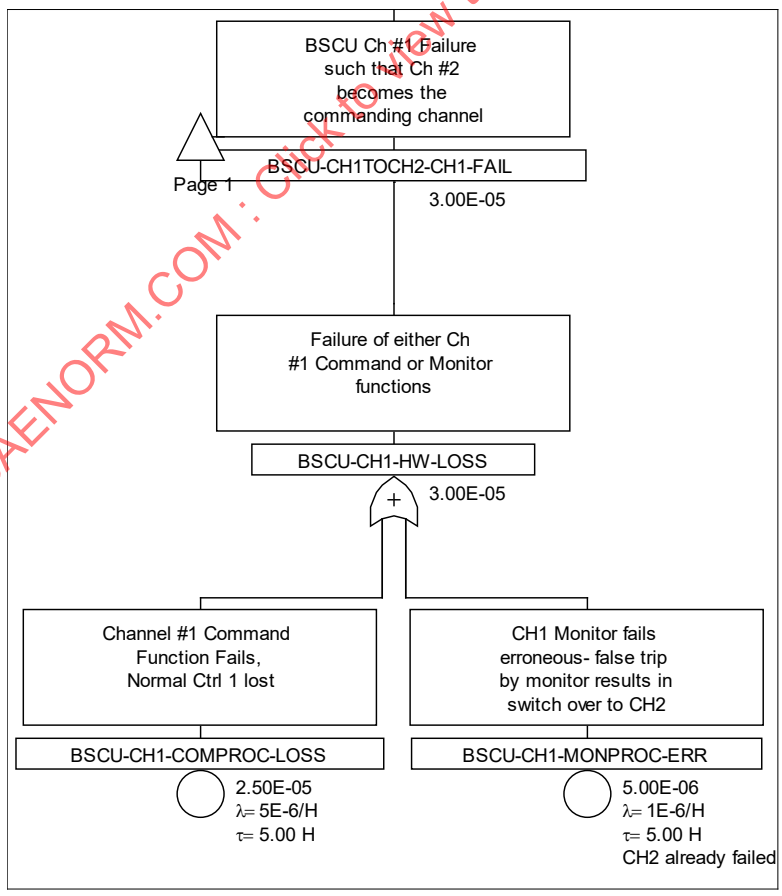


Figure Q.6-27 - (PSSA - BSCU - FTA)
BSCU update iteration: unannunciated erroneous braking command to the NMV (page 2 of 4)



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-28 - (PSSA - BSCU - FTA)
BSCU update iteration: unannunciated erroneous braking command to the NMV (page 3 of 4)

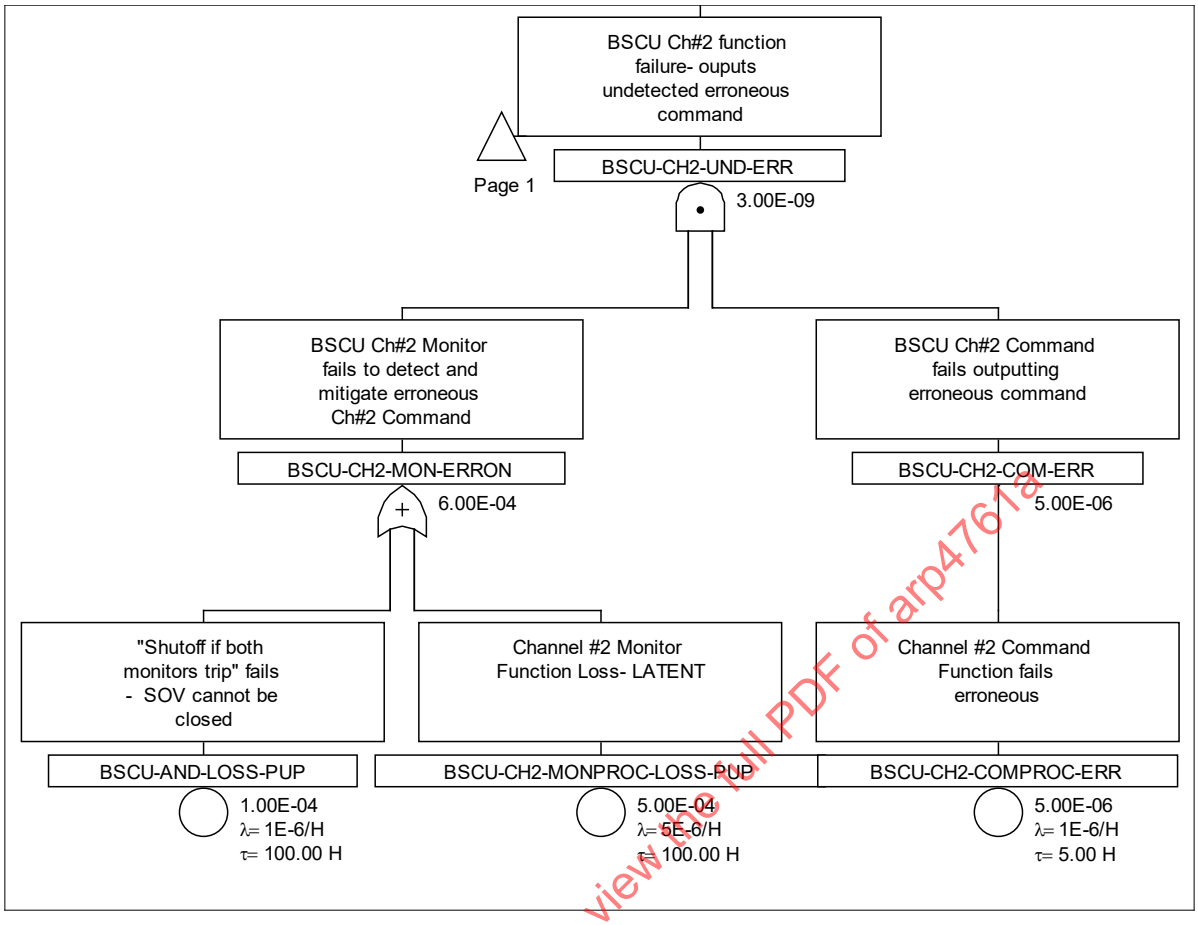


Figure Q.6-29 - (PSSA - BSCU - FTA)
BSCU update iteration: unannunciated erroneous braking command to the NMV (page 4 of 4)

(Editor's Note: Even though the presented FTA probability meets the 2.0E-04 per flight requirement, it was determined from analysis of the Catastrophic failure condition (1.1.MF1), not shown in this example, that a power supply monitor is required to mitigate erroneous operation.)

Since a power supply monitor was added during subsequent iterations, the first page of the final FTA is shown in Figure Q.6-30, which shows how the integration of the power supply monitors.

SAENORM.COM : Click to view the full PDF of arp4761a

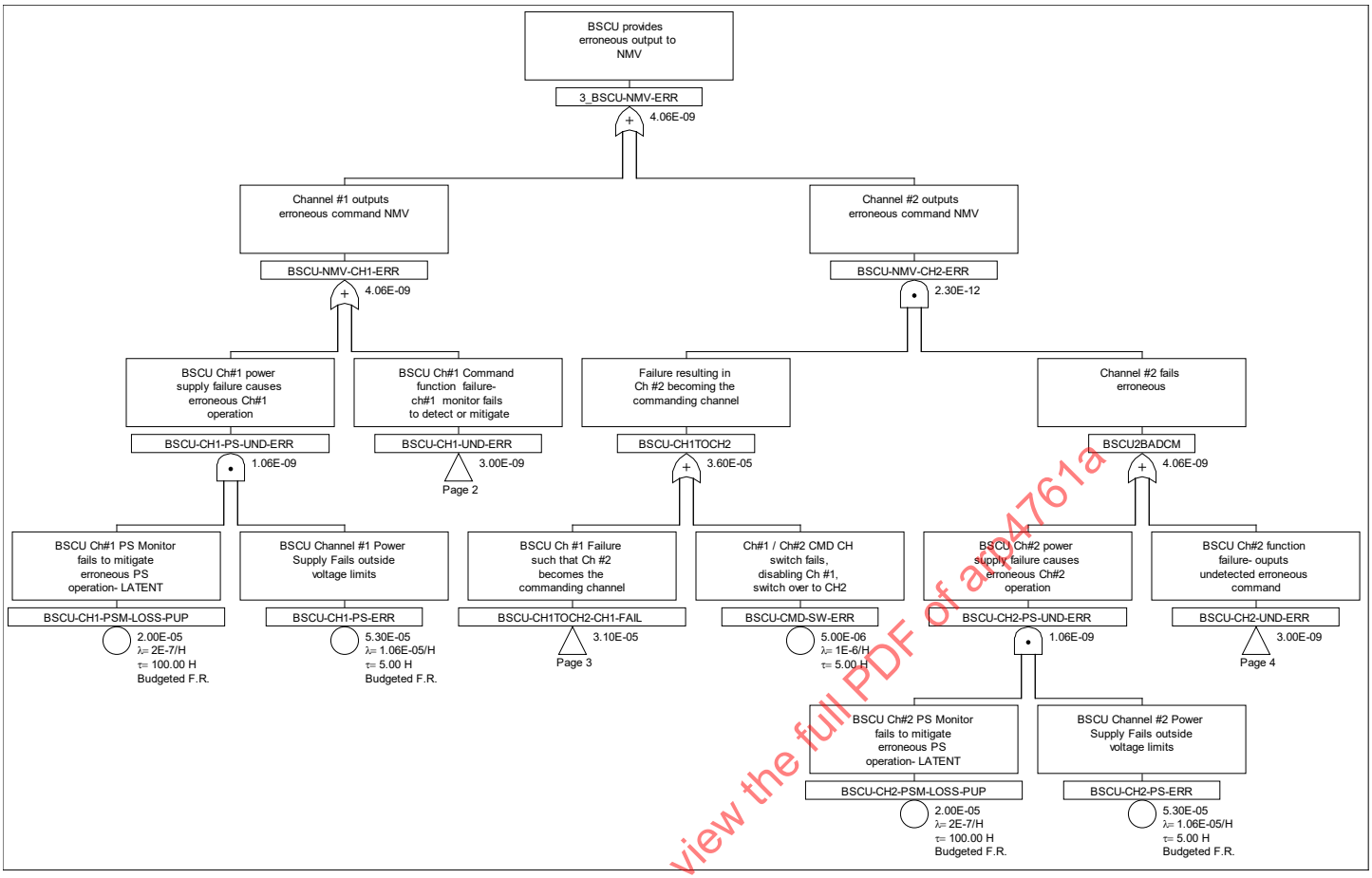
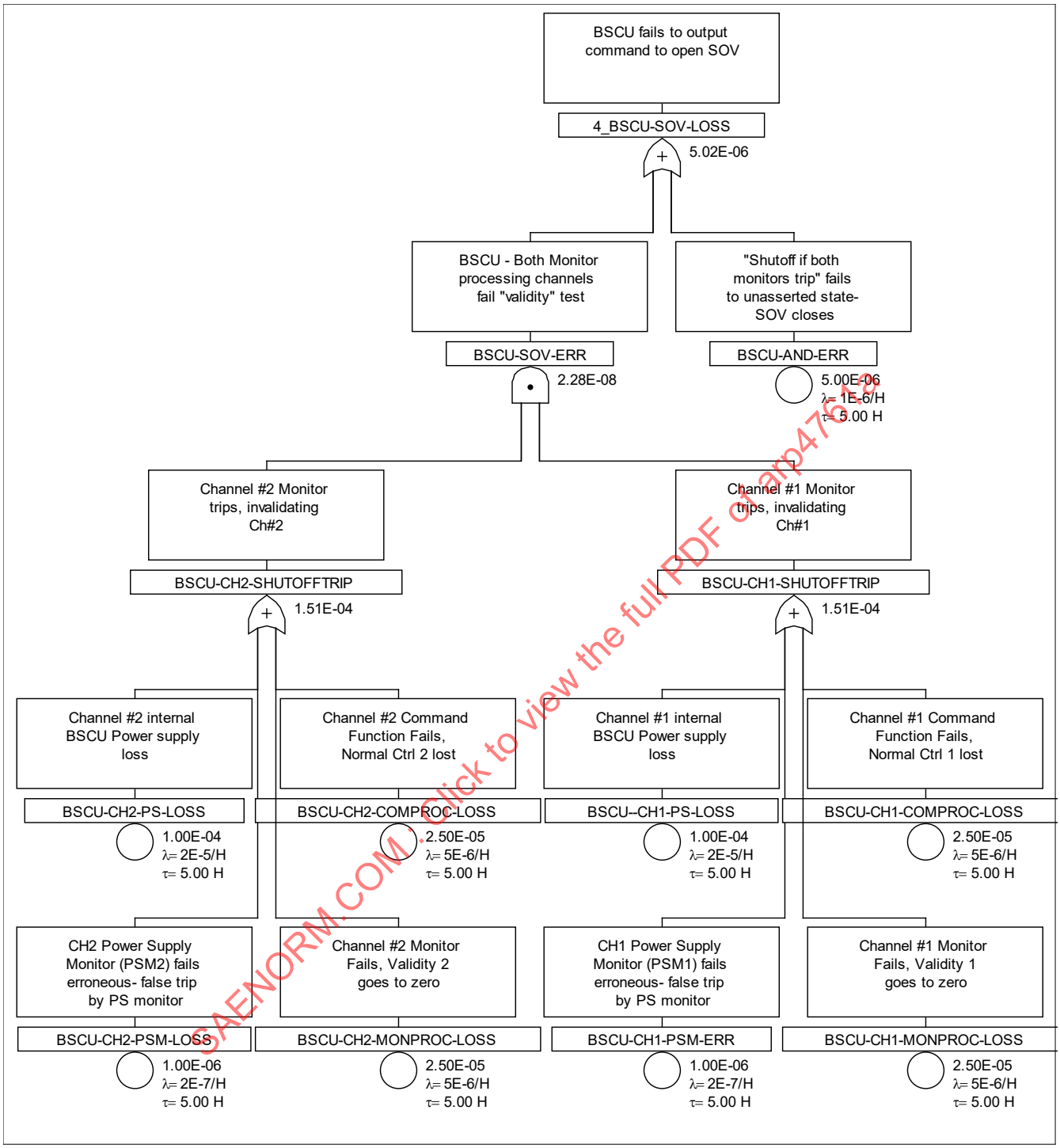


Figure Q.6-30 - (PSSA - BSCU - FTA)
Unannunciated erroneous braking command to the NMV (PS monitor added) (first page)

Q.6.4.3.2.3 FTA: BSCU Fails to Output Command to Open SOV

The fault tree for S18-BSCU-R-0004 “BSCU fails to output command to open SOV” is shown in Figure Q.6-31. The monitor logic will not command the SOV to the open position if either the monitor logic trips [BSCU-AND-FAIL] or if both channels of the BSCU fail “invalid” [BSCU-SOV-ERR]. For each channel, failure of any hardware element will result in that channel declaring itself as “invalid.”

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-31 - (PSSA - BSCU - FTA)
BSCU fails to output command to open SOV

The maximum exposure time used is flight time, as a monitor trip by either channel will result in a fault reported by the WBS, initiating a maintenance action. This was a design decision and is captured in the safety requirement BSCU-008 “Upon either Channel #1 or Channel #2 indicating a validity error, a WBS annunciation shall be output from the BSCU.”

The fault tree for S18-BSCU-R-0005 will be identical to that generated for S18-BSCU-R-0004, since unintended closure of the S/ASV requires either failure of both Channel #1 and #2, or a failure of the BSCU switching circuitry.

Q.6.4.3.3 Identify Latent Failures

Table Q.6-11 summarizes the latent failures that were identified in the FTA from Q.6.4.3.2.

Table Q.6-11 - (PSSA - BSCU - FTA)
Summary of fault tree latent failures

Basic Event Name	Description	Latency (Hours)
BSCU-CH2-PS-LOSS-PUP	Channel #2 internal BSCU Power supply fails (loss - undetected)	100
BSCU-CH2-COMPROC-LOSS-PUP	Channel #2 Command Function Fails, Normal Ctrl 2 lost (undetected)	100
BSCU-CMD-SW-LOSS-PUP	Ch#1 / Ch#2 CMD CH switch fails, stuck connected to CH1 (undetected)	100
ELEC_PED_POS_2-PUP	Elec Pedal Ps 2 fails (LOF)	100
BSCU-CH1-MONPROC-LOSS-PUP	BSCU Channel #1 Monitor Function fails - LATENT	100
BSCU-CH2-MONPROC-LOSS-PUP	Channel #2 Monitor Function Loss- LATENT	100
BSCU-CMD-SW-LOSS-PUP	Ch#1 / Ch#2 CMD CH switch fails, stuck connected to CH1 (undetected)	100
BSCU-CH1-PSM-LOSS-PUP	BSCU Ch#1 PS Monitor fails to mitigate erroneous PS operation - LATENT	100
BSCU-CH2-PSM-LOSS-PUP	BSCU Ch#2 PS Monitor fails to mitigate erroneous PS operation - LATENT	100
BSCU-AND-LOSS-PUP	"Shutoff if both monitors trip" fails - SOV cannot be closed	100

(Editor's Note: The latent failures listed in Table Q.6-11 were identified to the WBS through the PSSA process.)

Q.6.4.3.4 Identify Where Independence is Necessary

The Cut Set Analysis method is used here to develop requirements for independence. This may be used in place of the methods shown in Q.6.2.3.4. This is shown explicitly for the FTA shown in Figure Q.6-31. The cut sets identify where independence is necessary to support the qualitative model presented in the FTA.

The cut sets are usually generated using the same software used to generate the FTA model. The cut set listing is in order of decreasing probability, and shows the events or combinations of events (known as "cut sets") that contribute to the overall probability.

From Table Q.6-12 the first cut set containing two members models loss of the Channel 1 power supply and the Channel 2 power supply. In order for the model to be correct, both of the channel power supplies must be independent. That is, the operational state of power supply function is not affected in any way by the other. In a similar way, the next cut set requires independence between the Channel 1 power supply and the command channel switch. Many of the subsequent cut sets require independence between an element of Channel #1 and an element of Channel #2.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.6-12 - (PSSA - BSCU - FTA)
Cut sets for FTA BSCU-CMD-LOSS

Probability	Basic Event 1	Basic Event 2
5.00E-06	BSCU-AND-ERR	
1.00E-08	BSCU-CH1-PS-LOSS	BSCU-CH2-PS-LOSS
2.50E-09	BSCU-CH1-PS-LOSS	BSCU-CH2-COMPROC-LOSS
2.50E-09	BSCU-CH1-PS-LOSS	BSCU-CH2-MONPROC-LOSS
2.50E-09	BSCU-CH1-COMPROC-LOSS	BSCU-CH2-PS-LOSS
2.50E-09	BSCU-CH1-MONPROC-LOSS	BSCU-CH2-PS-LOSS
6.25E-10	BSCU-CH1-COMPROC-LOSS	BSCU-CH2-COMPROC-LOSS
6.25E-10	BSCU-CH1-COMPROC-LOSS	BSCU-CH2-MONPROC-LOSS
6.25E-10	BSCU-CH1-MONPROC-LOSS	BSCU-CH2-COMPROC-LOSS
6.25E-10	BSCU-CH1-MONPROC-LOSS	BSCU-CH2-MONPROC-LOSS
1.00E-10	BSCU--CH1-PS-LOSS	BSCU-CH2-PSM-LOSS
1.00E-10	BSCU-CH1-PSM-ERR	BSCU-CH2-PS-LOSS
2.50E-11	BSCU-CH1-COMPROC-LOSS	BSCU-CH2-PSM-LOSS

Using the cut sets shown in Table Q.6-12 and generating similar cut sets for the other FTAs, the BSCU Independence Principles shown in Table Q.6-13 are generated.

In addition, design analysis techniques are applied to the FDAL/IDAL assignment as developed in Q.6.4.3.1. Since Option 2 was selected, the need for an additional Independence Principle was evaluated related to the independence of the COMX and MONX software. It was determined that an Independence Principle already existed from the cut set method (i.e., within each channel, the command and monitor functions are independent).

Table Q.6-13 - (PSSA - BSCU)
BSCU Independence Principles

BSCU Independence Principle
Channel #1 is independent from Channel #2
Within each channel, the command and monitor functions are independent.
Within each channel the power supply and power supply monitor are independent.

(Editor's Note: PSSA would normally use a tailored version of the CMA questionnaire. This example uses a couple of checklist items to show the concept, there may be more checklist items evaluated when generating requirements for independence in an actual PSSA.)

The CMA questionnaire (Appendix M) is tailored to remove common failure or error source questions that do not apply to the BSCU such as hydraulics.

(Editor's Note: At the WBS level, common failure or error source questions related to hydraulics would be applicable.)

After each Independence Principle has been identified, the CMA questionnaire is utilized to identify the necessary independence requirements. If these requirements do not exist, the Safety process will identify the need for the requirements.

The Independence Principle "within each channel, the command and monitor functions are independent" is selected from the list above and applied to the tailored CMA questionnaire shown in Table Q.6-14.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.6-14 - (PSSA - BSCU - CMA)
CMA questionnaire for independence between command and monitor

Independence Principle: Within each channel, the command and monitor functions are independent		
Common Failure or Error Source	**Description of Effect on Principle**	**Description of Mitigating Factors or Lack of Independence**
Power source/supply malfunction?	Common power input source causes loss or erroneous operation of BSCU command and monitor functions within a channel.	Current model considers a common power source input to both command and monitor in each channel. This is modeled and determined to be numerically acceptable. However, the single power input into each channel approach may not support the Independence Principle between command and monitor, depending upon the BSCU internal power supply design. An additional requirement is needed to mitigate the common cause power input source effects on BSCU command and monitor lanes due to the designed response of the internal power supply. *(Editor's Note: This CMA mitigating factor drove the proposed requirements BSCU-004, BSCU-005 in Table Q.6-15.)*
Common functions used in power distribution system? Common components/piece-parts used in power distribution system?	Common electrical power source components/piece-parts (e.g., circuit breakers, relays, connectors) or inadequate BSCU grounding causes loss or erroneous operation of BSCU command and monitor functions.	Loss or erroneous power source input into each channel will be detected by independent power supply monitor resulting in Channel shutdown and activation of redundant BSCU channel. *(Editor's Note: This CMA mitigating factor drove the proposed requirement BSCU-004.)*
Power distribution cabling?	Common electrical power source wiring (external to BSCU or internal to BSCU) causes loss or erroneous operation of BSCU command and monitor functions.	
Common data sources	Common pedal position data sources cause loss or erroneous operation of BSCU command and monitor functions.	Redundant left and right brake pedal position signal inputs are separated into different connectors into channel 1 and 2. Position signals are then electrically isolated between channels 1 and 2 and between command and monitor lanes. *(Editor's Note: This is based on system functionality not modeled in the FTA. For brevity only the Left pedal inputs are modeled.)*
Processing	Loss or failure of BSCU common devices cause loss or erroneous operation of BSCU command and monitor functions.	Command and monitor functions implemented using physically independent and redundant interface and computing processing hardware.
Specification	Common BSCU specification errors or specification interpretation errors cause loss or erroneous operation of BSCU command and monitor functions.	Mitigation of common effects by BSCU FDAL Level A development process.

SAENORM.COM : Click to view the full PDF of arp4761a

Independence Principle: Within each channel, the command and monitor functions are independent		
Common Failure or Error Source	**Description of Effect on Principle**	**Description of Mitigating Factors or Lack of Independence**
Software development/design	Common command and monitor software functionality (same software design, common data packaging software routines, a software error common to both functions - software drivers) would defeat Independence Principle	Evaluation of BSCU command and monitor software requirement specification Items resulted in establishing that BSCU command lane and monitor lane software will sufficiently implement different designs using different requirements. This satisfies the item development independence attribute and supports the IDAL Level B assigned.
Hardware development/design	Common command and monitor functions implementations using the same hardware design, a common hardware error would defeat Independence Principle	Mitigation of common command and monitor hardware design errors will be through DO-254/ED-80 development assurance Level A.
Thermal	Common environmental failure could cause both Command and monitor to be lost or function erroneously, defeating independence.	BSCU to be developed and qualified through testing to continue normal operation in specified installed environments.

Q.6.4.3.5 Identify Necessary Proposed Safety Requirements

Table Q.6-15 shows additional proposed safety requirements that were identified during the BSCU PSSA process. The rationale ties the proposed requirement to the specific analysis (or portion of analysis) that indicates the need for the requirement. When characteristics at the WBS level are required to support the safety assessment in addition to the proposed requirement, an assumption is identified in Table Q.6-15 to be passed to the WBS level.

Table Q.6-15 - (PSSA - BSCU)
Proposed safety requirements

ID	Resulting Requirement	Rationale	Assumption to WBS Level
BSCU-001	Channel #1 shall have physical independence from Channel #2	CMA	N/A
BSCU-002	Within each channel, the command function shall have physical independence from the monitor function	CMA	N/A
BSCU-003	The COMX software and MONX software shall be developed using different software requirement specifications	CMA	N/A
BSCU-004	Within each channel, a power supply monitor shall shutoff the power supply when any voltage is detected to be out of specification	Required to limit impact of power supply failures. Figure Q.6-30, CMA	N/A
BSCU-005	Within each channel, the operational state of the power supply shall have no effect on the operational state of the power supply monitor	CMA	N/A
BSCU-006	Upon Channel #1 indicating an “invalid” state, Channel #2 shall command the “Normal Control” output	Required monitor response for redundant model in safety analysis to be valid. Channel #1 normally in control with Channel #2 as backup	N/A
BSCU-007	Upon both Channel #1 and Channel #2 indicating “invalid” states, the “HYD 1 Enable” output shall be disabled	Required monitor response, when both channels are failed	When “HYD 1 Enable” is disabled, the BSCU brake control outputs are not used

SAENORM.COM : Click to view the full PDF of arp4761a

ID	Resulting Requirement	Rationale	Assumption to WBS Level
BSCU-008	Upon either Channel #1 or Channel #2 indicating a validity error, a WBS annunciation shall be output from the BSCU	Required to limit exposure time of either Channel in an invalid state to flight time., Figure Q.6-31	A BSCU maintenance action will be initiated, if the WBS Status indicates a failure
BSCU-009	At power-up the BSCU shall perform a self-test of Channel #2 including the ability to switch control from Channel #1 to Channel #2	Required to limit exposure time of Channel #2 to 100 hours., Figure Q.6-25	N/A
BSCU-010	At power-up each channel of the BSCU shall implement a test of its power supply monitor	Required to limit exposure time of power supplies to 100 hours., Figure Q.6-25	N/A
BSCU-011	If the power-up test fails a WBS annunciation shall be output from the BSCU	Annunciation for self-test in BSCU-009, BSCU-010	A BSCU maintenance action will be initiated, if the WBS Status indicates a failure

(Editor's Note: Independence requirement (BSCU-001) could have been implemented using a different strategy to physical independence. Physical separation is one way to achieve physical independence.)

Q.6.4.4 PSSA BSCU Completion - BSCU Update Iteration

The proposed BSCU architecture is evaluated using the following PSSA completion checks. The analysis attributes considered are discussed in Section D.5.

a. The quantitative analyses in Q.6.4.3.2 show that the proposed system implementation architecture can reasonably be expected to satisfy the numerical requirements and safety objectives from Q.6.4.1.1.

b. The FDALs and IDALs for the functions and items implementing the system were assigned including a rationale to substantiate the assignment in Q.6.4.3.1.1 and Q.6.4.3.1.2.

c. Independence requirements between the functions and items were identified and are listed in Q.6.4.3.4.

d. The proposed safety requirements were identified in Q.6.4.3.5.

e. The development/design team has accepted all requirements identified by safety including FDAL and IDAL assignment.

f. The proposed architecture did not introduce additional failure conditions not included in the SFHA.

g. The relationship between the proposed safety requirements and the safety assessment are identified in Q.6.4.3.5.

h. No assumptions were received from lower-level PSSAs since BSCU is the lowest level.

i. Assumptions for independence of electrical power were identified and passed up to the WBS.

Q.6.4.5 PSSA BSCU Outputs - BSCU Update Iteration

Once accepted by the development process, proposed safety requirements generated from PSSA are captured in the BSCU's requirement set and identified as safety requirements.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.6.4.5.1 Outputs to WBS PSSA

Assumptions identified by the BSCU PSSA (Q.6.4.3.5) are passed back to the WBS PSSA, as shown in Table Q.6-16.

Table Q.6-16 - (PSSA - BSCU)
Assumptions to WBS level

Assumption to WBS Level
When “HYD 1 Enable” is disabled, the BSCU brake control outputs are not used.
A BSCU maintenance action will be initiated, if the WBS Status indicates a failure.

Q.6.5 WBS PSSA Update Based on BSCU PSSA

The BSCU results are passed back to the WBS which evaluates the results and incorporates any necessary changes into the WBS PSSA process.

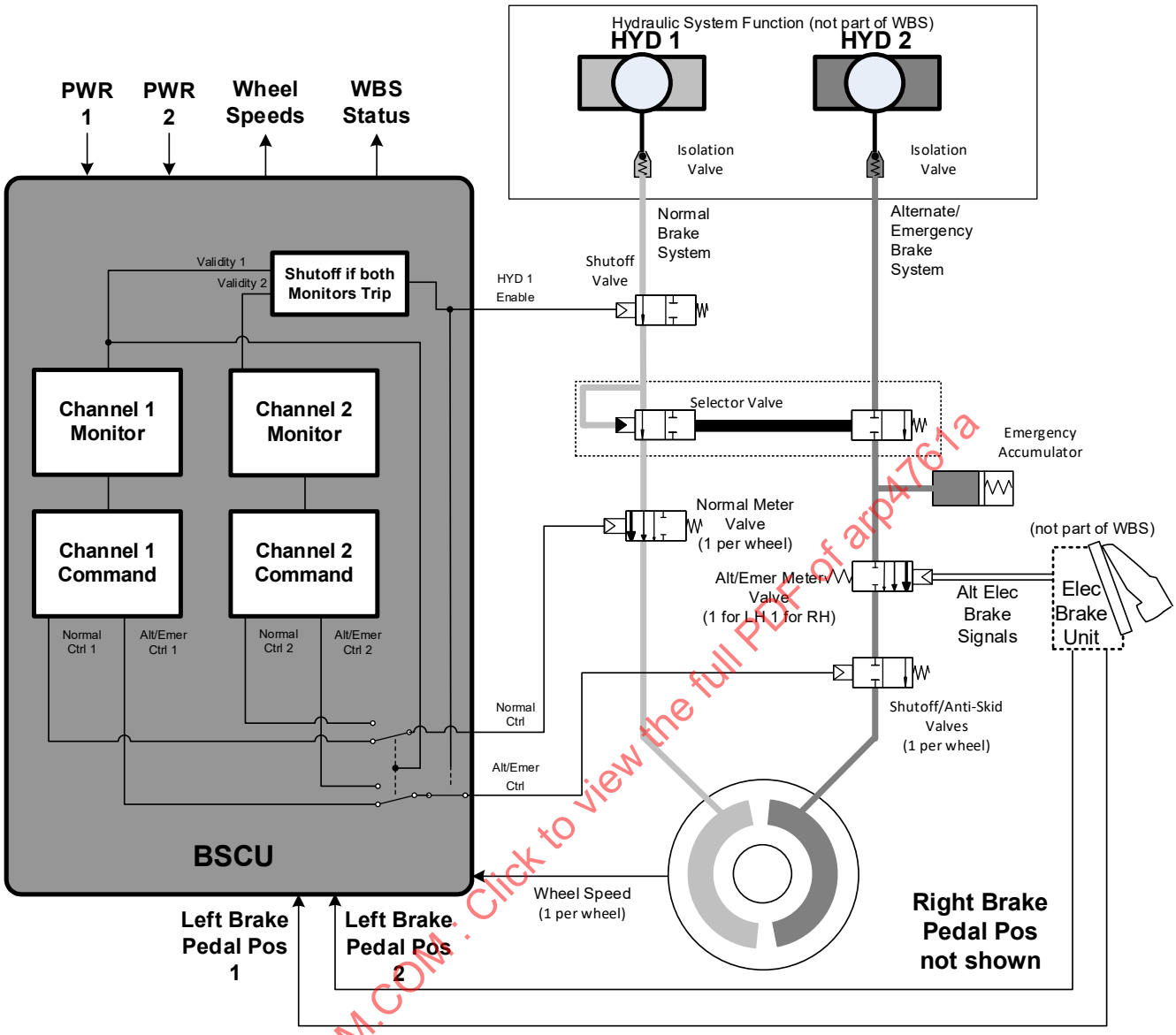
(Editor’s Note: The WBS receives the results of the BSCU PSSA including any assumptions and IDAL assignments.)

The BSCU supplier made an internal design decision that they need monitors for each command channel. The PSSA received from the BSCU supplier contains fault trees that model this implementation. The WBS updates the fault trees to include the results of the BSCU PSSA.

The BSCU supplier made a decision to assign IDAL = B to both command and monitor channel software. The WBS confirms that this assignment is acceptable since no assignment of FDALs was performed based on independence.

The WBS PSSA process confirmed that BSCU IDAL assignments are acceptable. There is no IDAL assignment at the BSCU level that violates the overall FDAL A at the WBS level. The WBS PSSA process also confirmed that a maintenance action is to be initiated if the WBS Status indicates a failure. The final architecture is shown in Figure Q.6-32.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.6-32 - (PSSA - WBS)
Final PSSA WBS architecture (NORMAL Mode: Channel 1 in control)

Q.6.5.1 WBS PSSA Completion

(Editor's Note: The following questions are stated in Appendix D, and together determine if the architecture can be reasonably expected to meet the safety objectives. These questions and answers are stated here to illustrate the associated thought process, but do not need to be captured in PSSA documentation.)

The proposed WBS architecture is evaluated using the following PSSA completion checks. The analysis attributes considered are discussed in Section D.5.

a. The quantitative analyses in Q.6.2.3.2 show that the proposed system implementation architecture can reasonably be expected to satisfy the numerical requirements and safety objectives in Q.6.2.1.

   (Editor's Note: Since the BSCU PSSA shows that it meets the allocated requirements, there were no resulting changes at the WBS level.)

b. The FDALs for the functions implementing the system were assigned including a rationale to substantiate the assignment in Q.6.2.3.1.

c. Independence requirements between the functions were identified and captured in Q.6.2.3.5.

d. The proposed safety requirements were identified in Q.6.2.3.5.

e. The development team has accepted all requirements identified by safety.

f. The proposed architecture did not introduce additional failure conditions not included in the SFHA.

g. The relationship between the proposed safety requirements and the safety assessment are identified in Q.6.2.3.5.

h. The assumptions from the BSCU PSSA were confirmed per ARP4754B/ED-79B, Appendix E.

i. Assumptions are captured in Q.6.2.5.

j. Derived requirements reviewed per ARP4754B/ED-79B, Appendix E.

Q.6.5.2 PSSA Outputs

Q.6.5.2.1 Capturing PSSA Process Data

Once accepted by the development process, proposed safety requirements generated from PSSA are captured in the WBS's requirement set and identified as safety requirements.

(Editor's Note: Even though this update to the WBS PSSA process was not fully developed here, similar artifacts would be captured.)

Q.6.5.2.2 Outputs to PASA

The PSSA process output data discussed in Q.6.5.2.1 are provided to the PASA process. The following information is highlighted here to illustrate the connectivity between the PASA and PSSA processes.

Previously identified assumptions which were provided to the airplane level are repeated here for clarity (Q.6.2.5):

a. The probability of "Loss of Normal Braking System Hydraulic Components" will be less than 3.3E-05 per flight.

b. The probability of "Loss of Alternate Braking System Hydraulic Components" will be less than 3.3E-05 per flight.

c. The probability of seven or more wheel speed sensors erroneous or inoperative will be less than 1.0E-07 per flight.

d. The probability of loss of an airplane electrical power bus will be less than 1.0E-04 per flight.

e. The probability of loss of a Left brake pedal position input will be less than 1.0E-06 per flight.

f. Airplane electrical power bus 1 is independent from airplane electrical power bus 2.

g. HYD 1 hydraulic system is independent from HYD 2 hydraulic system.

(Editor's Note: As f. and g. are PASA requirements it is not necessary to provide them as assumptions, though it may be a good practice to do so for confirmation.)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.7 S18 AIRPLANE - BRAKE SYSTEM CONTROL UNIT (BSCU) DEPENDENCE DIAGRAM (DD) EXAMPLE

DD Example

Q.7.1 DD Example Introduction

This section presents the Brake System Control Unit (BSCU) Dependence Diagram (DD) analysis example for the S18 airplane. The results from the BSCU DD analysis may be used in the WBS SSA as an alternative means to the FTA currently used in the WBS SSA example (see Section Q.13).

(Editor's Note: For the sake of brevity, only the requirements needed to support the WBS SSA example - Section Q.13 are developed in detail for this BSCU DD example. Other requirements could be assessed by the same method shown here.)

(Editor's Note: This example is not intended to standardize the format of a DD report. The intent of this example is to show an example DD analysis that could be part of the BSCU SSA process.)

Q.7.2 Summary of BSCU DD Results

Table Q.7-1 summarizes the dependence diagram results for the BSCU requirements identified.

Table Q.7 1 - (SSA - BSCU - DD)
BSCU DD results summary

ID	BSCU Allocated Requirement	Allocation (/flight)	Result (/flight)	Figure Reference
S18-BSCU-R-0002	The probability of BSCU failure resulting in loss of a valid braking command output to the NMV shall not exceed 2.0E-04 per flight.	2.0E-04	8.07E-06	Q.7-1 and Q.7-2
S18-BSCU-R-0003	The probability of BSCU failure resulting in unannunciated erroneous braking command to the NMV shall not exceed 2.0E-04 per flight.	2.0E-04	3.76E-09	Q.7-3 and Q.7-4
S18-BSCU-R-0004	The probability of BSCU failure resulting in the loss of command to open the SOV (resulting in permanent non-conducting state of SOV) shall not exceed 2.0E-04 per flight.	2.0E-04	5.02E-06	Q.7-5
S18-BSCU-R-0005	The probability of BSCU failure resulting in unintended closure of the S/ASV (resulting in non-conducting state of S/ASV) shall not exceed 2.0E-04 per flight.	2.0E-04	5.02E-06 (See Note 1)	Q.7-5

Note 1: The DD analysis for S18-BSCU-R-0005 will be identical to that generated for S18-BSCU-R-0004, since unintended closure of the Shutoff/Anti-Skid Valve requires either failure of both Channel #1 and #2, or a failure of the BSCU switching circuitry.

SAENORM.COM : Click to view the full PDF of arp4761a

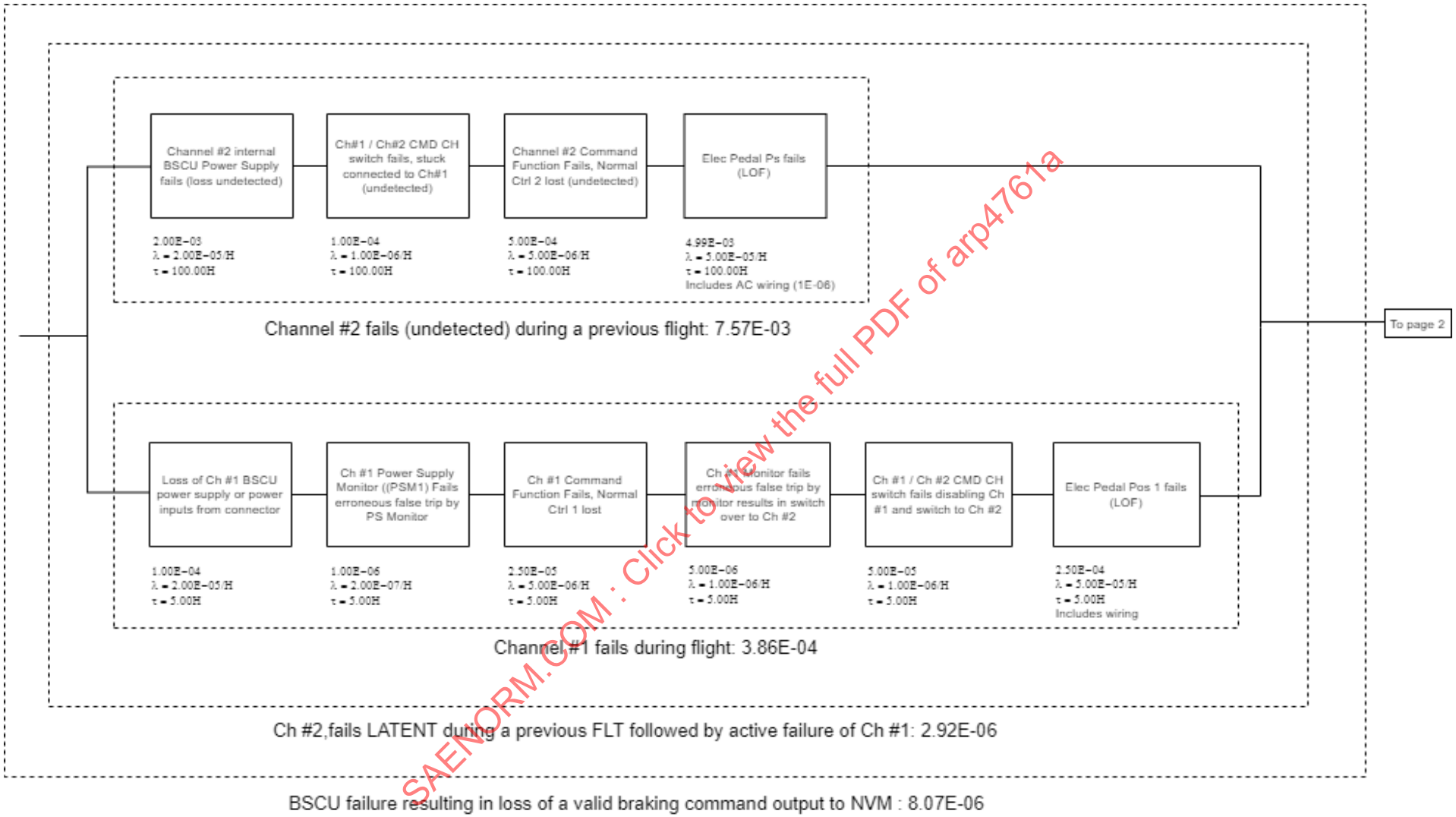
Q.7.3 BSCU DD Detail

The following sub-sections detail the DD performed for the BSCU. Failure rates for each event in the DDs were sourced from reliability predictions and the BSCU FMEA.

(Editor's Note: For brevity, not all the failure rates shown in the FTAs have an identifiable source within this example.)

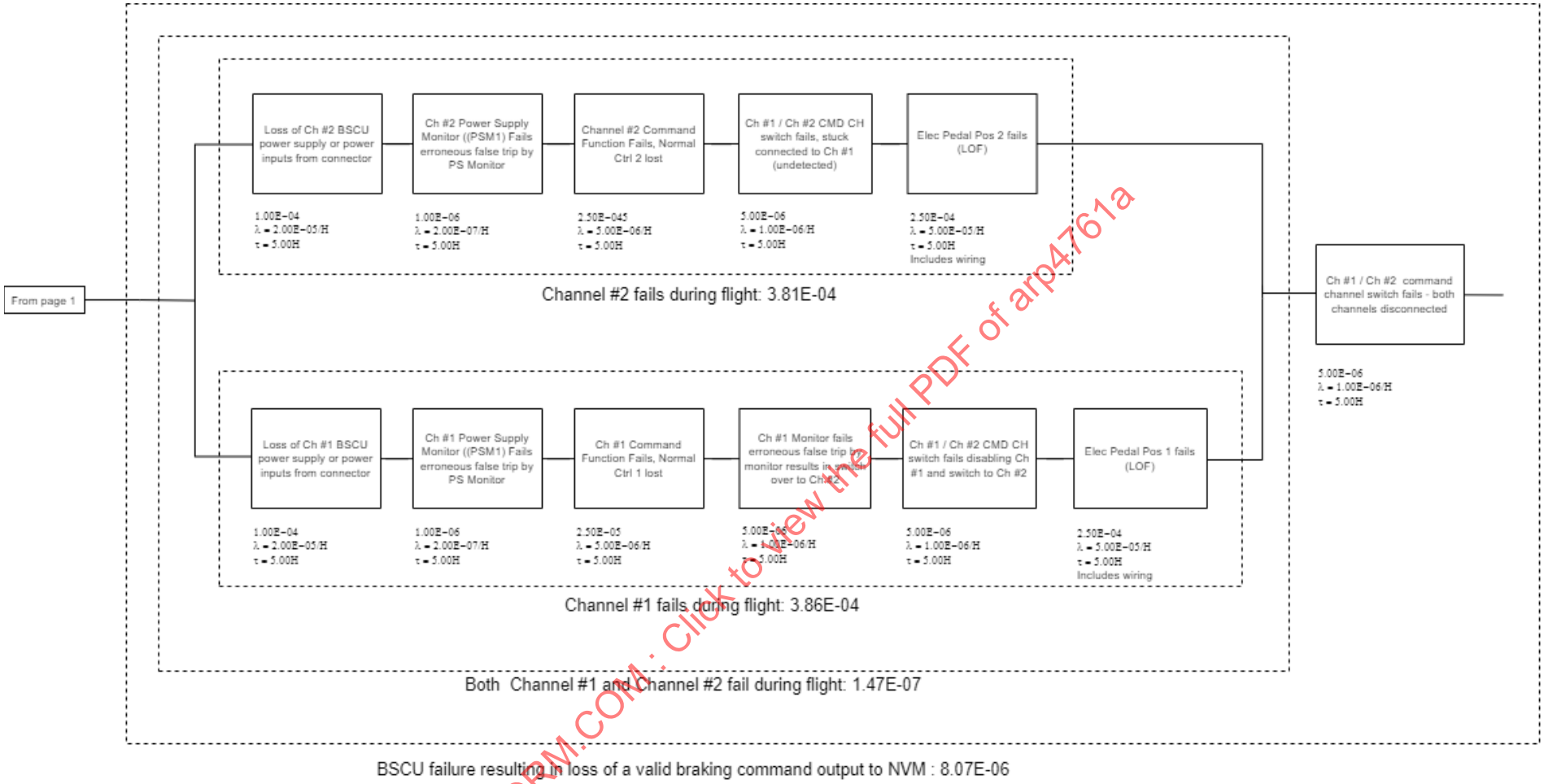
Q.7.3.1 BSCU Loss of Normal Braking Command to Normal Meter Valve

Figures Q.7-1 and Q.7-2 show the DD for S18-BSCU-R-0002, loss of a valid braking command output to the Normal Meter Valve (NMV). This analysis uses a 100hr check time based on the power-on test that checks Channel #2 is working.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.7-1 - (SSA - BSCU - DD)
Loss of normal braking command to NMV from BSCU (page 1)



SAENORM.COM : Click to view the full PDF of arp4761a

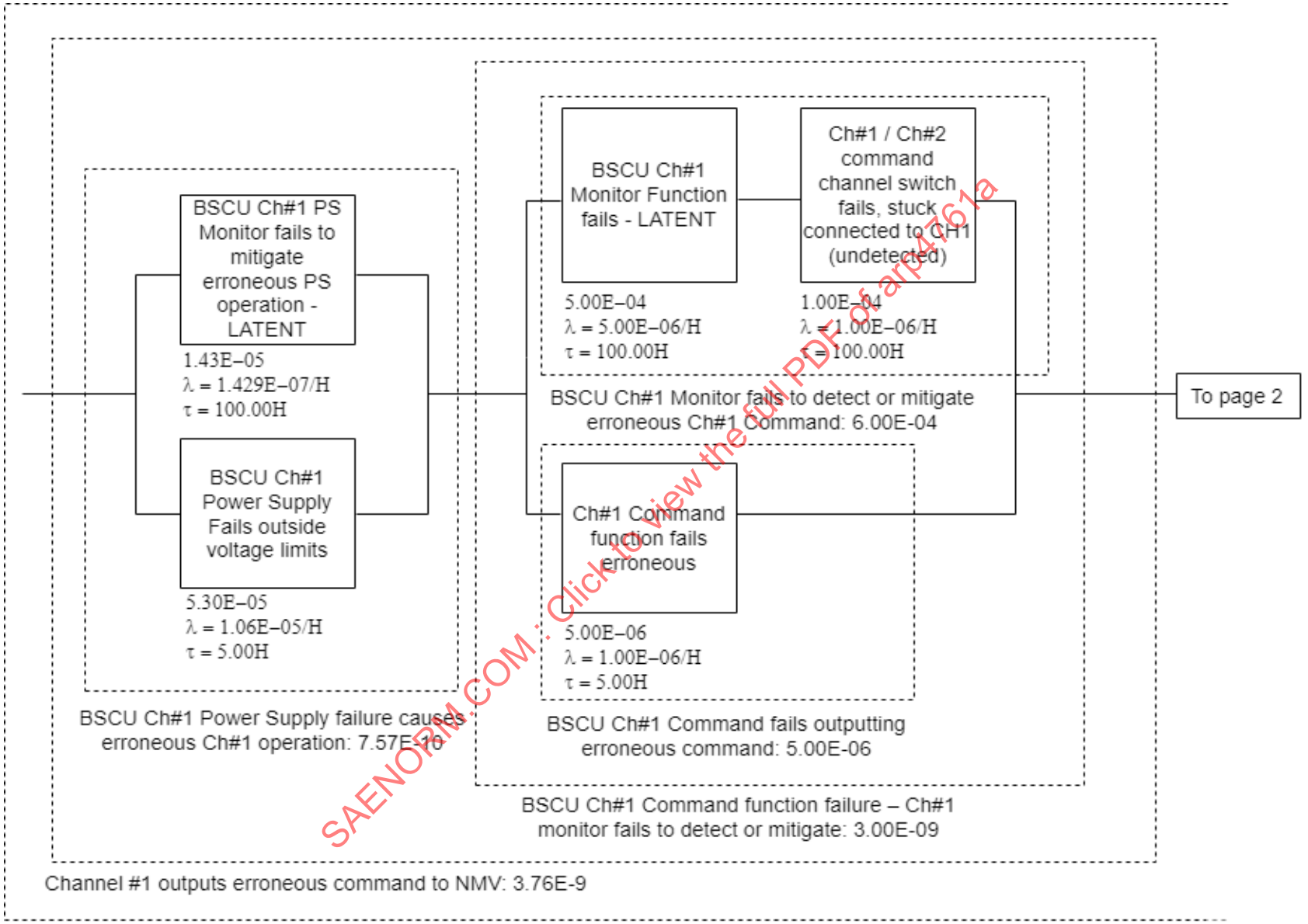
Figure Q.7-2 - (SSA - BSCU - DD)
Loss of normal braking command to NMV from BSCU (page 2)

Q.7.3.2 BSCU Provides Erroneous Output to Normal Meter Valve - Inadvertent

Figure Q.7-3 and Q.7-4 show the DD for S18-BSCU-R-0003, BSCU provides an unannunciated, erroneous braking command to the NMV. This analysis uses a 100-hour check time for the power supply monitor based on the power-on test that verifies the monitor is working.

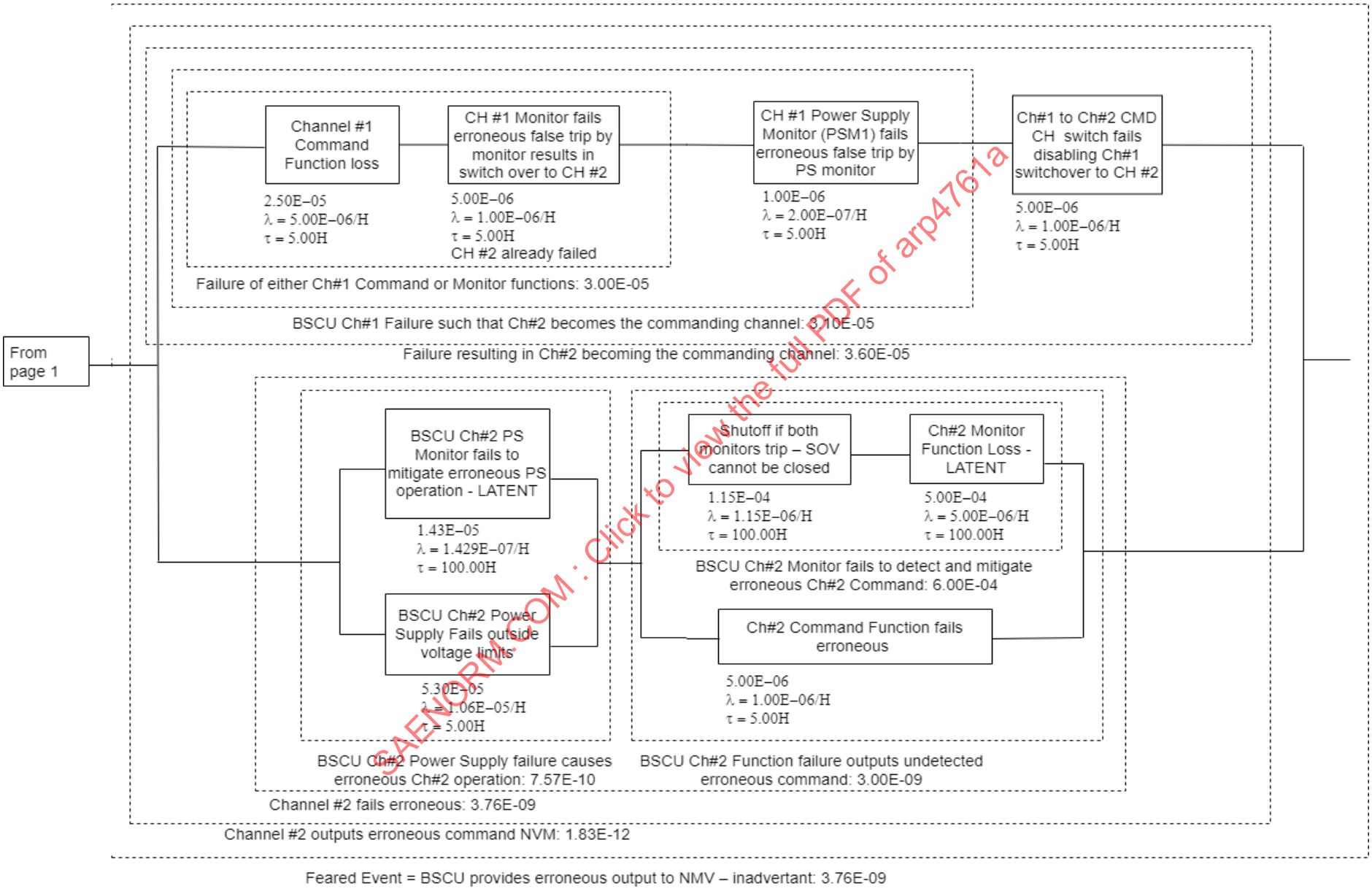
Q.7.3.3 BSCU Fails to Output Command to Open Shutoff Valve

Figure Q.7-5 shows the DD for S18-BSCU-R-0004, BSCU fails to output command to open Shutoff Valve (SOV). This DD is also applicable to S18-BSCU-R-0005, unintended closure of the Shutoff/Anti-Skid Valve.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.7-3 - (SSA - BSCU - DD)
BSCU provides erroneous output to NMV: inadvertent (page 1)



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.7-4 - (SSA - BSCU - DD)
BSCU provides erroneous output to NMV: inadvertent (page 2)

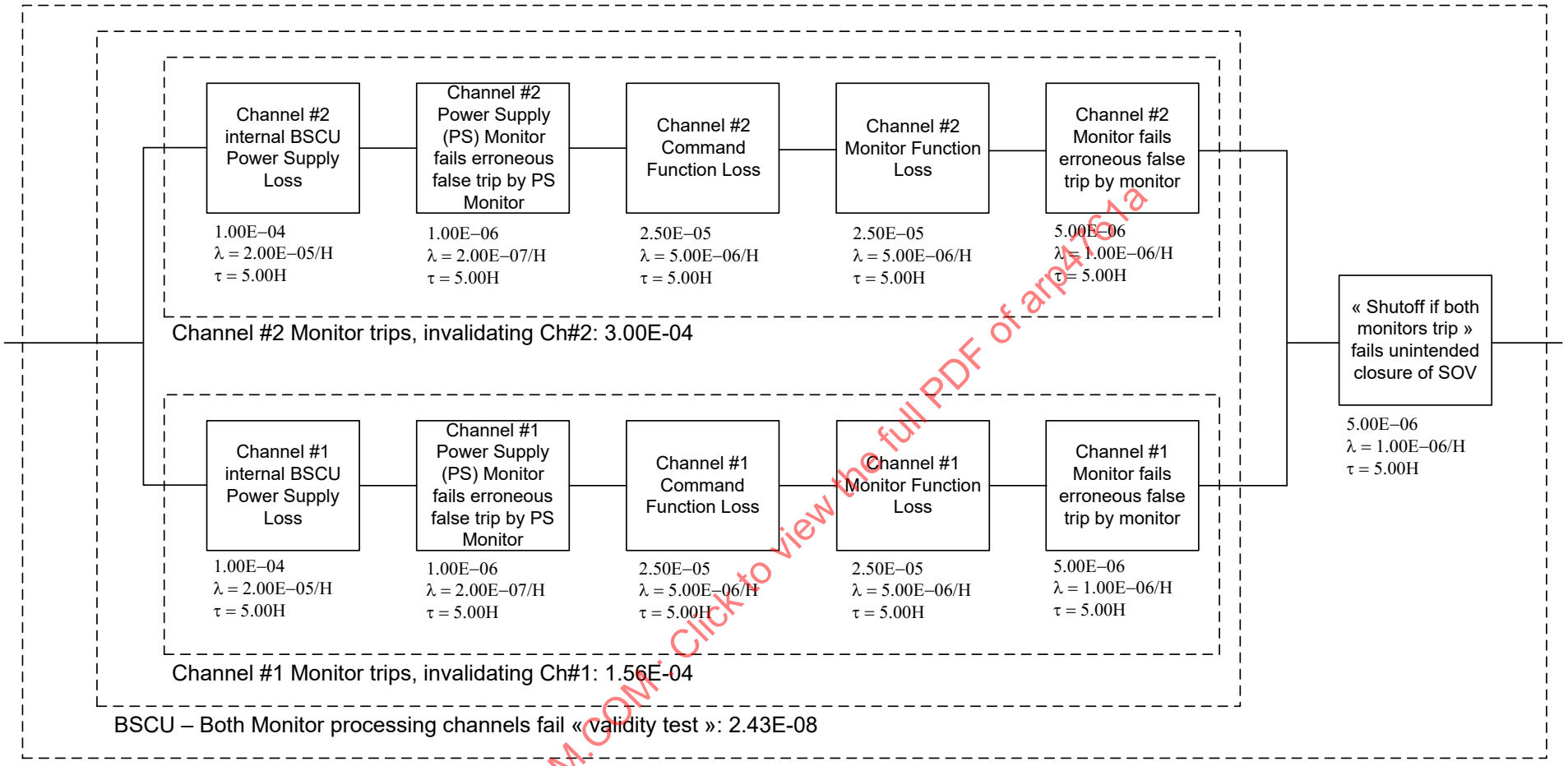


Figure Q.7-5 - (SSA - BSCU - DD)
BSCU fails to output command to open SOV

SAENORM.COM : Click to view the full PDF of arp4761a

Q.8 S18 AIRPLANE - MARKOV ANALYSIS (MA) EXAMPLE

MA Example

Q.8.1 MA Example Introduction

This appendix section models the Wheel Brake System (WBS) PSSA failure conditions (modeled in Section Q.6 using FTA) using Markov Models (MM). The goal of this section is to show that Markov Analysis (MA) is an equivalent technique to FTA and produced the same failure probability for failure conditions considering the same system failure behavior, failure events, failure rates and exposure times.

(Editor's Note: The MA appendix (Appendix I) details the basic theory of MMs and shows the power of MA in modeling time dependent fault-tolerant systems with or without different type of repairs. The MA while capturing time-dependent behavior also improves accuracy of the latent events calculations while reporting the average probability per flight results.)

Q.8.2 Background

Appendix I shows examples with MM drawings, and their respective equations were solved using analytical methods or by using spreadsheets. For modeling complex systems with several events such an approach can be infeasible as the number of states of the MM increase. One needs software tools that can take system architecture description and/or failure logic in order to automatically generate MM and solve their equations. This is similar to using an FTA software tool such as the one used in Appendix G which shows simple FTA examples with the Boolean algebra and probability calculations. It should be noted that the MA shown here are helping to verify the WBS quantitative safety requirements, "no single failure" requirements or Functional Failure Sets (FFS) used for FDAL/IDAL assignments.

Q.8.3 Markov Analysis Steps

This example shows the MM for the WBS failure condition (FC) and related safety requirements considered in Q.6, failure condition for the WBS (FC ID: 1.1.TL1.A) and three safety requirements for BSCU (S18-BSCU-R-0002, S18-BSCU-R-0003, S18-BSCU-R-0004). The analysis assumes average flight length of 5 hours. The final updated architecture in Q.6 with two independent BSCU channels with command and monitor is modeled here. An exposure time (repair time) of 100 hours (20 flights) is used for the BSCU latent failure events.

In each of the following MM, the following sequence of results are shown.

First an event table is shown which highlight the mapping of MM event name against the FTA basic event, and its failure rate and exposure time so it is easy to correlate to the FTA in Q.6. Note that each basic event in the FTA is considered in the MM. This can lead to a large state space as shown in the examples below. In a traditional hand-crafted MM, to minimize the extent of state space, the analyst may collect many failure events together into a single event (for example BSCU Channel 1 failure events with the same exposure time can be combined into a single event by summing the event failure rates). Such model simplification is possible even in the FT models as shown in Section Q.6 (e.g., combining events under OR-gates and compressing cascading OR-gates). But in the following examples since a tool that automatically generates the MM is used, such simplification is not attempted. Using this approach enables a comprehensive comparison of FTA and its MM model.

Next the MM state space is shown as a table (this is equivalent to the circles or bubbles shown in the MM diagram in Appendix I) which shows the state vector for each state (a "0" in a state for an event indicates the failed state of the event in that MM state). The rows corresponding to system failure states are highlighted in yellow. Note that in these examples there are as many system failure states as there are events. In Appendix I the system failure state is a single state but, in the examples, here the failure states are grouped by the last event failure which transitions from a system operational state to a system failed state. All these failure states could be aggregated (grouped) into one system failure state as in Appendix I, but it will not change the total system failure probability results and there are advantages to different types of aggregation of states. The MM generation tool uses a grouping by last event failure state.

SAENORM.COM : Click to view the full PDF of arp4761a

Next a table of transitions between states with a row for each transition from one state to another is shown (Each row corresponds to one failure “arc” or “arrow” in the MM diagram in Appendix I). The rows highlighted in the table represent transitions to system failure (they also have the “LAMBDA*X” type rate symbol). The repair arcs are not explicitly shown as the MM engine models repair events as discrete states. The repair arcs are assumed to restore the active events at the end of each flight and latent events at the end of their latency period (20 flights) from a state where they are failed (“0” in the state vector) to the state where they are operational (“1” in the state vector). This is similar to the transient analysis spreadsheet examples in Appendix I (e.g., Table I4). The transient analysis method using discrete repair is the most accurate and realistic method and is used by the software tool.

Finally, the results from the transient analysis of the MM are shown as a table of system failure probabilities at the end of each flight. A sample of 10 flights for the cases of no latent events and 100 flights (500 hours) for latent events is used to show the difference between the effect of latent events or lack thereof. For the MM with latent events, the results show the time dependent nature of risk and the average probability per flight. The average probability analysis is a standard feature of transient analysis using MM.

In all cases, it shows that the probability of failure matches the FTA results in Section Q.6. It should be noted that for the MM with latent events the peak flight risk will match the FTA result as the FTA in Section Q.6.

Q.8.4 Summary of WBS MA Results for Failure Condition: Total Loss of Wheel Deceleration (80% or More)

Tables Q.8-1 to Q.8-4 and Figure Q.8-1 summarize the Markov analysis results for the failure condition: Total loss of wheel deceleration (80% or more).

Table Q.8-1 - (PSSA - WBS - MA)
Markov Model event table

Event	PSSA FT Basic/Developed Event	Failure Rate Symbol	Failure or Occurrence Rate (per FH)	Exposure Time (Repair Time) (FH)
Pedal1	WBS-PDL1-LOSS	LAMBDA1	1.00E-06	5
Pedal2	WBS-PDL2-LOSS	LAMBDA2	1.00E-06	5
Power1	WBS-PWR1-LOSS	LAMBDA3	1.00E-04	5
Power2	WBS-PWR2-LOSS	LAMBDA4	1.00E-04	5
BSCUCmd	WBS-BSCU-CMD-LOSS	LAMBDA5	4.00E-05	5
BSCUErr	WBS-BSCU-ERR	LAMBDA6	4.00E-05	5
BSCUSov	WBS-BSCU-SOV-LOSS	LAMBDA7	4.00E-05	5
WhlSpdSens	WBS-BSCU-WHEEL-SEN-LOSS	LAMBDA8	2.00E-08	5
Hyd1	WBS-HYD1-LOSS	LAMBDA9	6.60E-06	5
Hyd2	WBS-HYD2-LOSS	LAMBDA10	6.60E-06	5
SOV	WBS-SOV-LOSS	LAMBDA11	1.00E-06	5
SelVlvOpn	WBS-SELVALVE-OPEN-LOSS	LAMBDA12	1.00E-06	5
MultNmvBrk	WBS-MULTNMV-LOSS	LAMBDA13	2.00E-07	5
SelVlvCls	WBS-SELVALVE-CLOSED-LOSS	LAMBDA14	1.00E-06	5
LHBkVlv	WBS-LH-BACKUPVALVE-LOSS	LAMBDA15	2.00E-06	5
RHBkVlv	WBS-RH-BACKUPVALVE-LOSS	LAMBDA16	2.00E-06	5
BSCUAskid	WBS-BSCU-AS-ERR	LAMBDA17	4.00E-05	5
AskidVlv	WBS-ASV-LOSS	LAMBDA18	1.00E-06	5

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.8-2 - (PSSA - WBS - MA)
WBS Markov Model state space table

Event Status (1= Event Not Occurred; 0= Event Occurred)																		
State #	Pedal1	Pedal2	Power1	Power2	BSCUCmd	BSCUErr	BSCUSov	WhlSpdSens	Hyd1	Hyd2	SOV	SelVlvOpn	MultNmvBrk	SelVlvCls	LHBkVlv	RHBkVlv	BSCUAskid	AskidVlv
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
8	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
9	Failure State Due to Last Failure of WhlSpdSens																	
10	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
… …																		
26	0	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
27	Failure State Due to Last Failure of Hyd2																	
28	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1
29	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1
30	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
31	Failure State Due to Last Failure of SelVlvCls																	
32	Failure State Due to Last Failure of LHBkVlv																	
33	Failure State Due to Last Failure of RHBkVlv																	
34	Failure State Due to Last Failure of BSCUAskid																	
35	Failure State Due to Last Failure of AskidVlv																	
36	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
… …																		
89	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1
90	Failure State Due to Last Failure of Pedal1																	
91	Failure State Due to Last Failure of Pedal2																	
92	Failure State Due to Last Failure of BSCUCmd																	
93	Failure State Due to Last Failure of BSCUErr																	
94	Failure State Due to Last Failure of BSCUSov																	
95	Failure State Due to Last Failure of Hyd1																	
96	Failure State Due to Last Failure of SOV																	
97	Failure State Due to Last Failure of SelVlvOpn																	
98	Failure State Due to Last Failure of MultNmvBrk																	
99	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1
… …																		
222	1	1	0	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1
223	Failure State Due to Last Failure of Power2																	
224	1	1	0	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1
… …																		
259	1	1	1	0	1	1	1	1	0	1	1	1	0	1	1	1	1	1
260	Failure State Due to Last Failure of Power1																	
261	1	1	1	0	1	1	1	1	1	0	1	1	1	0	1	1	1	1
… …																		
2255	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1	1	1	1

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: The total number of states in MM = 2255 including 18 system failure states; for brevity, not all states shown. Highlighted rows show transition from operational to a failure state.)

Table Q.8-3 - (PSSA - WBS - MA)
Markov Model state transitions table

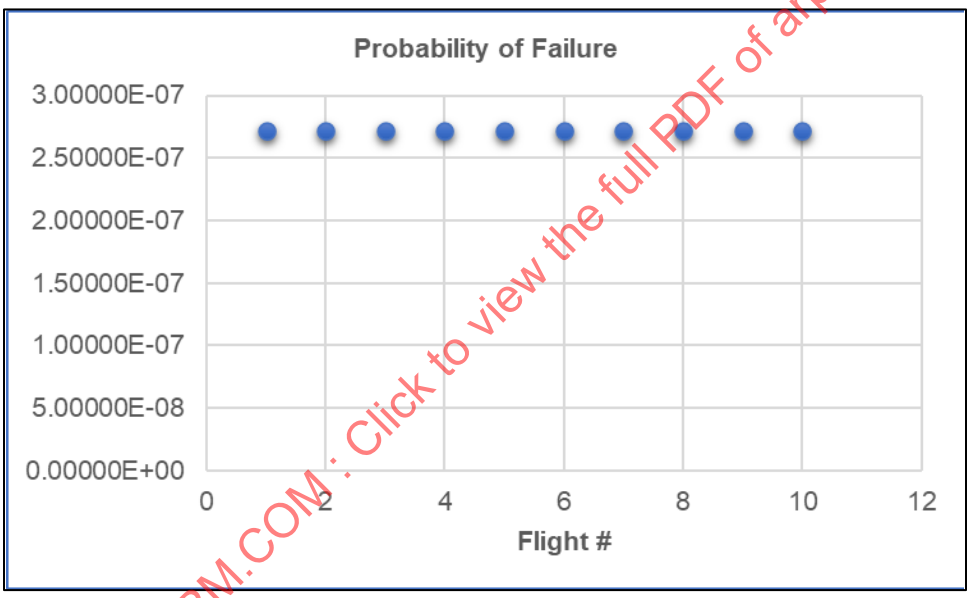
Transition #	FROM_STATE	TO_STATE	Transition Rate Symbol
1	1	2	LAMBDA1;
2	1	3	LAMBDA2;
3	1	4	LAMBDA3;
4	1	5	LAMBDA4;
5	1	6	LAMBDA5;
6	1	7	LAMBDA6;
7	1	8	LAMBDA7;
8	1	9	LAMBDA8*X;
9	1	10	LAMBDA9;
10	1	11	LAMBDA10;
11	1	12	LAMBDA11;
12	1	13	LAMBDA12;
13	1	14	LAMBDA13;
14	1	15	LAMBDA14;
15	1	16	LAMBDA15;
16	1	17	LAMBDA16;
17	1	18	LAMBDA17;
18	1	19	LAMBDA18;
19	2	20	LAMBDA2;
20	2	21	LAMBDA3;
21	2	22	LAMBDA4;
22	2	23	LAMBDA5;
23	2	24	LAMBDA6;
24	2	25	LAMBDA7;
25	2	9	LAMBDA8*X;
26	2	26	LAMBDA9;
27	2	27	LAMBDA10*X;
28	2	28	LAMBDA11;
29	2	29	LAMBDA12;
30	2	30	LAMBDA13;
31	2	31	LAMBDA14*X;
32	2	32	LAMBDA15*X;
33	2	33	LAMBDA16*X;
34	2	34	LAMBDA17*X;
35	2	35	LAMBDA18*X;
36	3	20	LAMBDA1;
		. . . .	
28285	2253	35	LAMBDA18*X;
28286	2254	2255	LAMBDA1;
		. . . .	
28300	2255	35	LAMBDA18*X;

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: The total number of state to state transitions in MM = 28300; for brevity, not all states are shown. Highlighted rows show transition from an operational state to a failure state.)

Table Q.8-4 - (PSSA - WBS - MA)
Markov Model results table

Flight #	Probability of Failure
1	2.72018E-07
2	2.72018E-07
3	2.72018E-07
4	2.72018E-07
5	2.72018E-07
6	2.72018E-07
7	2.72018E-07
8	2.72018E-07
9	2.72018E-07
10	2.72018E-07



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.8-1 - (PSSA - WBS - MA)
Total loss of wheel deceleration (80% or more)

Q.8.5 Summary of WBS MA Results for Failure Condition: BSCU Fails to Output Command to Open SOV

Tables Q.8-5 to Q.8-9 and Figure Q.8-2 summarize the MA results for the failure condition: “BSCU fails to output command to open SOV.” This analysis has no latent events for consideration.

Table Q.8-5 - (PSSA - BSCU - MA)
Markov Model event table

Event	PSSA FT Basic/Developed Event	Failure Rate Symbol	Failure or Occurrence Rate (per FH)	Exposure Time (Repair Time) (FH)
MonLogic	BSCU-AND-ERR	LAMBDA1	1.00E-06	5
PwrCh1	BSCU-CH1-PS-LOS	LAMBDA2	2.00E-05	5
PwrCh2	BSCU-CH2-PS-LOS	LAMBDA3	2.00E-05	5
CmdCh1	BSCU-CH1-COMPROC-LOSS	LAMBDA4	5.00E-06	5
CmdCh2	BSCU-CH2-COMPROC-LOSS	LAMBDA5	5.00E-06	5
MonCh1	BSCU-CH1-MONPROC-LOSS	LAMBDA6	5.00E-06	5
MonCh2	BSCU-CH2-MONPROC-LOSS	LAMBDA7	5.00E-06	5
PSMCh1Err	BSCU-CH1-PSM-ERR	LAMBDA8	2.00E-07	5
PSMCh2Err	BSCU-CH1-PSM-ERR	LAMBDA9	2.00E-07	5

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.8-6 - (PSSA - BSCU - MA)
BSCU Markov Model state space table

State #	MonLogic	PwrCh1	PwrCh2	CmdCh1	CmdCh2	MonCh1	MonCh2	PwrCh1Err	PwrCh2Err
1	1	1	1	1	1	1	1	1	1
2	Failure State Due to Last Failure of MonLogic								
3	1	0	1	1	1	1	1	1	1
4	1	1	0	1	1	1	1	1	1
5	1	1	1	0	1	1	1	1	1
6	1	1	1	1	0	1	1	1	1
7	1	1	1	1	1	0	1	1	1
8	1	1	1	1	1	1	0	1	1
9	1	1	1	1	1	1	1	0	1
10	1	1	1	1	1	1	1	1	0
11	Failure State Due to Last Failure of PwrCh2								
12	1	0	1	0	1	1	1	1	1
13	Failure State Due to Last Failure of CmdCh2								
14	1	0	1	1	1	0	1	1	1
15	Failure State Due to Last Failure of MonCh2								
16	1	0	1	1	1	1	1	0	1
17	Failure State Due to Last Failure of PwrCh2Err								
18	Failure State Due to Last Failure of PwrCh1								
19	Failure State Due to Last Failure of CmdCh1								
20	1	1	0	1	0	1	1	1	1
21	Failure State Due to Last Failure of MonCh1								
22	1	1	0	1	1	1	0	1	1
23	Failure State Due to Last Failure of PwrCh1Err								
24	1	1	0	1	1	1	1	1	0
25	1	1	1	0	1	0	1	1	1
26	1	1	1	0	1	1	1	0	1
27	1	1	1	1	0	1	0	1	1
28	1	1	1	1	0	1	1	1	0
29	1	1	1	1	1	0	1	0	1
30	1	1	1	1	1	1	0	1	0
31	1	0	1	0	1	0	1	1	1
32	1	0	1	0	1	1	1	0	1
33	1	0	1	1	1	0	1	0	1
34	1	1	0	1	0	1	0	1	1
35	1	1	0	1	0	1	1	1	0
36	1	1	0	1	1	1	0	1	0
37	1	1	1	0	1	0	1	0	1
38	1	1	1	1	0	1	0	1	0
39	1	0	1	0	1	0	1	0	1
40	1	1	0	1	0	1	0	1	0

Note that the total number of states in MM = 40 includes 9 system failure states. Highlighted rows show transition from operational to a failure state. 1 = Event not occurred. 0 = Event occurred.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.8-7 - (PSSA - BSCU - MA)
Markov Model state transitions table

Transition #	FROM_STATE	TO_STATE	Transition Rate Symbol
1	1	2	LAMBDA1*X;
2	1	3	LAMBDA2;
3	1	4	LAMBDA3;
4	1	5	LAMBDA4;
5	1	6	LAMBDA5;
6	1	7	LAMBDA6;
7	1	8	LAMBDA7;
8	1	9	LAMBDA8;
9	1	10	LAMBDA9;
10	3	2	LAMBDA1*X;
11	3	11	LAMBDA3*X;
12	3	12	LAMBDA4;
13	3	13	LAMBDA5*X;
14	3	14	LAMBDA6;
15	3	15	LAMBDA7*X;
16	3	16	LAMBDA8;
17	3	17	LAMBDA9*X;
18	4	2	LAMBDA1*X;
19	4	18	LAMBDA2*X;
20	4	19	LAMBDA4*X;
21	4	20	LAMBDA5;
22	4	21	LAMBDA6*X;
23	4	22	LAMBDA7;
24	4	23	LAMBDA8*X;
…			
212	40	18	LAMBDA2*X;
213	40	19	LAMBDA4*X;
214	40	21	LAMBDA6*X;
215	40	23	LAMBDA8*X;
521	72	29	LAMBDA10*X;
522	73	2	LAMBDA1*X;
523	73	13	LAMBDA3*X;
524	73	15	LAMBDA5*X;
525	73	17	LAMBDA7*X;
526	73	19	LAMBDA9*X;
527	73	21	LAMBDA11*X;
528	74	2	LAMBDA1*X;
529	74	22	LAMBDA2*X;
530	74	23	LAMBDA4*X;
531	74	25	LAMBDA6*X;
532	74	27	LAMBDA8*X;
533	74	29	LAMBDA10*X;

SAENORM.COM : Click to view the full PDF of arp4761a

(Editor's Note: The total number of state to state failure transitions in MM = 215, for brevity not all states are shown. Highlighted rows show transition from operational to a failure state.)

Table Q.8-8 - (PSSA - BSCU - MA)
Markov Model results table

Flight #	Probability of Failure
1	5.02278E-06
2	5.02278E-06
3	5.02278E-06
4	5.02278E-06
5	5.02278E-06
6	5.02278E-06
7	5.02278E-06
8	5.02278E-06
9	5.02278E-06
10	5.02278E-06

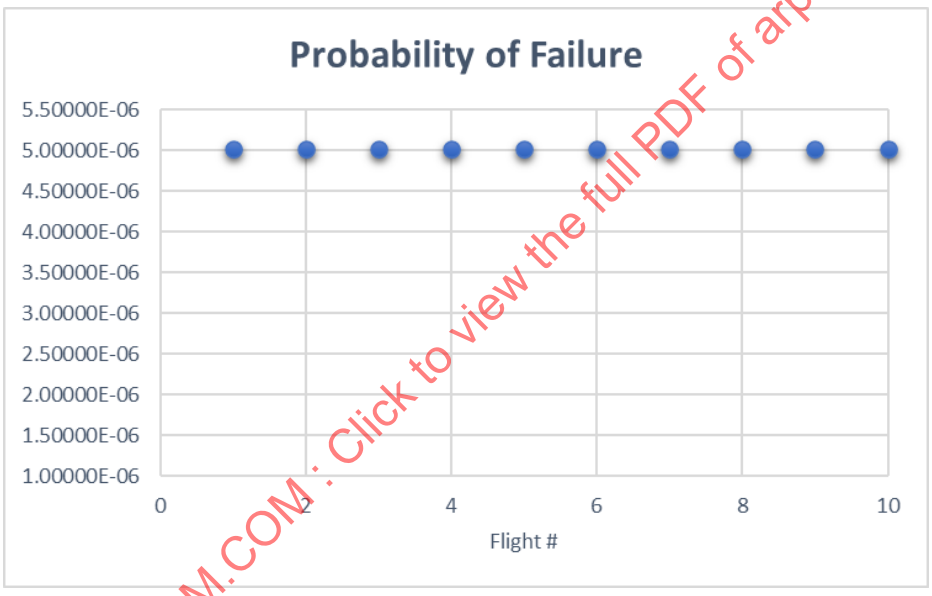


Figure Q.8-2 - (PSSA - BSCU - MA)
BSCU fails to output command to open SOV

SAENORM.COM : Click to view the full PDF of arp4761a

Q.8.6 Summary of WBS MA Results for Failure Condition: Loss of Braking Command to NMV from BSCU

Tables Q.8-9 to Q.8-12 and Figure Q.8-3 summarize the MA results for the failure condition: “Loss of braking command to NMV from BSCU”. This analysis has one latent event as shown highlighted in Table Q.8-9.

Table Q.8-9 - (PSSA - BSCU - MA)
Markov Model event table

Event	PSSA FT Basic/Developed Event	Failure Rate Symbol	Failure or Occurrence Rate (per FH)	Exposure Time (Repair Time) (FH)
SwCh1Ch2	BSCU-CMD-SW-TOTAL-ERR	LAMBDA1	1.00E-06	5
SwCh1Ch2	BSCU-CMD-SW-TOTAL-ERR	LAMBDA1	1.00E-06	5
SwCh1	BSCU-CMD-SW-ERR	LAMBDA2	1.00E-06	5
SwCh2	BSCU-CMD-SW-LOSS	LAMBDA3	1.00E-06	5
PwrCh1	BSCU-CH1-PS-LOSS	LAMBDA4	2.00E-05	5
PwrCh2	BSCU-CH2-PS-LOSS	LAMBDA5	2.00E-05	5
CmdCh1	BSCU-CH1-COMPROC-LOSS	LAMBDA6	5.00E-06	5
CmdCh2	BSCU-CH2-COMPROC-LOSS	LAMBDA7	5.00E-06	5
MonCh1Err	BSCU-CH1-MONPROC-ERR	LAMBDA8	1.00E-06	5
PwrCh1Err	BSCU-CH1-PSM-ERR	LAMBDA9	2.00E-07	5
PwrCh2Err	BSCU-CH2-PSM-ERR	LAMBDA10	2.00E-07	5
ElecPed1	ELEC_PED_POS_2-LOSS	LAMBDA11	5.00E-05	5
ElecPed2	ELEC_PED_POS_1-LOSS	LAMBDA12	5.00E-05	5
PwCh2Lat	BSCU-CH2-PS-LOSS-PUP	LAMBDA13	2.00E-05	100
SwCh2Lat	BSCU-CMD-SW-LOSS-PUP	LAMBDA14	1.00E-06	100
CmdCh2Lat	BSCU-CH2-COMPROC-LOSS-PUP	LAMBDA15	5.00E-06	100
EPed2Lat	ELE_PED_POS_2_PUP	LAMBDA16	5.00E-05	100

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.8-10 - (PSSA - BSCU - MA)
Markov Model state space table

State #	Sw Ch1Ch2	Sw Ch1	SwCh2	PwrCh1	PwrCh2	CmdCh1	CmdCh2	Mon Ch1Err	Pwr Ch1Err	Pwr Ch2Err	Elec Ped1	Elec Ped2	PwCh2Lat	SwCh2 Lat	Cmdch2 Lat	EPed2 Lat
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	Failure State Due to Last Failure of SwCh1Ch2															
3	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
5	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
6	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
8	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1
12	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1
14	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1
15	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
18	Failure State Due to Last Failure of SwCh2															
19	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1
20	Failure State Due to Last Failure of PwrCh2															
21	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1
22	Failure State Due to Last Failure of CmdCh2															
23	1	0	1	1	1	1	1	0	1	1	1	1	1	1	1	1
24	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1
25	Failure State Due to Last Failure of PwrCh2Err															
26	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1
27	Failure State Due to Last Failure of ElecPed2															
28	Failure State Due to Last Failure of PwrCh2Lat															
29	Failure State Due to Last Failure of SwCh2Lat															
30	Failure State Due to Last Failure of CmdCh2Lat															

SAENORM.COM : Click to view the full PDF of arp4761a

State #	Sw Ch1Ch2	Sw Ch1	SwCh2	PwrCh1	PwrCh2	CmdCh1	CmdCh2	Mon Ch1Err	Pwr Ch1Err	Pwr Ch2Err	Elec Ped1	Elec Ped2	PwCh2Lat	SwCh2 Lat	Cmdch2 Lat	EPed2 Lat
31	Failure State Due to Last Failure of EPed22Lat															
32	Failure State Due to Last Failure of SwCh1															
33	Failure State Due to Last Failure of PwrCh1															
34	1	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1
35	Failure State Due to Last Failure of CmdCh1															
36	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1
37	Failure State Due to Last Failure of MonCh1Err															
38	Failure State Due to Last Failure of PwrCh1Err															
39	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1
40	Failure State Due to Last Failure of ElecPed1															
41	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1
42	1	1	0	1	1	1	1	1	1	1	1	1	0	1	1	1
43	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1
44	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	1
45	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0
. . . .																
590	1	1	1	1	0	1	0	1	1	0	1	0	0	0	0	0
591	1	1	0	1	0	1	0	1	1	0	1	0	0	0	0	0

(Editor's Note: The total number of states in MM = 591 including 17 system failure states, for brevity not all states shown. Highlighted rows show transition from operational to a failure state. 1 = Event not occurred. 0 = Event occurred.)

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.8-11 - (PSSA - BSCU - MA)
Markov Model state transitions table

Transition #	FROM_STATE	TO_STATE	Transition Rate Symbol
1	1	2	LAMBDA1*X;
2	1	3	LAMBDA2;
3	1	4	LAMBDA3;
4	1	5	LAMBDA4;
5	1	6	LAMBDA5;
6	1	7	LAMBDA6;
7	1	8	LAMBDA7;
8	1	9	LAMBDA8;
9	1	10	LAMBDA9;
10	1	11	LAMBDA10;
11	1	12	LAMBDA11;
12	1	13	LAMBDA12;
13	1	14	LAMBDA13;
14	1	15	LAMBDA14;
15	1	16	LAMBDA15;
16	1	17	LAMBDA16;
17	3	2	LAMBDA1*X;
18	3	18	LAMBDA3*X;
19	3	19	LAMBDA4;
20	3	20	LAMBDA5*X;
21	3	21	LAMBDA6;
22	3	22	LAMBDA7*X;
23	3	23	LAMBDA8;
24	3	24	LAMBDA9;
25	3	25	LAMBDA10*X;
26	3	26	LAMBDA11;
27	3	27	LAMBDA12*X;
28	3	28	LAMBDA13*X;
29	3	29	LAMBDA14*X;
30	3	30	LAMBDA15*X;
31	3	31	LAMBDA16*X;
32	4	2	LAMBDA1*X;
33	4	32	LAMBDA2*X;
34	4	33	LAMBDA4*X;
35	4	34	LAMBDA5;
36	4	35	LAMBDA6*X;
37	4	36	LAMBDA7;
38	4	37	LAMBDA8*X;
39	4	38	LAMBDA9*X;
40	4	39	LAMBDA10;
41	4	40	LAMBDA11*X;
42	4	41	LAMBDA12;
. . .			
6685	589	591	LAMBDA5;
6686	589	35	LAMBDA6*X;
6687	589	37	LAMBDA8*X;
6688	589	38	LAMBDA9*X;
6689	589	40	LAMBDA11*X;
6690	590	2	LAMBDA1*X;
6691	590	32	LAMBDA2*X;
6692	590	591	LAMBDA3;
6693	590	33	LAMBDA4*X;
6694	590	35	LAMBDA6*X;

SAENORM.COM : Click to view the full PDF of arp4761a

Transition #	FROM_STATE	TO_STATE	Transition Rate Symbol
6695	590	37	LAMBDA8*X;
6696	590	38	LAMBDA9*X;
6697	590	40	LAMBDA11*X;
6698	591	2	LAMBDA1*X;
6699	591	32	LAMBDA2*X;
6700	591	33	LAMBDA4*X;
6701	591	35	LAMBDA6*X;
6702	591	37	LAMBDA8*X;
6703	591	38	LAMBDA9*X;
6704	591	40	LAMBDA11*X;

(Editor's Note: The total number of state to state failure transitions in MM = 6704. Highlighted rows show transition from operational to a failure state. For brevity not all live states are shown.)

Table Q.8-12 - (PSSA - BSCU - MA)
Markov Model results table

Flight #	Probability of Failure	Average Probability
1	5.29356E-06	6.67847E-06
2	5.44002E-06	6.67847E-06
3	5.58636E-06	6.67847E-06
4	5.73259E-06	6.67847E-06
5	5.87870E-06	6.67847E-06
6	6.02471E-06	6.67847E-06
7	6.17060E-06	6.67847E-06
8	6.31638E-06	6.67847E-06
9	6.46204E-06	6.67847E-06
10	6.60760E-06	6.67847E-06
11	6.75304E-06	6.67847E-06
12	6.89837E-06	6.67847E-06
13	7.04358E-06	6.67847E-06
14	7.18869E-06	6.67847E-06
15	7.33368E-06	6.67847E-06
16	7.47857E-06	6.67847E-06
17	7.62334E-06	6.67847E-06
18	7.76799E-06	6.67847E-06
19	7.91254E-06	6.67847E-06
20	8.05698E-06	6.67847E-06
21	5.29356E-06	6.67847E-06
22	5.44002E-06	6.67847E-06
23	5.58636E-06	6.67847E-06
24	5.73259E-06	6.67847E-06
25	5.87870E-06	6.67847E-06
26	6.02471E-06	6.67847E-06
27	6.17060E-06	6.67847E-06
28	6.31638E-06	6.67847E-06
29	6.46204E-06	6.67847E-06
30	6.60760E-06	6.67847E-06
31	6.75304E-06	6.67847E-06
32	6.89837E-06	6.67847E-06
33	7.04358E-06	6.67847E-06
34	7.18869E-06	6.67847E-06
35	7.33368E-06	6.67847E-06
36	7.47857E-06	6.67847E-06
37	7.62334E-06	6.67847E-06
38	7.76799E-06	6.67847E-06

SAENORM.COM : Click to view the full PDF of arp4761a

Flight #	Probability of Failure	Average Probability
39	7.91254E-06	6.67847E-06
40	8.05698E-06	6.67847E-06
41	5.29356E-06	6.67847E-06
42	5.44002E-06	6.67847E-06
43	5.58636E-06	6.67847E-06
44	5.73259E-06	6.67847E-06
45	5.87870E-06	6.67847E-06
46	6.02471E-06	6.67847E-06
47	6.17060E-06	6.67847E-06
48	6.31638E-06	6.67847E-06
49	6.46204E-06	6.67847E-06
50	6.60760E-06	6.67847E-06
51	6.75304E-06	6.67847E-06
52	6.89837E-06	6.67847E-06
53	7.04358E-06	6.67847E-06
54	7.18869E-06	6.67847E-06
55	7.33368E-06	6.67847E-06
56	7.47857E-06	6.67847E-06
57	7.62334E-06	6.67847E-06
58	7.76799E-06	6.67847E-06
59	7.91254E-06	6.67847E-06
60	8.05698E-06	6.67847E-06
61	5.29356E-06	6.67847E-06
62	5.44002E-06	6.67847E-06
63	5.58636E-06	6.67847E-06
64	5.73259E-06	6.67847E-06
65	5.87870E-06	6.67847E-06
66	6.02471E-06	6.67847E-06
67	6.17060E-06	6.67847E-06
68	6.31638E-06	6.67847E-06
69	6.46204E-06	6.67847E-06
70	6.60760E-06	6.67847E-06
71	6.75304E-06	6.67847E-06
72	6.89837E-06	6.67847E-06
73	7.04358E-06	6.67847E-06
74	7.18869E-06	6.67847E-06
75	7.33368E-06	6.67847E-06
76	7.47857E-06	6.67847E-06
77	7.62334E-06	6.67847E-06
78	7.76799E-06	6.67847E-06
79	7.91254E-06	6.67847E-06
80	8.05698E-06	6.67847E-06
81	5.29356E-06	6.67847E-06
82	5.44002E-06	6.67847E-06
83	5.58636E-06	6.67847E-06
84	5.73259E-06	6.67847E-06
85	5.87870E-06	6.67847E-06
86	6.02471E-06	6.67847E-06
87	6.17060E-06	6.67847E-06
88	6.31638E-06	6.67847E-06
89	6.46204E-06	6.67847E-06
90	6.60760E-06	6.67847E-06
91	6.75304E-06	6.67847E-06
92	6.89837E-06	6.67847E-06
93	7.04358E-06	6.67847E-06
94	7.18869E-06	6.67847E-06

SAENORM.COM : Click to view the full PDF of arp4761a

Flight #	Probability of Failure	Average Probability
95	7.33368E-06	6.67847E-06
96	7.47857E-06	6.67847E-06
97	7.62334E-06	6.67847E-06
98	7.76799E-06	6.67847E-06
99	7.91254E-06	6.67847E-06
100	8.05698E-06	6.67847E-06
Average		6.67847E-06

(Editor's Note: For brevity, not all flights with probability of failures are shown.)

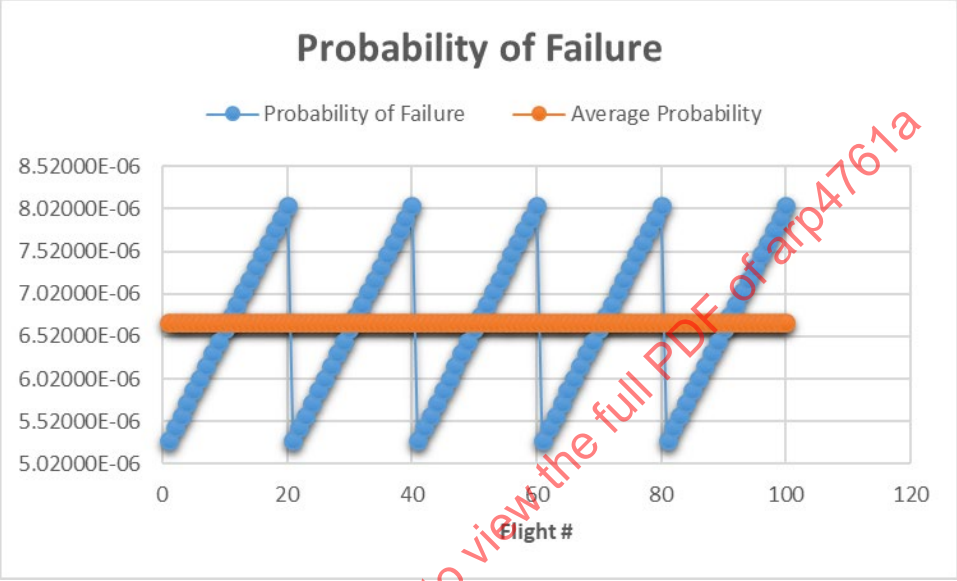


Figure Q.8-3 - (PSSA - BSCU - MA)
Loss of braking command to NMV from BSCU

SAENORM.COM : Click to view the full PDF of arp4761a

Q.8.7 Summary of WBS MA Results for Failure Condition: BSCU Provides Unannunciated Erroneous Output to NMV Inadvertently

Tables Q.8-13 to Q.8-16 and Figure Q.8-4 summarize the MA results for the failure condition: “BSCU provides unannunciated erroneous output to NMV inadvertently”. This analysis has multiple latent events as shown highlighted in Table Q.8-13.

Table Q.8-13 - (PSSA - BSCU - MA)
Markov Model event table

Component/Event	PSSA FT Basic/Developed Event	Failure Rate Symbol	Failure or Occurrence Rate (per FH)	Exposure Time (Repair Time) (FH)
Pwr1Err	BSCU-CH1-PS-ERR	LAMBDA1	1.06E-05	5
Pwr1Mon	BSCU-CH1-PSM-LOSS-PUP	LAMBDA2	2.00E-07	100
Pwr2Err	BSCU-CH2-PS-ERR	LAMBDA3	1.06E-05	5
Pwr2Mon	BSCU-CH2-PSM-LOSS-PUP	LAMBDA4	2.00E-07	100
CmdCh1Hw	BSCU-CH1-COMPROC-ERR	LAMBDA5	1.00E-06	5
CmdCh1	BSCU-CH1-COMPROC-LOSS	LAMBDA6	5.00E-06	5
MonCh1Hw	BSCU-CH1-MONPROC-LOSS-PUP	LAMBDA7	5.00E-06	100
CmdCh2Hw	BSCU-CH2-COMPROC-ERR	LAMBDA8	1.00E-06	5
MonCh2Hw	BSCU-CH2-MONPROC-LOSS-PUP	LAMBDA9	5.00E-06	100
Ch1Ch2Sw	BSCU-CMD-SW-ERR	LAMBDA10	1.00E-06	5
Ch1Ch2SwL	BSCU-CMD-SW-LOSS-PUP	LAMBDA11	1.00E-06	100
ANDSwFail	BSCU-AND-LOSS-PUP	LAMBDA12	1.00E-06	100
MonCh1Err	BSCU-CH1-MONPROC-ERR	LAMBDA13	1.00E-06	5
Pwr1MonErr	BSCU-CH1-PSM-ERR	LAMBDA14	2.00E-07	5

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.8-14 - (PSSA - BSCU - MA)
Markov Model state space table

State #	Pwr1Err	Pwr1Mon	Pwr2Err	Pwr2Mon	CmdCh1Hw	CmdCh1	MonCh1Hw	CmdCh2Hw	MonCh2Hw	Ch1Ch2Sw	Ch1Ch2SwL	ANDSwFail	MonCh1Err	Pwr1MonErr
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	0	1	1	1	1	1	1	1	1	1	1	1	1
4	1	1	0	1	1	1	1	1	1	1	1	1	1	1
5	1	1	1	0	1	1	1	1	1	1	1	1	1	1
. . .														
14	1	1	1	1	1	1	1	1	1	1	1	1	0	1
15	1	1	1	1	1	1	1	1	1	1	1	1	1	0
16	Failure State Due to Last Failure of Pwr1Mon													
17	0	1	0	1	1	1	1	1	1	1	1	1	1	1
18	0	1	1	0	1	1	1	1	1	1	1	1	1	1
19	0	1	1	1	0	1	1	1	1	1	1	1	1	1
. . .														
29	Failure State Due to Last Failure of Pwr1Err													
30	1	0	0	1	1	1	1	1	1	1	1	1	1	1
31	1	0	1	0	1	1	1	1	1	1	1	1	1	1
. . .														
64	Failure State Due to Last Failure of MonCh1Hw													
65	1	1	1	1	0	1	1	0	1	1	1	1	1	1
66	1	1	1	1	0	1	1	1	0	1	1	1	1	1
67	1	1	1	1	0	1	1	1	1	0	1	1	1	1
68	Failure State Due to Last Failure of Ch1Ch2SwL													
. . .														
80	Failure State Due to Last Failure of CmdCh1Hw													
81	1	1	1	1	1	1	0	0	1	1	1	1	1	1
. . .														
238	Failure State Due to Last Failure of CmdCh1													
239	1	1	0	0	1	1	0	1	1	1	1	1	1	1
240	1	1	0	0	1	1	1	0	1	1	1	1	1	1
241	1	1	0	0	1	1	1	1	0	1	1	1	1	1
242	Failure State Due to Last Failure of Ch1Ch2Sw													
243	1	1	0	0	1	1	1	1	1	1	0	1	1	1
244	1	1	0	0	1	1	1	1	1	1	1	0	1	1
245	Failure State Due to Last Failure of MonCh1Err													
246	Failure State Due to Last Failure of Pwr1MonErr													
247	1	1	0	1	0	0	1	1	1	1	1	1	1	1
. . .														
254	Failure State Due to Last Failure of Pwr2Mon													
255	1	1	0	1	1	0	0	1	1	1	1	1	1	1
. . .														
298	Failure State Due to Last Failure of Pwr2Err													
299	1	1	1	0	1	0	0	1	1	1	1	1	1	1
300	1	1	1	0	1	0	1	0	1	1	1	1	1	1
. . .														
363	Failure State Due to Last Failure of MonCh2Hw													
364	1	1	1	1	1	0	1	0	1	0	1	1	1	1
365	1	1	1	1	1	0	1	0	1	1	0	1	1	1

SAENORM.COM : Click to view the full PDF of arp4761a

366	Failure State Due to Last Failure of ANDSwFail													
367	1	1	1	1	1	0	1	0	1	1	1	1	0	1
368	1	1	1	1	1	0	1	0	1	1	1	1	1	0
369	Failure State Due to Last Failure of CmdCh2Hw													
370	1	1	1	1	1	0	1	1	0	0	1	1	1	1
...														
3869	1	0	1	0	1	0	0	1	0	0	0	0	0	0

(Editor's Note: The total number of states in MM = 3869 including 14 system failure states, for brevity not all states are shown. Highlighted rows show transition from operational to a failure state. 1 = Event not occurred. 0 = Event occurred.)

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.8-15 - (PSSA - BSCU - MA)
Markov Model state transitions table

Transition #	FROM_STATE	TO_STATE	Transition Rate Symbol
1	1	2	LAMBDA1;
2	1	3	LAMBDA2;
3	1	4	LAMBDA3;
4	1	5	LAMBDA4;
5	1	6	LAMBDA5;
		. . . .	
15	2	16	LAMBDA2*X;
		. . . .	
27	2	28	LAMBDA14;
28	3	29	LAMBDA1*X;
29	3	30	LAMBDA3;
		. . . .	
71	6	63	LAMBDA6;
72	6	64	LAMBDA7*X;
73	6	65	LAMBDA8;
74	6	66	LAMBDA9;
75	6	67	LAMBDA10;
76	6	68	LAMBDA11*X;
77	6	69	LAMBDA12;
78	6	70	LAMBDA13;
		. . . .	
96	8	55	LAMBDA4;
97	8	80	LAMBDA5*X;
98	8	72	LAMBDA6;
		. . . .	
148	12	59	LAMBDA4;
149	12	80	LAMBDA5*X;
150	12	76	LAMBDA6;
		. . . .	
196	15	108	LAMBDA13;
197	17	16	LAMBDA2*X;
		. . . .	
33520	3869	369	LAMBDA8*X;

Note that the total number of state to state failure transitions in MM = 33520. Highlighted rows show transition from operational to a failure state.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.8-16 - (PSSA - BSCU - MA)
Markov Model results table

Flight #	Probability of Failure	Average Probability
1	2.030033E-10	2.13099E-09
2	4.059984E-10	2.13099E-09
3	6.089854E-10	2.13099E-09
4	8.119643E-10	2.13099E-09
5	1.014935E-09	2.13099E-09
6	1.217898E-09	2.13099E-09
7	1.420852E-09	2.13099E-09
8	1.623799E-09	2.13099E-09
9	1.826737E-09	2.13099E-09
10	2.029668E-09	2.13099E-09
11	2.232590E-09	2.13099E-09
12	2.435504E-09	2.13099E-09
13	2.638410E-09	2.13099E-09
14	2.841307E-09	2.13099E-09
15	3.044197E-09	2.13099E-09
16	3.247079E-09	2.13099E-09
17	3.449952E-09	2.13099E-09
18	3.652818E-09	2.13099E-09
19	3.855675E-09	2.13099E-09
20	4.058524E-09	2.13099E-09
21	2.030033E-10	2.13099E-09
22	4.059984E-10	2.13099E-09
23	6.089854E-10	2.13099E-09
24	8.119643E-10	2.13099E-09
25	1.014935E-09	2.13099E-09
26	1.217898E-09	2.13099E-09
27	1.420852E-09	2.13099E-09
28	1.623799E-09	2.13099E-09
29	1.826737E-09	2.13099E-09
30	2.029668E-09	2.13099E-09
31	2.232590E-09	2.13099E-09
32	2.435504E-09	2.13099E-09
33	2.638410E-09	2.13099E-09
34	2.841307E-09	2.13099E-09
35	3.044197E-09	2.13099E-09
36	3.247079E-09	2.13099E-09
37	3.449952E-09	2.13099E-09
38	3.652818E-09	2.13099E-09
39	3.855675E-09	2.13099E-09
40	4.058524E-09	2.13099E-09
41	2.030033E-10	2.13099E-09
42	4.059984E-10	2.13099E-09
43	6.089854E-10	2.13099E-09
44	8.119643E-10	2.13099E-09
45	1.014935E-09	2.13099E-09
46	1.217898E-09	2.13099E-09
47	1.420852E-09	2.13099E-09
48	1.623799E-09	2.13099E-09
49	1.826737E-09	2.13099E-09
50	2.029668E-09	2.13099E-09
51	2.232590E-09	2.13099E-09
52	2.435504E-09	2.13099E-09
53	2.638410E-09	2.13099E-09
54	2.841307E-09	2.13099E-09
55	3.044197E-09	2.13099E-09
56	3.247079E-09	2.13099E-09
57	3.449952E-09	2.13099E-09
58	3.652818E-09	2.13099E-09

SAENORM.COM : Click to view the full PDF of arp4761a

Flight #	Probability of Failure	Average Probability
59	3.855675E-09	2.13099E-09
60	4.058524E-09	2.13099E-09
61	2.030033E-10	2.13099E-09
62	4.059984E-10	2.13099E-09
63	6.089854E-10	2.13099E-09
64	8.119643E-10	2.13099E-09
65	1.014935E-09	2.13099E-09
66	1.217898E-09	2.13099E-09
67	1.420852E-09	2.13099E-09
68	1.623799E-09	2.13099E-09
69	1.826737E-09	2.13099E-09
70	2.029668E-09	2.13099E-09
71	2.232590E-09	2.13099E-09
72	2.435504E-09	2.13099E-09
73	2.638410E-09	2.13099E-09
74	2.841307E-09	2.13099E-09
75	3.044197E-09	2.13099E-09
76	3.247079E-09	2.13099E-09
77	3.449952E-09	2.13099E-09
78	3.652818E-09	2.13099E-09
79	3.855675E-09	2.13099E-09
80	4.058524E-09	2.13099E-09
81	2.030033E-10	2.13099E-09
82	4.059984E-10	2.13099E-09
83	6.089854E-10	2.13099E-09
84	8.119643E-10	2.13099E-09
85	1.014935E-09	2.13099E-09
86	1.217898E-09	2.13099E-09
87	1.420852E-09	2.13099E-09
88	1.623799E-09	2.13099E-09
89	1.826737E-09	2.13099E-09
90	2.029668E-09	2.13099E-09
91	2.232590E-09	2.13099E-09
92	2.435504E-09	2.13099E-09
93	2.638410E-09	2.13099E-09
94	2.841307E-09	2.13099E-09
95	3.044197E-09	2.13099E-09
96	3.247079E-09	2.13099E-09
97	3.449952E-09	2.13099E-09
98	3.652818E-09	2.13099E-09
99	3.855675E-09	2.13099E-09
100	4.058524E-09	2.13099E-09
Average	2.13099E-09	

(Editor's Note: For brevity, not all flights with probability of failures are shown.)

SAENORM.COM : Click to view the full PDF of arp4761a

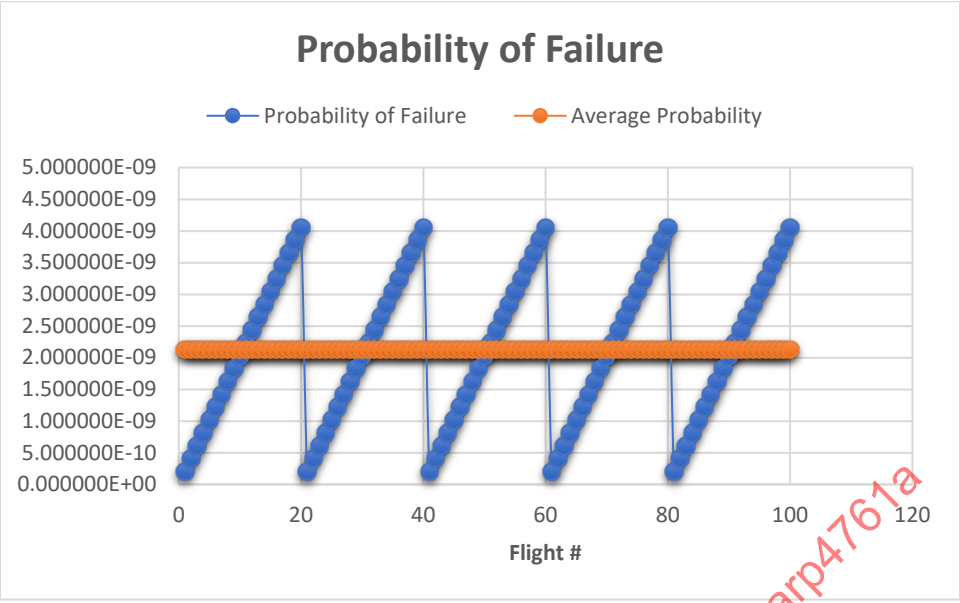


Figure Q.8-4 - (PSSA - BSCU - MA)
BSCU provides unannunciated erroneous output to NMV inadvertently

Q.8.8 Summary and Conclusions

Appendix Q.8 considered the MM for one failure condition for WBS and three safety requirements and replicated the system failure logic and the failure rates and exposure times as represented by the PSSA Section Q.6. The objective was to show that MM are equivalent to FTA as a technique for safety analysis from a final results point of view and the results demonstrate the equivalence. The results also show the power of MM in modeling average probability per flight and handling the transient failure behavior of a system due to detection and repair latency. The power of MM is discussed further in Appendix I but the focus here is on the specific WBS PSSA and the equivalence in V&V of safety requirements and allocations.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.9 S18 AIRPLANE - WBS PSSA EXAMPLE USING MODEL BASED SAFETY ANALYSIS (MBSA)

WBS PSSA MBSA Example

Q.9.1 MBSA Example Introduction

This section provides an example of a Model-Based Safety Analysis (MBSA) used to support a PSSA or an SSA. For the sake of brevity, this example considers only supporting a PSSA. This MBSA PSSA example is simplified and does not make the same assumptions as those in the Wheel Brake System (WBS) PSSA using Fault Tree Analysis in Section Q.6.

Q.9.2 MBSA Modeling

An MBSA safety model is an abstraction of the candidate system to be developed from a safety point of view. The model development may substantiate the safety analysis supporting the strategies or concepts that are design choices to satisfy the upper-level requirements.

The safety analyst receives explicit inputs from the design team and/or captures rationales to fully understand the design characteristics. As long as the upper-level requirements are not fulfilled, the design architecture is improved and refined. The safety model evolves accordingly.

As the design architecture is refined, the MBSA model may not be refined to the same level of detail. The model refinement continues until sufficient decomposition to get independent blocks regarding the effects of random failures or until the ability to verify each safety requirement is achieved.

Multiple safety model iterations are presented in this example. At each iteration, the following MBSA process was followed:

1. Account for MBSA inputs: Failure Conditions, refined requirements, design architecture, and updates.
2. Model the architecture: Identify modeling assumptions to be confirmed and capture acceptable simplifications.
3. Perform the MBSA Failure Condition Evaluation (generation of Functional Failure Sets (FFSs) and/or minimal cut sets, probability computation).
4. Assess the PASA and refined safety requirements verification status.
5. Provide MBSA outputs: New proposed requirements, design recommendations, or architecture suggestions to cope with unsatisfied requirements.

The WBS and the associated function is decelerate wheels during the landing phase (landing gear extended) were used in this example. Two safety models were developed corresponding to the two design description iterations of the WBS.

Q.9.3 High-Level Model of the Wheel Brake System

A dedicated high-level model, which only includes functions to be realized by the WBS, is used to determine the first architecture requirements from the safety point of view. This high-level model implements the relevant failure modes of these functions. After a verification of the model by simulation, a generation of the FFSs and minimal cut sets from this model is performed. The analysis results are used to aid in allocating qualitative and quantitative requirements.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.9.3.1 High-Level Model MBSA Inputs

Q.9.3.1.1 High-Level Model Inputs from the SFHA

(Editor's Note: For the sake of brevity, only two failure conditions from the SFHA were selected. The crew annunciation will not be considered within the MBSA example.)

The following two failure conditions are analyzed in this example:

1.1.TL: Total loss of wheel deceleration (80% coverage or more), Hazardous failure condition, renamed for simplicity as "Loss of Wheel Braking" function.

1.1.MF1: Uncommanded full symmetric wheel deceleration, Catastrophic failure condition, renamed for simplicity as "Uncommanded Wheel Braking" function.

Q.9.3.1.2 High-Level Model Inputs from the PASA

(Editor's Note: For the sake of brevity, only the specific requirements of concern for the internal WBS design were selected from the PASA.)

(Editor's Note: The Uncommanded wheel braking failure condition was not analyzed in the PASA example (see Editor's Note of Section Q.4.5). However, the SFHA example identified one additional failure condition to address the Uncommanded Braking (see 1.1 MF1 in Section Q.5). This failure condition was further refined in this example into two requirements: one quantitative (PASA-SR-XY) and one qualitative (PASA-SR-XX).)

PASA-SR-01: Decelerate wheels Function shall be developed FDAL A.

PASA-SR-05: Complete loss of wheel brake shall be less than 1.0E-07 for a landing.

PASA-SR-XX: No single failure shall result in an uncommanded full symmetric wheel deceleration during a takeoff roll.

PASA-SR-XY: Uncommanded full symmetric wheel deceleration shall be less than 1.0E-09 for a takeoff.

PASA-SR-12: Loss of power from both hydraulic subsystems powered by the engines shall not lead to complete loss of wheel braking.

PASA-SR-14: Two redundant control lanes shall be provided between the Electric Brake Unit (EBU) and each of the two Alternate/Emergency Meter Valves.

Q.9.3.2 High-Level WBS Model

The WBS model is functionally implemented as shown in Figure Q.9-1. The main functions of the WBS are modeled as well as the external systems and equipment which have functional dependencies (e.g., command, resources).

(Editor's Note: Design data provided by the design team was used to develop the model in this example.)

SAENORM.COM : Click to view the full PDF of arp4761a

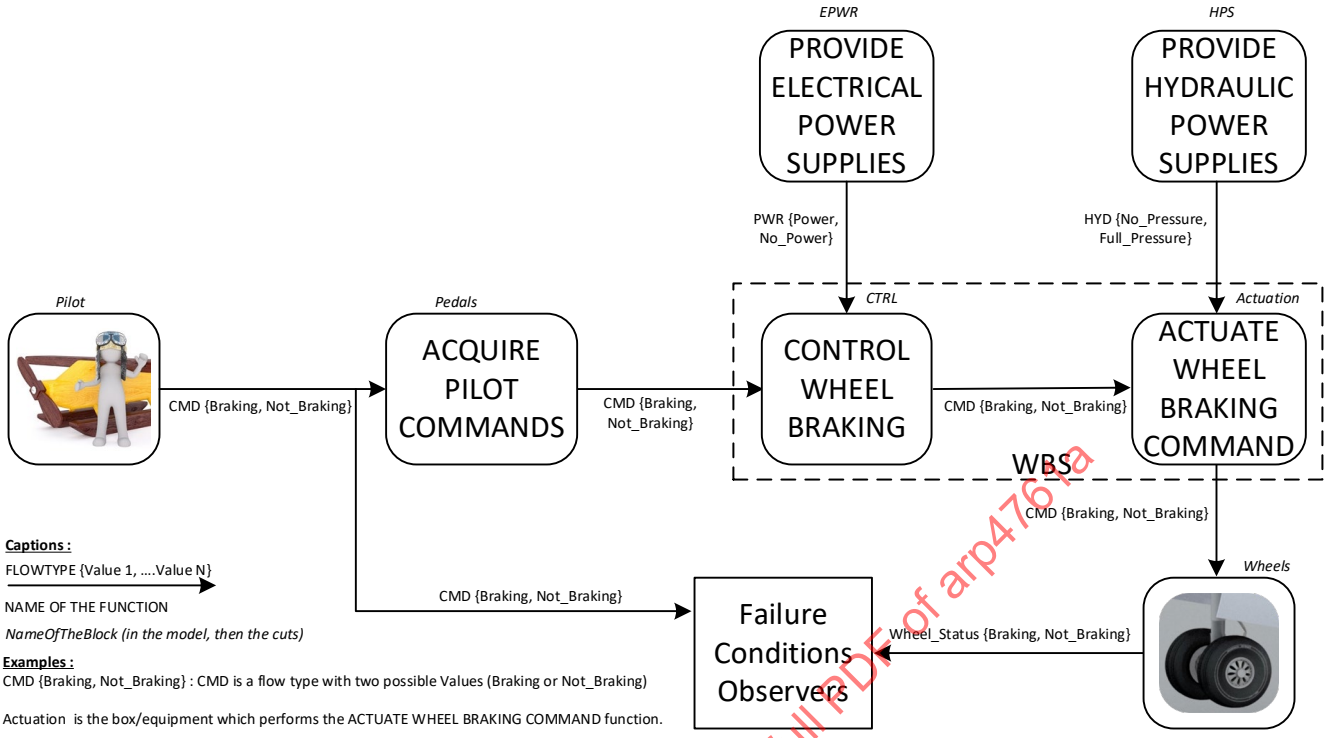


Figure Q.9-1 - (PSSA - WBS - MBSA)
WBS high-level model

Each model block is an abstraction of one or more functions or a piece of equipment. Each modeling block computes its outputs taking into account the block inputs and internal block states.

a. At this level of the model, five blocks represent sub-functions of the braking function:

   1. Pedals performing the “ACQUIRE PILOT COMMANDS” function.
   2. CTRL performing the “CONTROL WHEEL BRAKING” function.
   3. EPWR performing the “PROVIDE ELECTRICAL POWER SUPPLIES” function.
   4. HPS performing the “PROVIDE HYDRAULIC POWER SUPPLIES” function.
   5. Actuation performing the “ACTUATE WHEEL BRAKING COMMAND” function.

b. Two blocks (Pilot and Wheels) represent the braking command from the pilot and the effectiveness of the braking function on the wheels, respectively.

c. One block (failure conditions observers) represents the observers for each failure condition.

(Editor’s Note: As the two blocks entitled “Pilot” and “Wheels” shown in Figure Q.9.1 represent the input and the output of the studied system, we decided not to include dysfunctional behavior in them.)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.9.3.2.1 High-Level WBS Model Block Definition

Each high-level WBS model block was defined in accordance with the following process.

- Identify the inputs/outputs of the block.
- Identify the events; e.g., failure modes, external events (lightning, icing, fire, etc.).
- Identify the internal states of the block.
- Identify the conditions (events and/or inputs) that trigger transitions between states.
- Define the functional and dysfunctional behaviors of the block. The functional behavior is taken into account as far as it has an impact on the failure propagation (e.g., reconfiguration mechanisms). The dysfunctional behavior defines the outputs of the block depending on the inputs and the internal states.

The two blocks entitled “Pilot” and “Wheels,” shown in Figure Q.9-1, did not include any dysfunctional behavior as they represent the input and the output of the system.

(Editor’s Note: For consistency with the PSSA example based on FTA, no external events were addressed in this example.)

Q.9.3.2.2 High-Level WBS Model Flow Definition

Information relationship links were defined between the different model blocks. While the flow of information can be continuous, the information is characterized into discrete values and/or states, and then modeled. These values or states reflect failure modes or states of operation that are considered in downstream blocks. The values of the discretized flow are modeling choices.

Information flow examples:

- For a hydraulic flow: Full_Pressure, No_Pressure.

  (Editor’s Note: at this stage, the Degraded_Pressure is not considered.)

- For an electrical flow: Power, No_Power.

  (Editor’s Note: at this stage, the Degraded_Power is not considered.)

- For a braking command flow: the discrete value of braking command which could be: Braking or Not_Braking.

Q.9.3.2.3 High-Level WBS Model Failure Condition Definition

The failure condition definitions of interest are:

- Loss of wheel braking (1.1.TL): Pilot_CMD is Braking AND Wheels are Not_Braking.
- Uncommanded wheel braking (1.1.MF1): Pilot_CMD is Not_Braking AND Wheels are Braking.

Within the model, a dedicated block named “Failure Conditions Observers” was created. Each observer implemented the top Boolean equation relevant to the definitions of each failure condition.

(Editor’s Note: The two functional flow values (Braking, Not_Braking) were deemed sufficient to provide the information necessary to observe the selected failure conditions (a modeling choice).)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.9.3.2.4 High-Level WBS Detailed Model

The WBS high-level model detail is shown in Figure Q.9-2.

In the pilot block, two initial states were defined (Braking and Not_Braking). The initial state then depended upon which failure condition was being analyzed. The pilot initial state is Braking to assess the “Loss of wheel braking” failure condition; pilot initial state is Not_Braking to assess the “Uncommanded wheel braking” failure condition.

In all other blocks the first state defined represents the initial state.

SAENORM.COM : Click to view the full PDF of arp4761a

Editor's Note 1: In the pilot block, we chosed to define 2 initial states (Braking and Not_Braking) depending on the analyzed Failure Condition. The pilot initial state is Braking to assess the *Loss of Wheel Braking* Failure Condition, Not_Braking to assess the *Inadvertent Wheel Braking* Failure Condition.

Editor's Note 2: in each block (except pilot block), the first state defined represents the initial state.

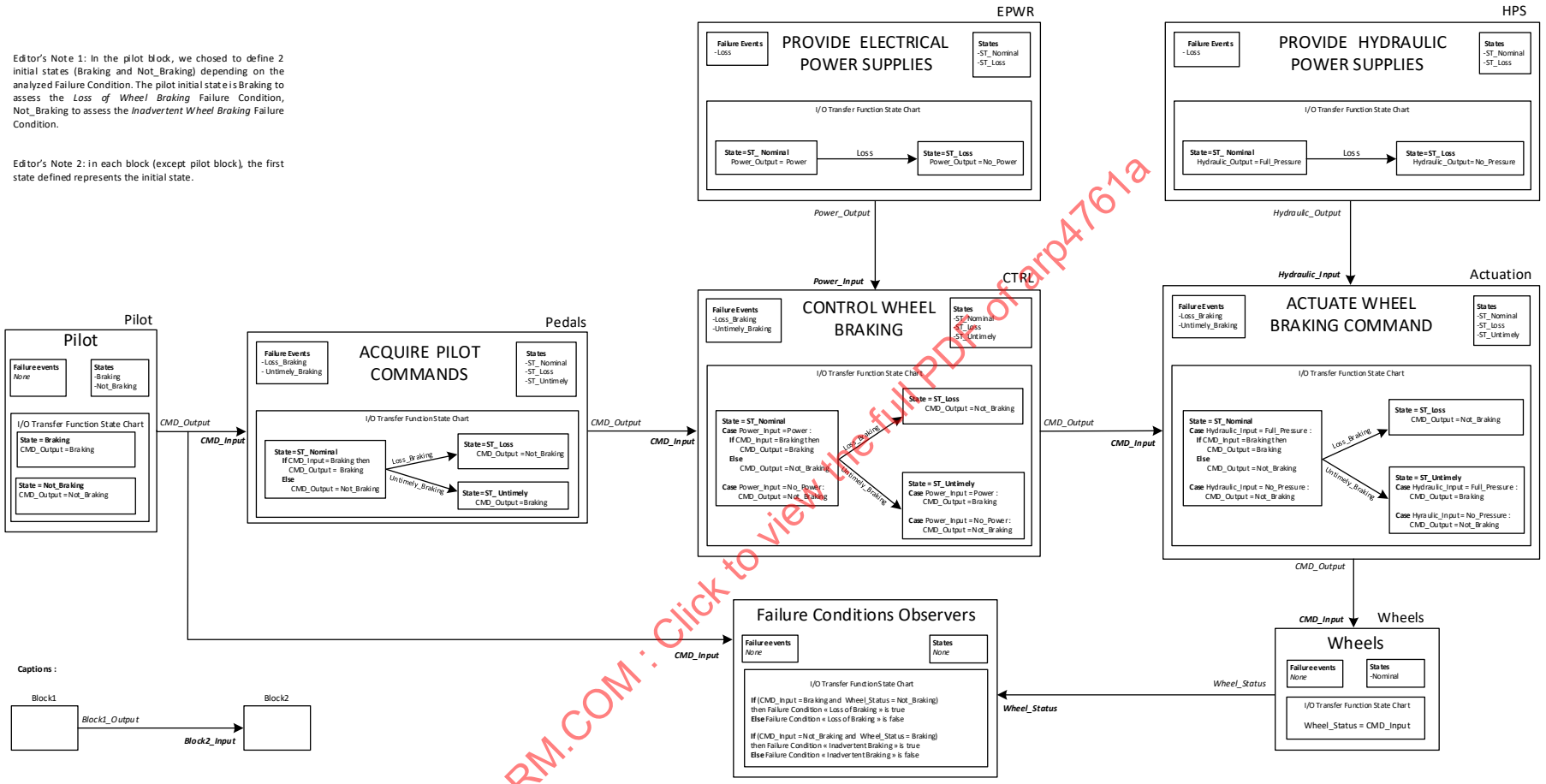


Figure Q.9-2 - (PSSA - WBS - MBSA)
Detailed Wheel Brake System high-level model

SAENORM.COM : Click to view the full PDF of arp4761a

The Control Wheel Braking “CTRL” block, shown in Figure Q.9.3, is taken as an example to illustrate how each block was created.

- Two inputs:
  - CMD_Input is the command received from “Pedals” and its type is CMD, as defined previously. It can take two different values “Braking” or “Not_Braking.”
  - Power_Input is the electrical power supply received from “EPWR” and its type is PWR. Two different values are possible: “Power” and “No_Power.”
- One output:
  - CMD_Output is the command sent to “Actuation” and its type is CMD. It can take two different values “Braking” or “Not_Braking.”
- Two events (failure modes of the block in this case):
  - Loss_Braking.
  - Untimely_Braking (Braking when not requested).
- Three internal states:
  - ST_Nominal.
  - ST_Loss.
  - ST_Untimely.
- Behavior of the block depending of inputs and internal states.

If the block is electrically powered:

- If ST_Nominal, it propagates the input value i.e., CMD_Output = CMD_Input.
- If ST_Loss, it produces the Not_Braking command, irrespective of the CMD_Input.
- If ST_Untimely, it produces the Braking command, irrespective of the CMD_Input.

Else (the block is not electrically powered):

- CMD_Output = Not_Braking, irrespective of the internal state of the block and of the CMD_Input.

SAENORM.COM : Click to view the full PDF of arp4761a

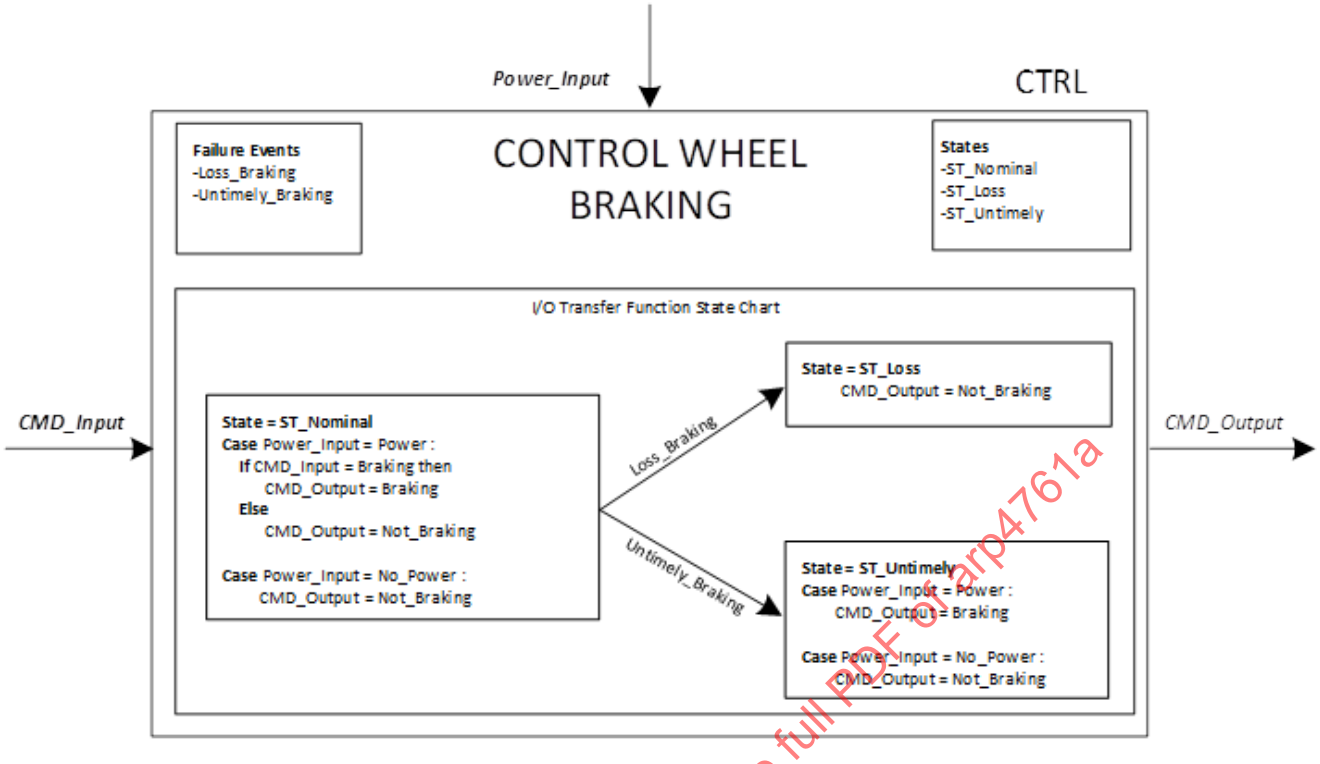


Figure Q.9-3 - (PSSA - WBS - MBSA)
Detailed Control Wheel Braking "CTRL" block

Q.9.3.3 High-Level WBS Model MBSA Failure Condition Evaluation

Two failure conditions (Loss and Uncommanded) were evaluated.

An MBSA tool is used to generate the Minimal Cut Sets (MCS) associated to each failure condition. The tool used the dysfunctional behavior (and the relevant functional behavior) defined in the Failure Propagation Model (FPM). The Minimal Cut Sets combine the failure events defined in the model.

An evaluation of the planned development flow (captured in the PSSA Q.6-20) has identified that development errors will also result in the failure conditions under study due to the lack of development independence. In this example case then, the model "failure events" represent either development errors (for FFS DAL allocation activity) or random failures (for no single failure analysis and quantitative analysis) at the WBS level.

(Editor's Note: Reminder of the difference between FFS and MCS:

The definition of an FFS (main body 2.2 is: "FUNCTIONAL FAILURE SET (FFS): A set of one or more members that are considered to be independent from one another (not necessarily limited to one system), whose development error(s) leads to a top-level failure condition.

A parallel is drawn between FFS and MCS in Appendix P, P.3.2.3: "an FFS is the equivalent to a fault tree MCS, whose members represent the result of potential development errors rather than failures.")

SAENORM.COM : Click to view the full PDF of arp4761a

Q.9.3.3.1 Loss of Wheel Braking Failure Condition

The FFSs/MCSs of the failure condition “Loss of wheel braking” are the following five single members:

a. {“ACTUATION.Loss”}

b. {“CTRL.Loss”}

c. {“EPWR.Loss”}

d. {“HPS.Loss”}

e. {“PEDALS.Loss”}

All FFSs/MCSs are of Order 1.

(Editor’s Note: In this example, the notation for the FFSs or for the MCSs is the following: { “XXXX.yyyy” } represents an FFS or a MCS of Order 1, where XXXX represents a block and where yyyy is one of the failure events of the block. { “XXXX.yyyy”, “AAAA.bbbb” } represents an FFS or a MCS of Order 2: { “XXXX.yyyy”, “AAAA.bbbb”, “TTTT.uuuu” } represents an FFS or a MCS of Order 3.)

Q.9.3.3.2 Uncommanded Wheel Braking Failure Condition

The FFSs/MCSs of the failure condition “Uncommanded braking (erroneous braking)” are:

a. {“ACTUATION.Untimely_Braking”}

b. {“CTRL.Untimely_Braking”}

c. {“PEDALS.Untimely_Braking”}

All FFSs/MCSs are of Order 1.

(Editor’s Note: As presented in Figure Q.9-2, the model does not consider any failure modes of Hydraulic Power Supply function or Electrical Power Supply resulting in untimely braking.)

Q.9.4 Satisfying PASA and Proposed Safety Requirements

This section discusses the evaluation of PASA input requirements and the development of proposed MBSA safety requirements.

Q.9.4.1 PASA-SR-01

PASA-SR-01	Decelerate Wheels Function shall be developed FDAL A.

Two functions contribute to the Decelerate Wheels function: the Control Wheel Braking function and the Actuate Wheel Braking Command function. As they are in series and as each function does not mitigate the failure modes of the other one, nor are independence attributes satisfied, these two functions shall be also developed in accordance with FDAL A objectives.

Proposed WBS safety requirement:

MBSA-SR-01	The Control Wheel Braking function and the Actuate Wheel Braking Command function shall be developed to FDAL A.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.9.4.2 PASA-SR-05

PASA-SR-015	Complete loss of wheel brake shall be less than 1.0E-07 for a landing.

Taking into account that there are five minimal cut sets of Order 1 identified by the high-level model, the allocation for failure rate to each block may be 1.00E-07 divided by 5. The result is given in Table Q.9-1.

(Editor's Note: The safety and design teams need to define the probability budget of each element. This can be done using two methods: Equal distribution or allocate based on failure rates of the different failure modes using engineering experience. In this example, the first way is chosen. The probability budgets are dependent on the architecture chosen, which is an organization activity. The safety team ensures that the choices meet the requirements.)

Table Q.9-1 - (PSSA - WBS - MBSA)
High-level model probability budget allocation for PASA-SR-015

Probability Budget	Events
2.00E-08	ACTUATION.Loss
2.00E-08	CTRL.loss
2.00E-08	EPWR.loss
2.00E-08	HPS.loss
2.00E-08	PEDALS.loss

Q.9.4.3 PASA-SR-XX

PASA-SR-XX	No single failure shall result in an uncommanded full symmetric wheel deceleration during a takeoff roll.

There are three MCSs of Order 1. As a result, each contributor (Actuation, CTRL and Pedals) shall also satisfy the no single failure criteria.

Q.9.4.4 PASA-SR-XY

PASA-SR-XY	Uncommanded full symmetric wheel deceleration shall be less than 1.0E-09 for a takeoff.

Taking into account that there are three minimal cut sets of Order 1, the allocation for failure rate to each block may be 1.00E-09 divided by 3. The result is given in Table Q.9-2.

Table Q.9-2 - (PSSA - WBS - MBSA)
High-level model probability budget allocation for PASA-SR-XY

Probability Budget	Events
3.33E-10	ACTUATION.Untimely_Braking
3.33E-10	CTRL.Untimely_Braking
3.33E-10	PEDALS.Untimely_Braking

Q.9.4.5 PASA-SR-12

PASA-SR-12	Loss of power from both hydraulic subsystems powered by the engines shall not lead to complete loss of wheel braking.

At this stage of development, this requirement is not fulfilled as there is only one HYD power supply and no other means to decelerate wheels or reverse thrust.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.9.4.6 PASA-SR-14

PASA-SR-14	Two redundant control lanes shall be provided between the Electric Brake Unit (EBU) and each of the two Alternate/Emergency Meter Valves.

At this stage of development, this requirement is not fulfilled: there is only one command path.

Q.9.5 High-Level WBS MBSA Model Outputs

The high-level model was a first step used to verify functional mapping based on available information that describe the inputs/outputs and functions of the system.

The model outputs have been used to support quantitative and qualitative allocations as well as evaluate and develop high-level requirements for the system. This was accomplished in an iterative manner with the other stakeholders of the design team.

The results analyses for the two failure conditions are summarized in the following sub-sections.

Q.9.5.1 Loss of Wheel Braking (1.1.TL)

Based on engineering experience, a simplex architecture is not technically capable of satisfying the safety objective of 1.00E-07 per flight hour (pfh).

Then, one solution is to use two hydraulic paths for braking. It requires two hydraulic sources and brake calipers as shown in Figure Q.9-4. By convention, one will be represented in blue and the other one in green.

SAENORM.COM : Click to view the full PDF of arp4761a

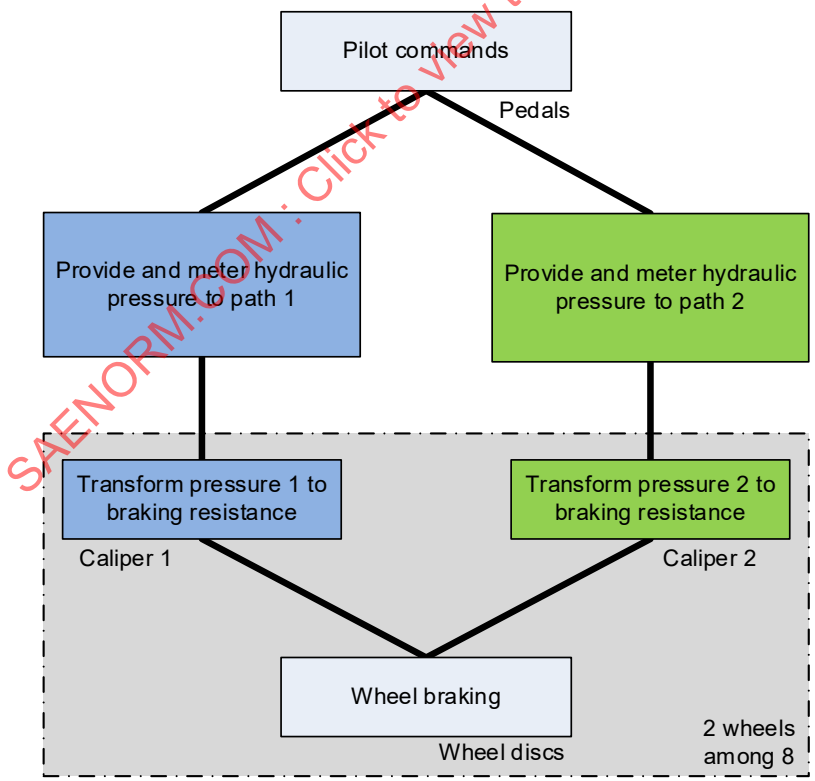


Figure Q.9-4 - (PSSA - WBS - MBSA)
Proposed architecture with two hydraulic paths

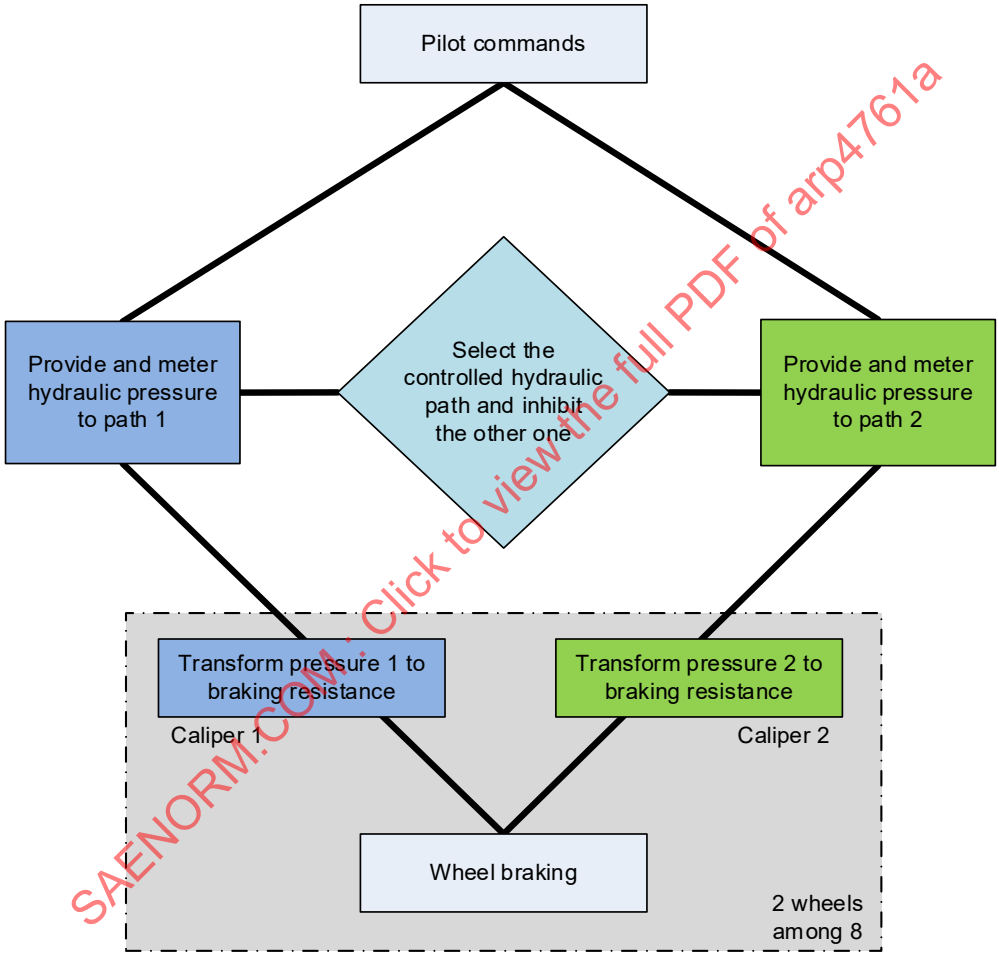
There is a need of minimum independence between path 1 and path 2. As this event is classified HAZ, a full Independence Principle is not required and the probability of a common cause that may defeat the independence would be acceptable under the condition that the occurrence rate is lower than 1.00E-07 pfh.

At this stage of the braking concept development, there are several ways to implement those two functions. One design choice was to avoid having two brake calipers working together at any time with only one path active and the other not active as shown in Figure Q.9-5.

The select function was a potential common point of failure between two paths for which a minimum independence is expected. This means that the design of this function, if not carefully executed, could have resulted in malfunction that rendered both paths active together, or worse both paths inactive together.

(Editor's Note: One important requirement coming from the PASA referenced PASA-SR-12 is the need to provide a wheel brake when both hydraulic sources are lost. This will be addressed later.)

Next, the question of the integrity of the control paths was addressed.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.9-5 - (PSSA - WBS - MBSA)
Proposed architecture with active/inhibited paths

Q.9.5.2 Uncommanded Wheel Braking (1.1.MF1)

The “No single failure criteria” was applicable to this Catastrophic failure condition.

Each path is susceptible to be in control and to provide hydraulic fluid pressure to the brake caliper. A single failure in the path control may directly lead to uncommanded braking. To cover the command failure cases that could lead to an uncommanded braking, each path needed a new “safety” function to mitigate these failures. The failures of erroneous or spuriously rising pressure, were mitigated by a means that shut off the hydraulic pressure propagation to the corresponding brake caliper. The mitigation function should, for instance:

- Stop the pressure (closing the path).
- Release the pressure (bypass/deviate the pressure and flow).

(Editor’s Note: Evaluating all of the possible solutions that may mitigate the uncommanded braking is not the aim of this example. Only some possible solutions are considered.)

The mitigation function may be placed upstream or downstream of the hydraulic metering function, as illustrated in Figure Q.9-6.

SAENORM.COM : Click to view the full PDF of arp4761a

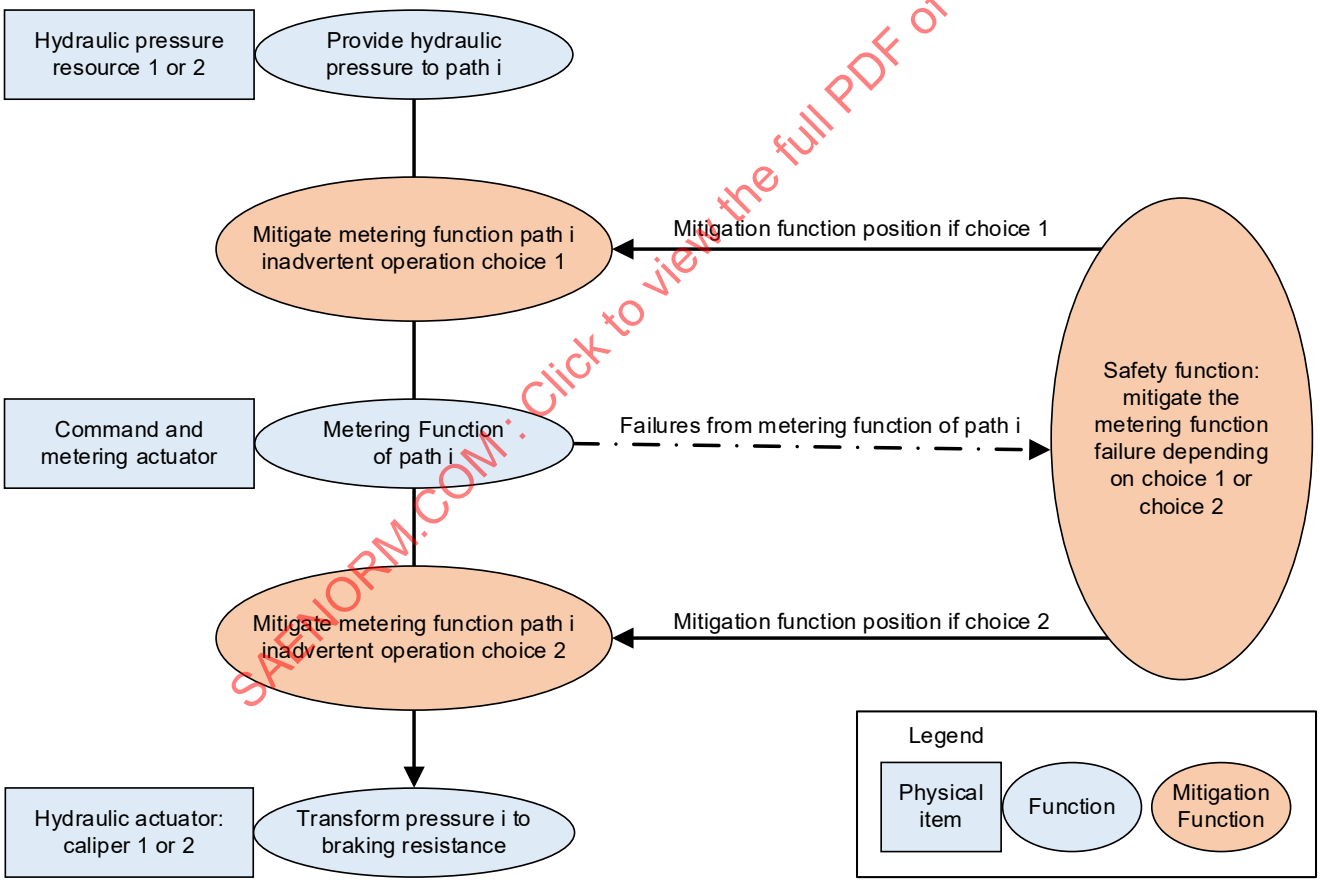


Figure Q.9-6 - (PSSA - WBS - MBSA)
Architecture rationale to justify what is necessary to mitigate the command failures

To prevent any uncommanded braking due to a single failure requires the following Independence Principle: “The functional chain that commands and actuates the metering function shall be independent from the functional chain that commands and actuates the mitigation function (shutoff function).”

Q.9.6 Low-Level WBS Model - First Iteration

The safety team evaluated the proposed system design organization architectures against the WBS safety requirements. To proceed, the safety team enriched the safety model by incorporating the new features chosen and defined by the system design organization.

As a result, the low-level model supports the PSSA process by refining the functions and by identifying new low-level safety requirements if any. During the PSSA activity, as the architecture was improved the model was adapted accordingly.

Q.9.6.1 Low-Level WBS Model MBSA Inputs

Q.9.6.1.1 Inputs from Design

There are multiple ways to allocate the different functions and interactions between the functions in order to satisfy all the requirements (e.g., safety, availability, weight, costs). Generally, the re-use of existing equipment or architectures influence the design choices that seriously impact the requirements refinement.

ARP4754B/ED-79B, Appendix E, E.4.6.2 gives a detailed description of the WBS initial architecture as shown in Figure Q.9-7.

SAENORM.COM : Click to view the full PDF of arp4761a

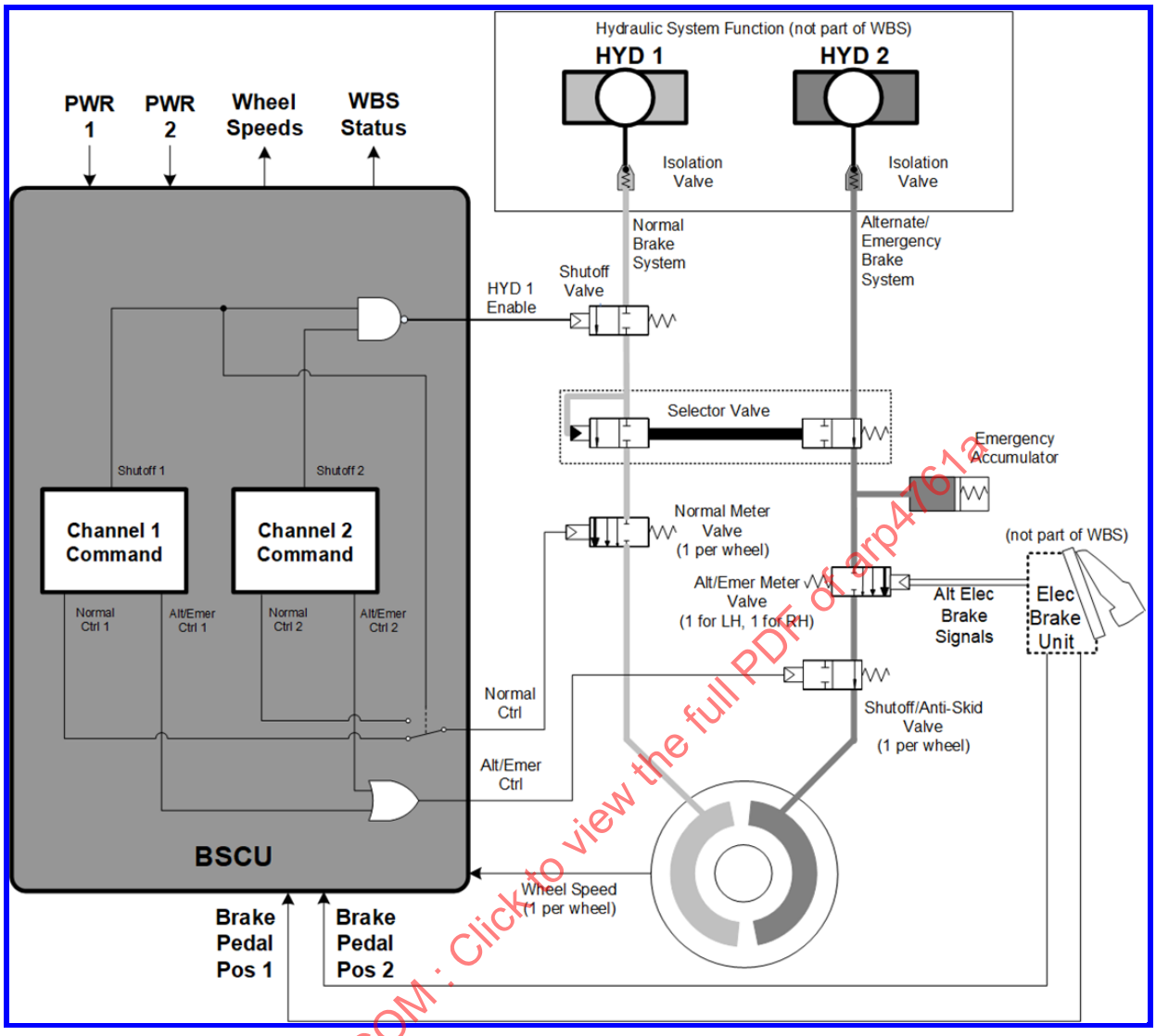


Figure Q.9-7 - (PSSA - WBS - MBSA)
WBS initial architecture diagram

SAENORM.COM : Click to view the full PDF of arp4761a

The following questions were raised by the safety team:

- Why the output signal of the Command 1 block is called “Shutoff 1” instead of “HYD 1 Enable”?
- Why the NAND gate logic is used to build the output signal of the BSCU called “HYD 1 Enable”?
- Why the OR-gate logic is used to build the output signal of the BSCU called “Alt/Emer Ctrl”?
- What prevents both Command 1 and 2 from being active?
- Why the logic for the Alt/Emer Ctrl is not the same as the logic used to control the Normal Meter Valve (NMV)?
- What about the lack of Internal Power to adapt the external power supply to the BSCU?
- If no internal validity is considered for each command, how is it possible to command the Shutoff/Anti-Skid Valve?
- How are the Command 1 and Command 2 aware of the HYD 1 status? [Not answered at this stage.]

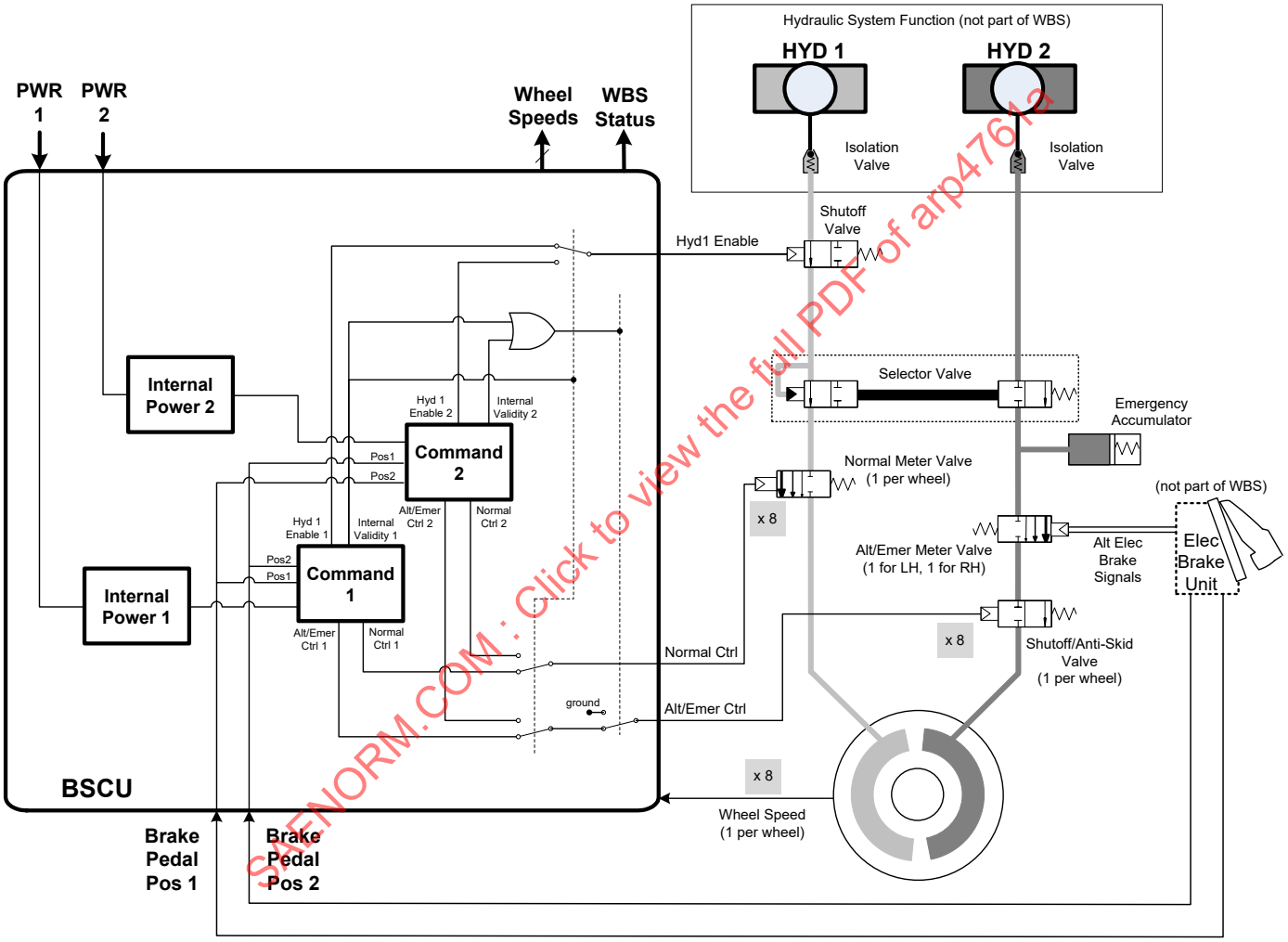
After discussions and some explanations from the design organization, Figure Q.9-7 was revised as shown in Figure Q.9-8.

Q.9.6.2 Analysis of Different Operational Modes

In order to understand the functional/reconfiguration behavior, some operating modes were analyzed and verified, with the support of the design team, as shown in Figures Q.9-9 to Q.9-13.

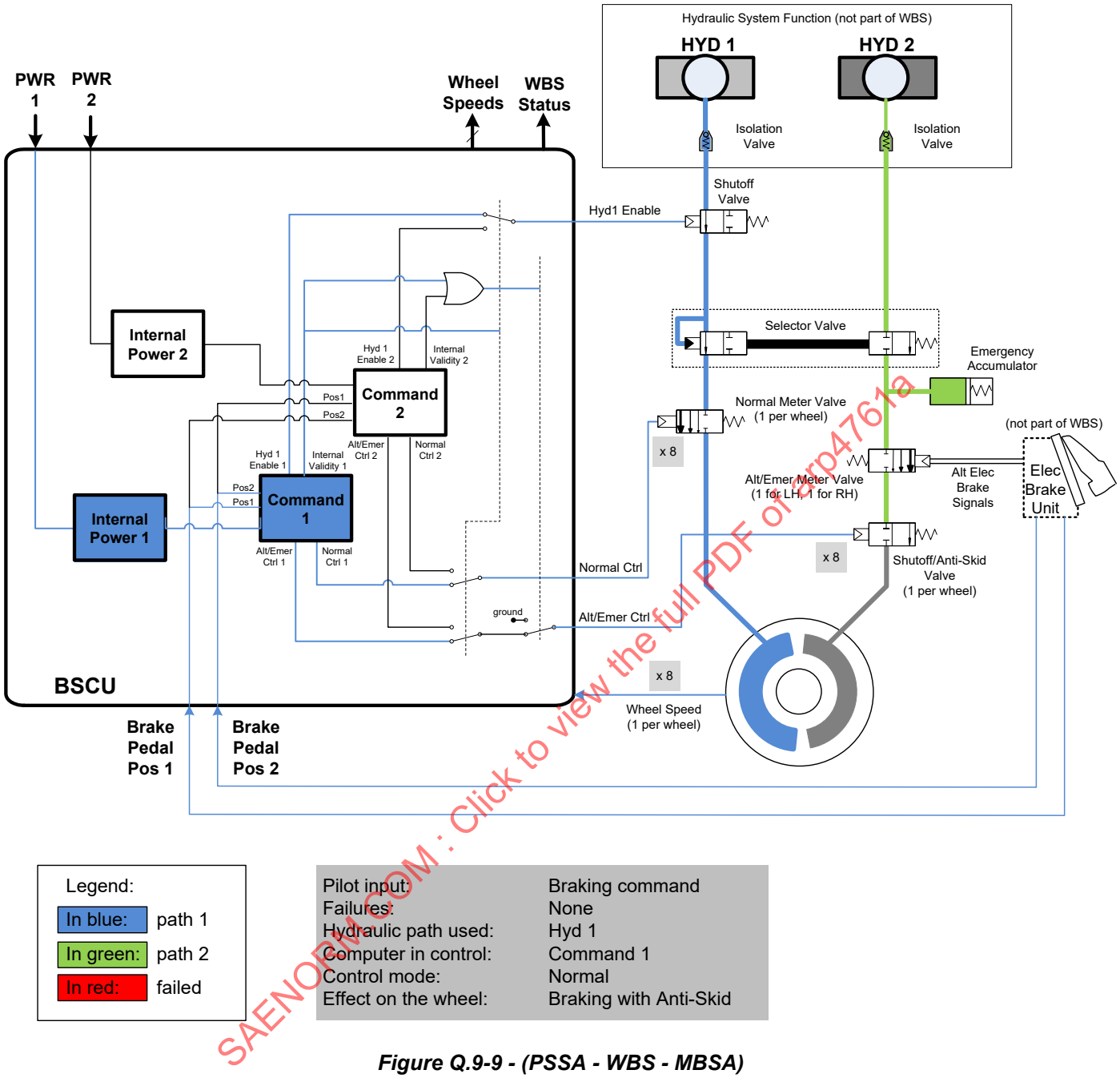
In flight (main landing gear retracted), the BSCU inhibits HYD 1 (for the Braking System) and enables HYD 2 in order to fill the emergency accumulator. The BSCU then reverts back to command the HYD 1 path after main landing gear extension.

In NORMAL Mode (Figure Q.9-9), HYD 1 is available, the Shutoff Valve is open, the Selector Valve is in the Normal position and the Command 1 controls the Normal Meter Valve to brake with Anti-Skid. The Shutoff/Anti-Skid Valve remains closed to keep the emergency accumulator full and avoid any twin control conflicts.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.9-8 - (PSSA - WBS - MBSA)
WBS architecture diagram revision



Legend:

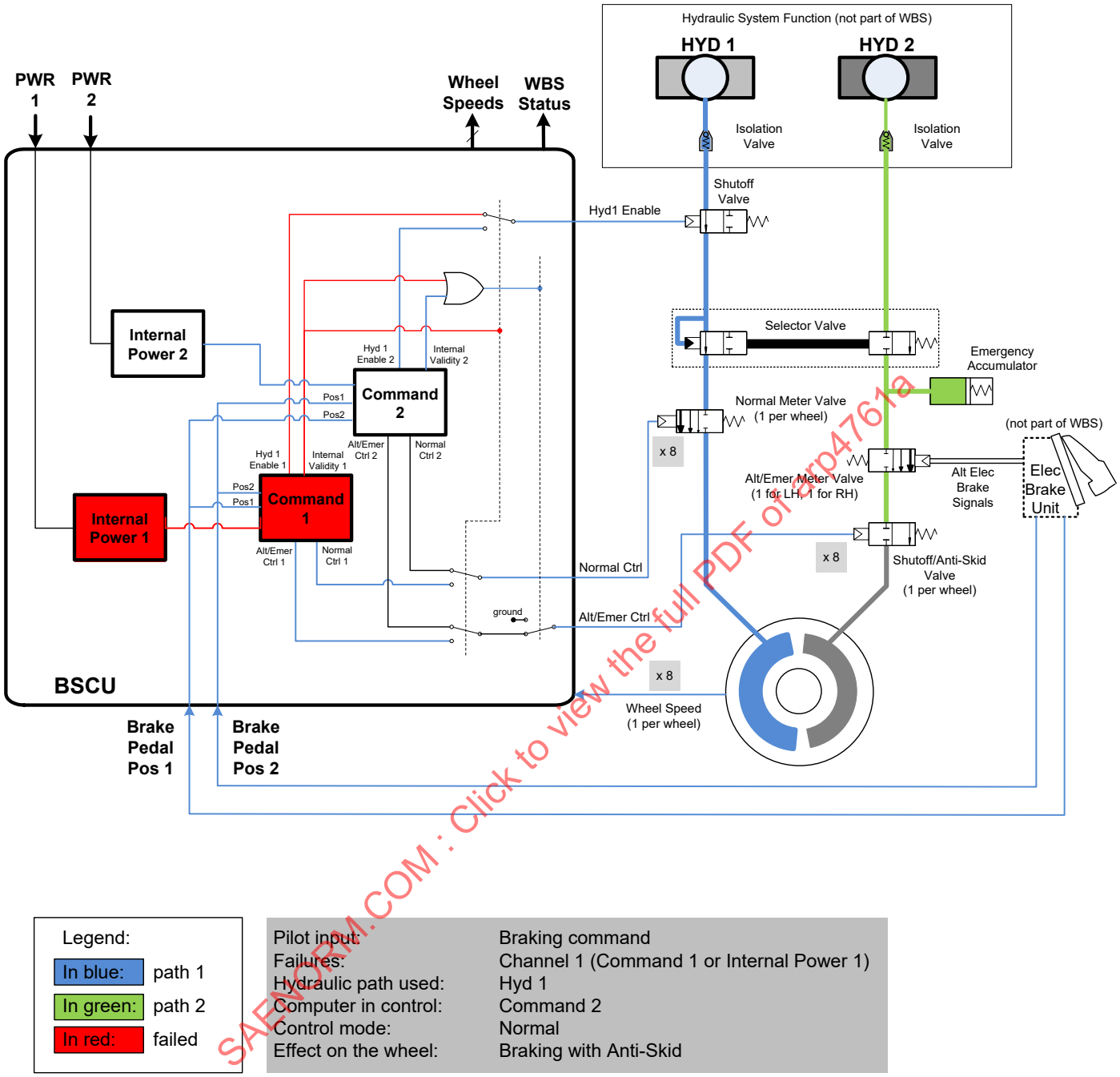
In blue:	path 1
In green:	path 2
In red:	failed

Pilot input:	Braking command
Failures:	None
Hydraulic path used:	Hyd 1
Computer in control:	Command 1
Control mode:	Normal
Effect on the wheel:	Braking with Anti-Skid

SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.9-9 - (PSSA - WBS - MBSA) NORMAL mode

In case of a detected failure of Channel 1 (e.g., loss of Internal Power 1 or loss of Command 1), the BSCU switches to Channel 2, as shown in Figure Q.9-10. The system remains in NORMAL mode.



SAENORM.COM : Click to view the full PDF of arp4761a

Legend:	
In blue:	path 1
In green:	path 2
In red:	failed

Pilot input:	Braking command
Failures:	Channel 1 (Command 1 or Internal Power 1)
Hydraulic path used:	Hyd 1
Computer in control:	Command 2
Control mode:	Normal
Effect on the wheel:	Braking with Anti-Skid

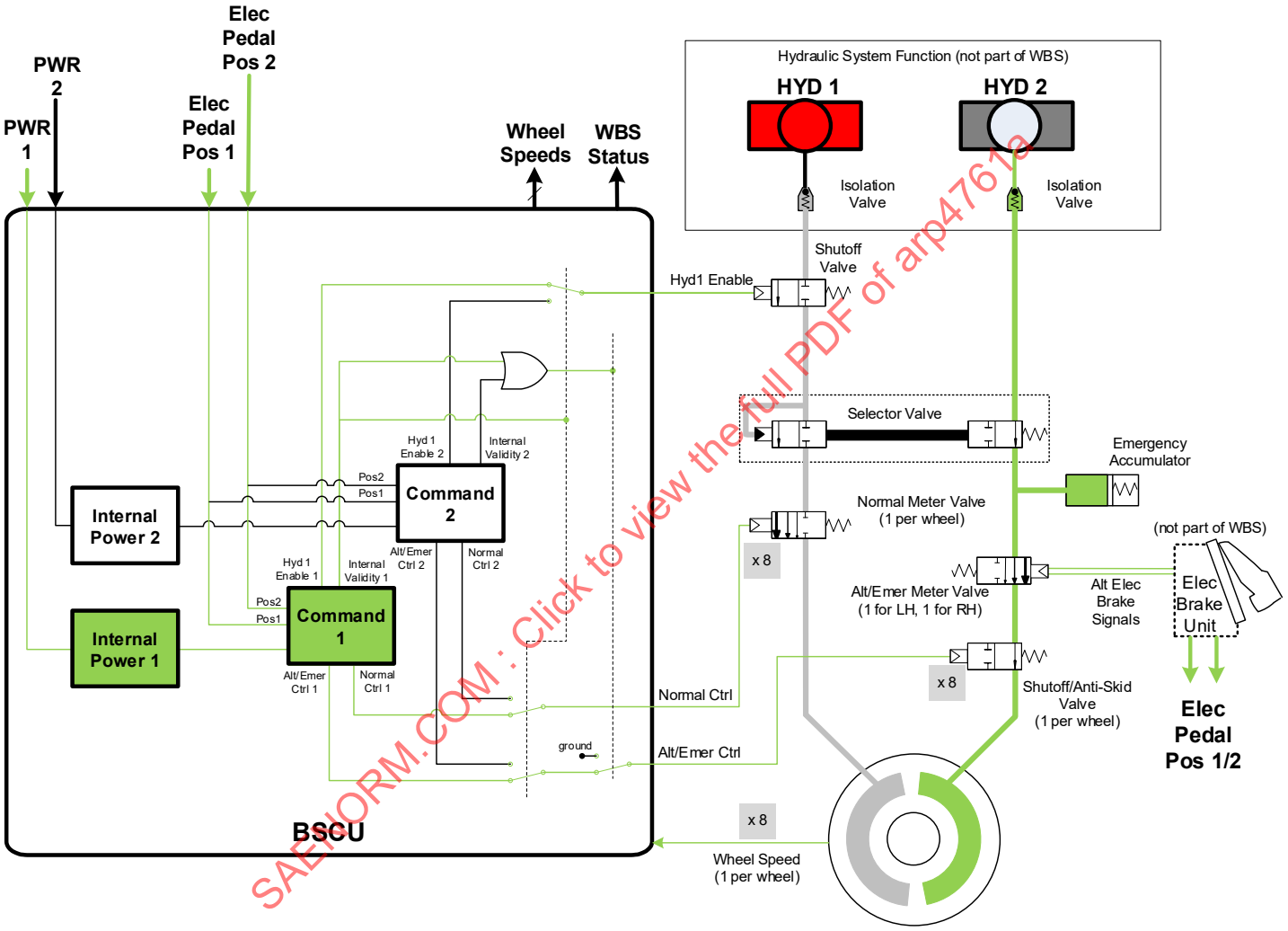
Figure Q.9-10 - (PSSA - WBS - MBSA)
NORMAL Mode with Channel 1 failure

There is a lack of direct information from HYD 1 path status at the output of the Selector Valve, which is common to the eight HYD 1 wheel paths and to the Command blocks (e.g., no inputs from a pressure sensor). This status would be useful to detect HYD 1 path loss and then to switch from NORMAL Mode to ALTERNATE Mode. As a consequence, an assumption was made and will have to be confirmed by the design team:

MBSA-BSCU-R-01	If Braking is commanded, the loss of braking on at least three wheels triggers the switch from NORMAL Mode to ALTERNATE Mode and a switch from the HYD 1 path to HYD 2 path.

The analysis considered that the cause of the loss of braking is much more likely to be a HYD 1 failure than the failure of three items among wheel speed sensors and NMVs. This rationale is based on failure rate considerations: the loss of one Wheel Speed Sensor failure rate is on the order of 1.00E-05 pfh and the loss of one NMV failure rate is on the order of 5.00E-06 pfh. Thus, the loss of three sensors results in a failure rate of approximately 1.00E-15 pfh (the loss of two sensors and the NMV failure rate is 5.00E-16 pfh), which is much lower than loss of HYD 1 failure rate of approximately 3.3E-05 pfh.

Starting from an initial state (no failure): if HYD 1 is lost (low pressure), the Selector Valve switches to Alternate path position, the Shutoff Valve is closed and the system switches to ALTERNATE Mode (see Figure Q.9-11). The HYD 2 path is now active. Command 1 controls the shutoff/anti-skid to brake with anti-skid (pulse command).



SAENORM.COM : Click to view the full PDF of arp4761a

Legend:	
In blue:	path 1
In green:	path 2
In red:	failed

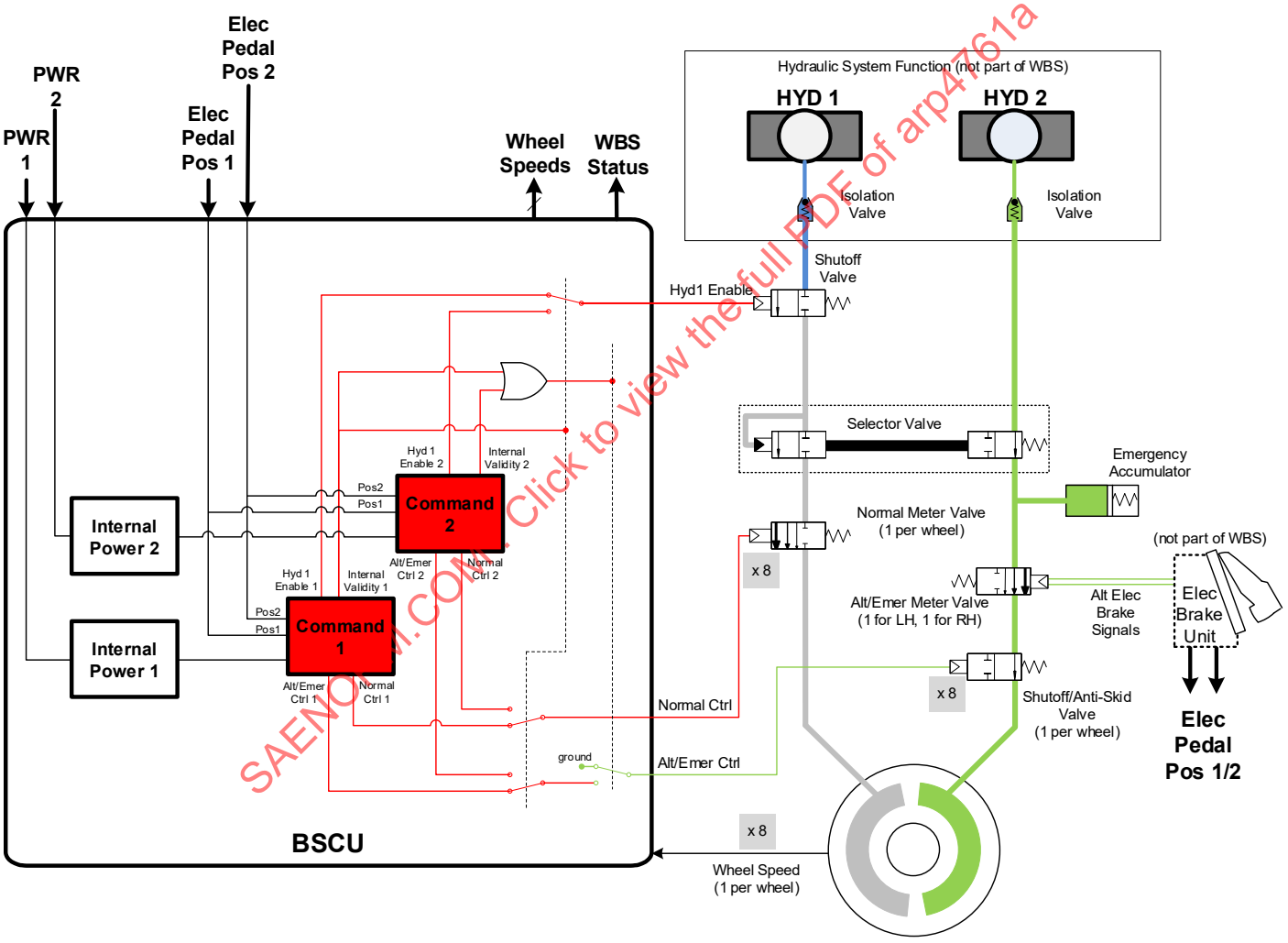
Pilot input:	Braking command
Failures:	Hyd 1
Hydraulic path used:	Hyd 2
Computer in control:	Command 1
Control mode:	Alternate
Effect on the wheel:	Braking with Anti-Skid

Figure Q.9-11 - (PSSA - WBS - MBSA)
ALTERNATE Mode with anti-skid

Another assumption was identified for confirmation by the design team:

MBSA-BSCU-R-02	The Shutoff Valve is used to control the Selector Valve in order to: - Fill the emergency accumulator in flight (main landing gears retracted). - Avoid unstable commutations between HYD 1/HYD 2. - Provide a mitigation means for a Normal Meter Valve failure which leads to an uncommanded braking of one wheel (risk of tire burst).* *Not in the frame of the study.

Starting from an initial state (i.e., no failure): if both commands are lost or invalid (due for instance to a software development error), the system switches to EMERGENCY Mode (Figure Q.9-12). In this case, the Shutoff/Anti-Skid Valve is no longer controlled and remains in the open position. The pilot will directly control braking according to the pedal position.



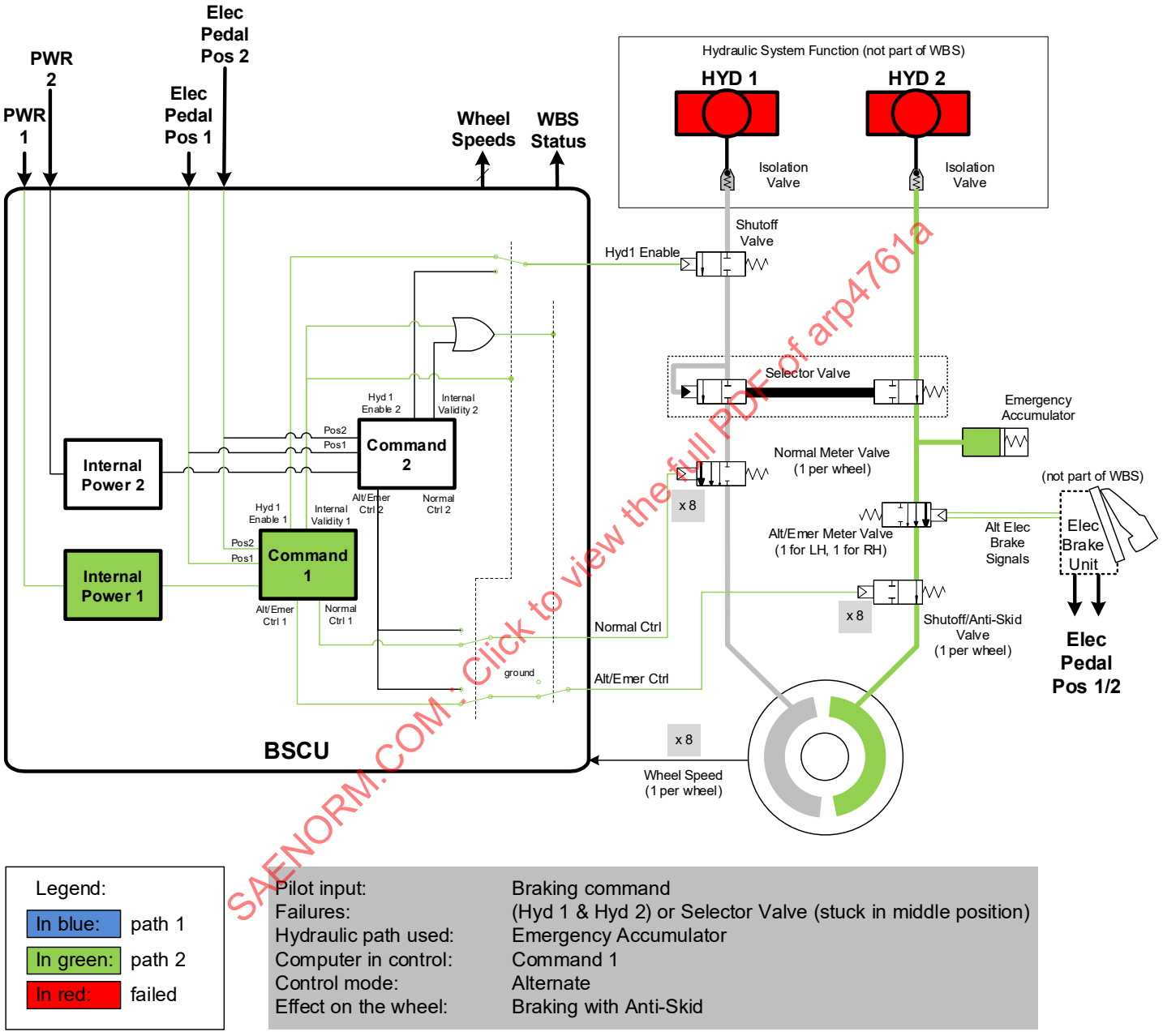
SAENORM.COM : Click to view the full PDF of arp4761a

Legend:
- In blue: path 1
- In green: path 2
- In red: failed

Pilot input:	Braking command
Failures:	Channel 1 and Channel 2 (common mode)
Hydraulic path used:	Hyd 2
Computer in control:	None (direct pilot command)
Control mode:	Emergency
Effect on the wheel:	Braking without Anti-Skid

Figure Q.9-12 - (PSSA - WBS - MBSA)
EMERGENCY Mode

Starting from an initial state (no failure): if no hydraulic power is available (e.g., loss of HYD 1 and HYD 2, or failure of the Selector Valve blocked in middle position), the system switches to ALTERNATE Mode (Figure Q.9-13). Command 1 controls the Shutoff/Anti-Skid Valve to brake with anti-skid (pulse command). ALTERNATE Mode is time limited due to emergency accumulator capacity.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.9-13 - (PSSA - WBS - MBSA)
ALTERNATE Mode using emergency accumulator

In ALTERNATE Mode, the HYD 2 Isolation Valve guarantees that the hydraulic coming from the emergency accumulator is dedicated to Braking Function (i.e., HYD 2 is not used by other airplane HYD 2 consumers).

Q.9.6.3 Architecture Candidate Hypotheses

In addition to the Figures Q.9-8 to Q.9-13 diagrams, some hypotheses were established:

- Basic hypotheses from the aircraft multisystem safety team (PASA):
  - Hydraulic circuits can be considered independent with an individual failure rate of 3.30E-05 pfh.
  - Electrical circuits can be considered independent with an individual failure rate of 1.00E-04 pfh.
- Basic hypotheses from the wheel braking design team:
  - All wheels capable of providing braking functionality were fitted with braking actuators on both hydraulic circuits.
  - BSCU de-energizes the Shutoff Valve in flight, when the main landing gear are retracted. As a result, the emergency accumulator can be considered as filled up when it would be required even if it is downstream of the Selector Valve.

Q.9.7 Low-Level WBS Model Iterations

The updated (first iteration) WBS was implemented in the model as shown in Figure Q.9-14.

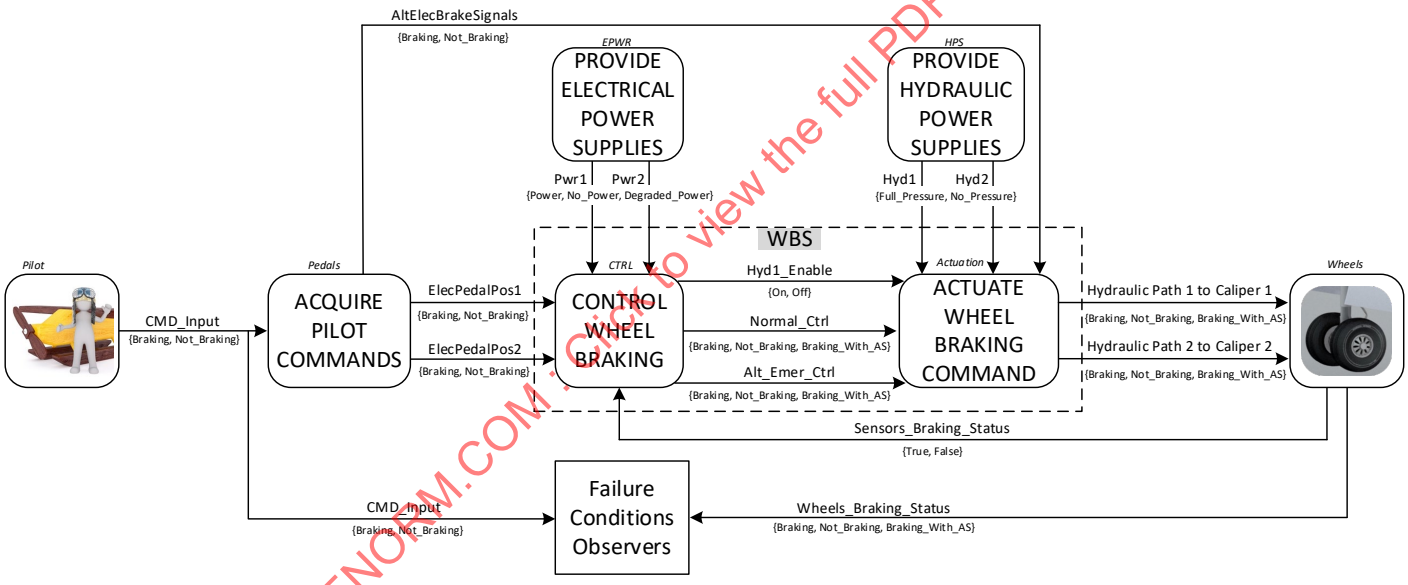


Figure Q.9-14 - (PSSA - WBS - MBSA)
WBS low-level model first iteration

SAENORM.COM : Click to view the full PDF of arp4761a

The low-level WBS model and the flows were refined at this stage:

- For electrical power supplies, the effect of Degraded_Power as it may affect the behavior of the BSCU is now considered.
- For hydraulic power supplies, no change was introduced as the focus is on the BSCU behavior.
- The Braking_With_AS value in the internal system command flow was introduced in order to differentiate a full braking (which may block the wheels) and a braking with anti-skid.

- The Sensors_Braking_Status was added to implement the MBSA-BSCU-R-01 assumption. To be consistent with Section Q.5 (SFHA) Table Q.5-4 “Total loss of wheel deceleration (80% coverage or more),” the status values were defined as follows:
    - False if at least three of eight wheels are not braking (in case braking command was commanded).
    - True otherwise.

In order to revise the model, the following assumptions have been considered:

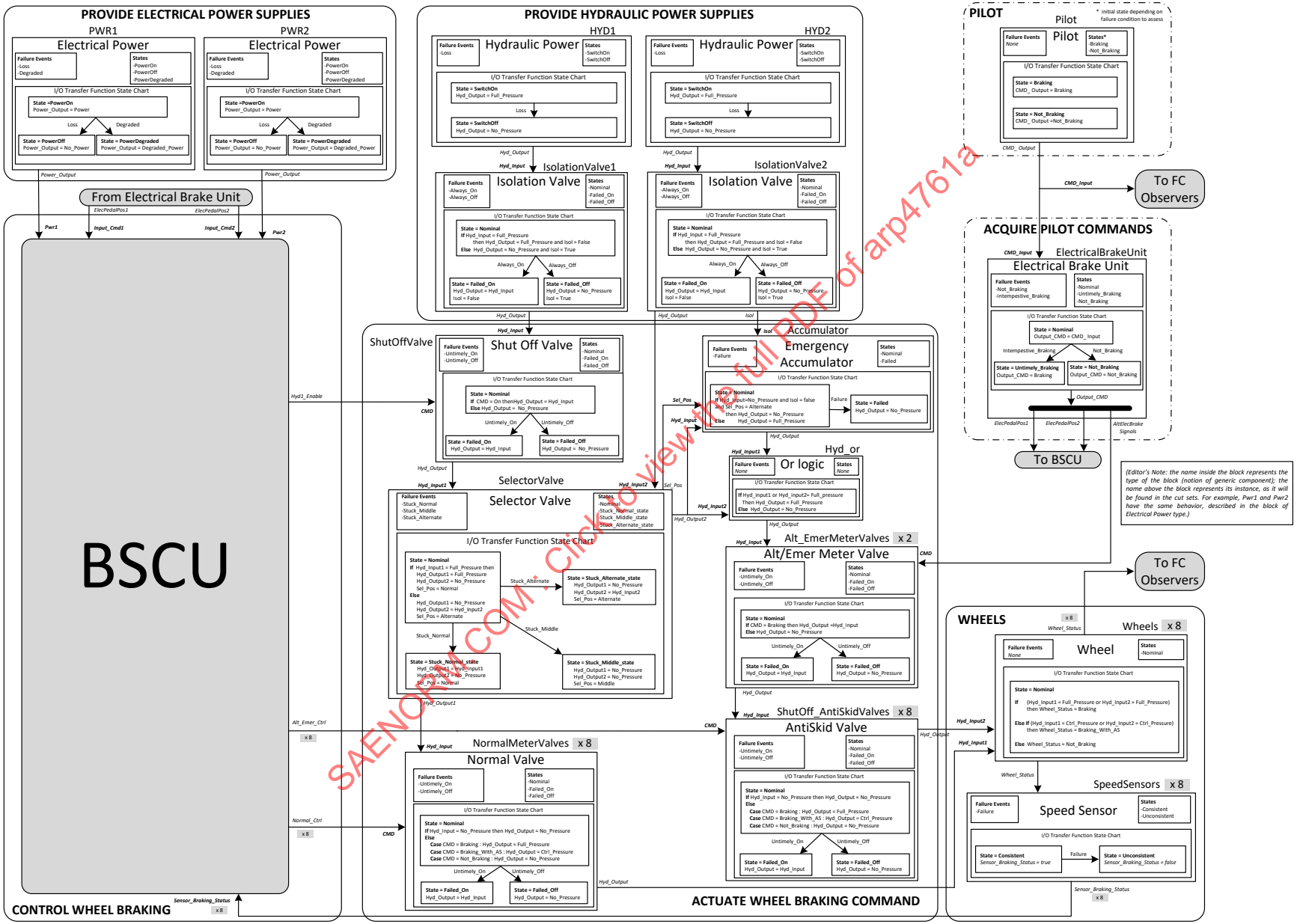
MBSA-BSCU-R-03	Electric Brake Unit (EBU) As the internal architecture of the EBU (e.g., number of sensors, number of pedals, electrical power supply was unknown, the EBU was considered a monolithic block which provides the three position data. As a consequence, only two failure modes were retained; one leading to a Not_Braking state, the other one leading to an Untimely_Braking state.
MBSA-BSCU-R-04	BSCU/EBU interface The two signals coming from the EBU were used inside the BSCU with the following logic: both signals shall be consistent to execute the braking command.
MBSA-BSCU-R-05	BSCU Command In case of Degraded Power, the worst-case was considered: the Internal Validity is still true and the output command is the opposite of the input command request.

These assumptions have to be confirmed/infirmed by the design organization for the next model iteration.

The updated WBS low-level model first iteration is shown in Figure Q.9-15.

The BSCU low-level model first iteration is shown in Figure Q.9-16.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.9-15 - (PSSA - WBS - MBSA)
WBS detailed low-level model first iteration

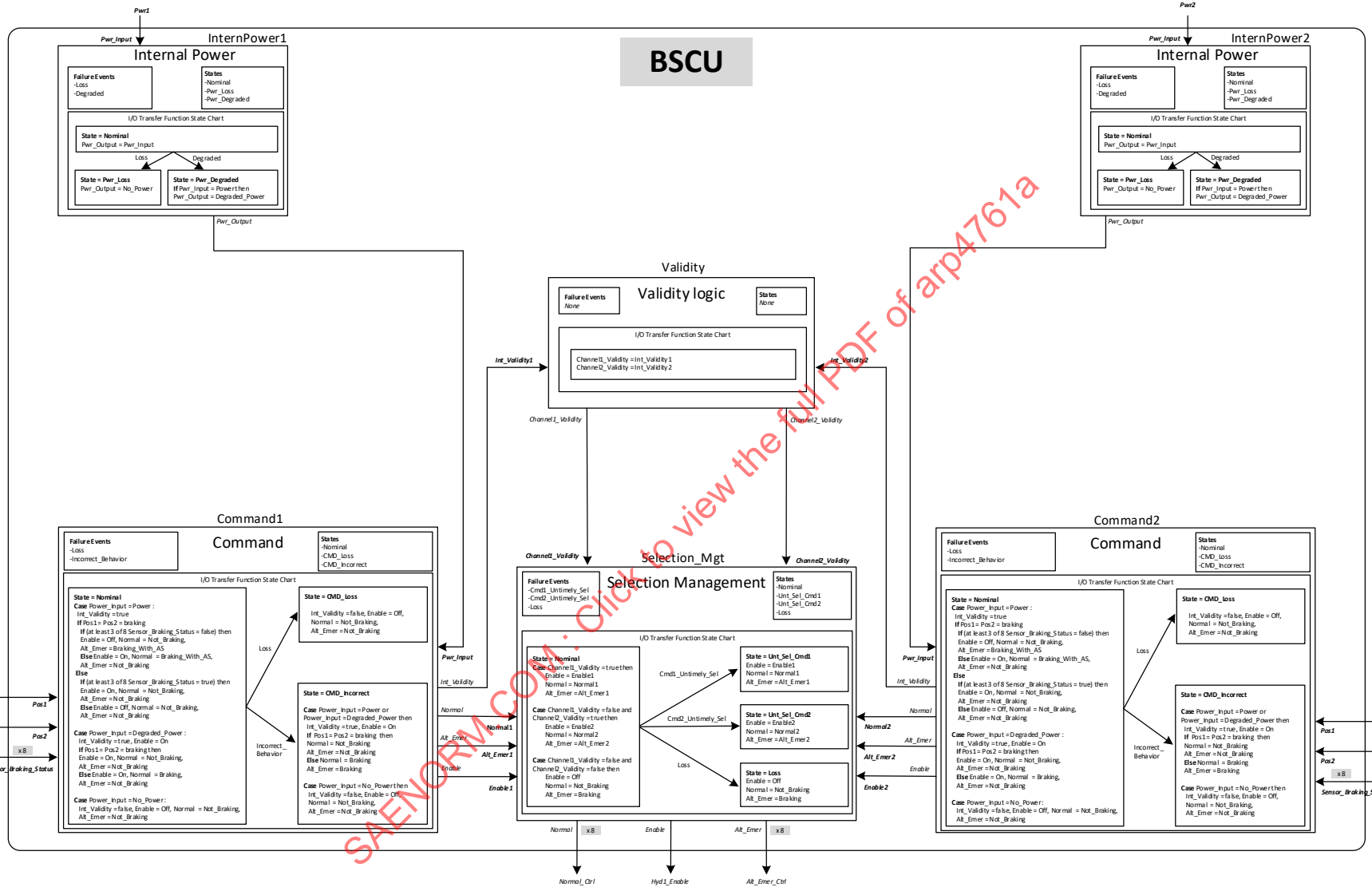


Figure Q.9-16 - (PSSA - WBS - MBSA)
BSCU detailed low-level model first iteration

Finally, the failure conditions observers were modeled as shown in Figure Q.9-17.

To be consistent with Section Q.5 (SFHA) Table Q.5-4, the “Total loss of wheel deceleration (80% coverage or more)” failure condition was reached if at least 7 out of 8 wheels were not braking (whereas pilot command is braking).

In the same manner, the “Uncommanded braking” failure condition was reached if at least 7 out of 8 wheels were braking (whereas pilot command is not braking) (80% coverage or more).

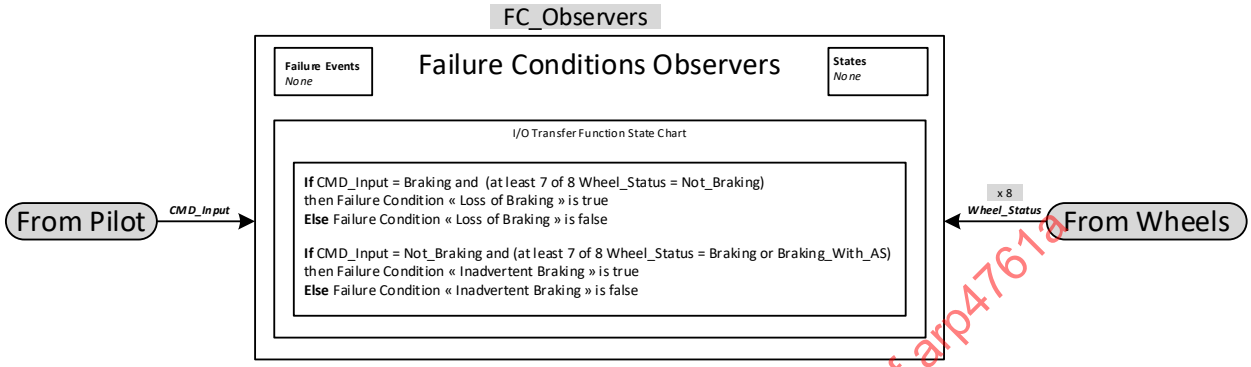


Figure Q.9-17 - (PSSA - WBS - MBSA)
Failure Conditions Observers block

Q.9.8 First Iteration MBSA Failure Condition Evaluation

Q.9.8.1 Loss of Wheel Braking Failure Condition

Table Q.9-3 presents the quantity of Functional Failure Sets/Minimal Cut Sets of the failure condition “Loss of wheel braking,” truncated to the Order 3.

Table Q.9-3 - (PSSA - WBS - MBSA)
Quantity of “Loss of wheel braking” FFSs/MCSs

Order of FFS/MCS	Number
Total	**49**
1	4
2	19
3	26

The Functional Failure Sets/Minimal Cut Sets, truncated to the Order 1, were the following:

a. {“COMMAND1.Incorrect_Behavior”}

b. {“ELECTRICALBRAKEUNIT.Not_Braking”}

c. {“INTERNALPOWER1.Degraded”}

d. {“PWR1.Degraded”}

SAENORM.COM : Click to view the full PDF of arp4761a

The computation regarding the loss of braking was done for a whole flight (5 flight hours). Table Q.9-4 presents the summary of minimal cut sets, truncated to the Order 3, with the respective computed probabilities:

Table Q.9-4 - (PSSA - WBS - MBSA)
"Loss of wheel braking" probability computation first iteration

Order of MCS	Number	Probability (per flight)
Total	**49**	**1.1310E-04**
1	4	1.1300E-04
2	19	1.0242E-07
3	26	2.9326E-12

Q.9.8.2 Uncommanded Wheel Braking failure condition

Table Q.9-5 presents the quantity of Functional Failure Sets/Minimal Cut Sets of the "Uncommanded wheel braking" failure condition, truncated to the Order 3:

Table Q.9-5 - (PSSA - WBS - MBSA)
Quantity of "Uncommanded Wheel Braking" FFSs/MCSs

Order of FFS/MCS	Number
Total	**17**
1	4
2	12
3	1

The Functional Failure Sets/Minimal Cut Sets, truncated to the Order 1, were the following:

a. {"COMMAND1.Incorrect_Behavior"}

b. {"ELECTRICALBRAKEUNIT. Untimely_Braking}

c. {"INTERNALPOWER1.Degraded"}

d. {"PWR1.Degraded"}

(Editor's Note: As explained in Q.9.3.3, the model "failure events" can represent either development errors or random failures. As a result, "Command1.Incorrect_Behavior" represents a development error that may lead to the incorrect behavior of Command1 when considering FFS, whereas it also represents a random failure of Command1 (failure rate: 1.00E-06 pfh) that leads to the incorrect behavior of Command1 when considering MCS.)

The computation regarding the uncommanded braking was done for a given time risk exposure (10 minutes for a takeoff). Table Q.9-6 presents the summary of MCSs, truncated to the Order 3, with the respective computed probabilities.

Table Q.9-6 - (PSSA - WBS - MBSA)
"Uncommanded Wheel Braking" probability computation

Order of MCS	Number	Probability (per flight)
Total	**17**	**3.7667E-06**
1	4	3.7667E-06
2	12	7.5599E-11
3	1	1.3888E-18

SAENORM.COM : Click to view the full PDF of arp4761a

Q.9.8.3 Satisfying PASA and Refined Safety Requirements

Q.9.8.3.1 PASA-SR-01

PASA-SR-01	Decelerate Wheels Function shall be developed FDAL A.
MBSA-SR-01	The Control Wheel Braking function and the Actuate Wheel Braking Command function shall be developed to FDAL A.

These requirements were not evaluated during this iteration.

Q.9.8.3.2 PASA-SR-05

PASA-SR-05	Complete loss of wheel brake shall be less than 1.0E-07 for a landing.

At this stage in development, this requirement was not fulfilled, due to the probabilities of the four MCSs of Order 1.

Q.9.8.3.3 PASA-SR-XX

PASA-SR-XX	No single failure shall result in an uncommanded full symmetric wheel deceleration during a takeoff roll.

At this stage of development, this requirement was not fulfilled, due to four MCSs of Order 1.

Q.9.8.3.4 PASA-SR-XY

PASA-SR-XY	Uncommanded full symmetric wheel deceleration shall be less than 1.0E-09 for a takeoff.

At this stage of development, this requirement was not fulfilled, due to the probabilities of the four MCSs of Order 1.

Q.9.8.3.5 PASA-SR-12

PASA-SR-12	Loss of power from both hydraulic subsystems powered by the engines shall not lead to complete loss of wheel braking.

This requirement was fulfilled due to the emergency accumulator integration.

Q.9.8.3.6 PASA-SR-14

PASA-SR-14	Two redundant control lanes shall be provided between the Electric Brake Unit (EBU) and each of the two Alternate/Emergency Meter Valves.

This requirement was fulfilled by design.

Q.9.8.4 First Iteration Low-Level Model MBSA Outputs

The cut sets presented in Section Q.9.8.2 show that there were four MCSs of first order. This implies that safety requirement PASA-SR-XX, PASA-SR-XY and PASA-SR-05 could not be fulfilled.

The MCSs corresponded to an erroneous output of the BSCU command Channel 1, due to the erroneous command, due to the power supply, or due to the EBU.

SAENORM.COM : Click to view the full PDF of arp4761a

Thus, safety team recommendation was to evolve the architecture of the BSCU to a dual redundant command/monitor, with power supply monitoring.

(Editor's Note: As the EBU was not part of the MBSA example study, its failure modes will not be taken into account for the next iteration.)

Q.9.9 Low-Level Model - Second Iteration

The safety team enhanced the first iteration MBSA functional model using the new descriptions and operating characteristics.

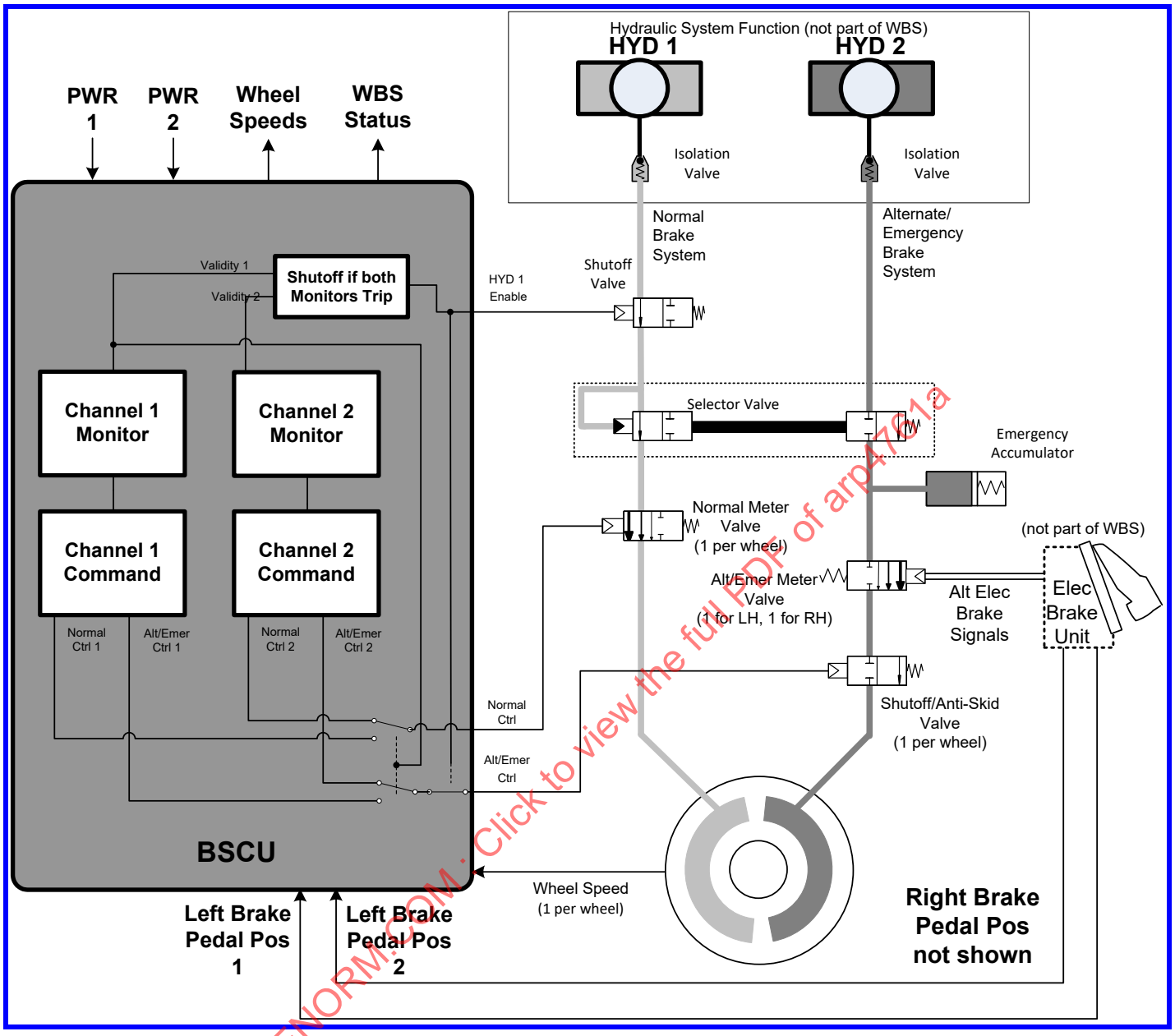
Q.9.9.1 Second Iteration Low-Level Model MBSA Inputs

Each channel of the BSCU was now fitted with a device which monitors:

- The internal power supply output, as the behavior of the control components cannot be assessed when powered by degraded power supply, due to either Internal or external power supply failures.
- The behavior of the control function outputs, as well HYD 1 Enable as Normal and Alt/Emer Control signals.

Figure Q.9-18 captures the upgraded WBS architecture described in ARP4754B/ED-79B, Appendix E, E.4.6.9.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.9-18 - (PSSA - WBS - MBSA)
WBS upgraded architecture

After some explanations and reviews with the design organization, Figure Q.9-18 evolved as shown in Figure Q.9-19.

(Editor's Note: The EBU Right and Left Brake pedal position signals 1 and 2 interface model, captured in Figure Q.9-19 and used in the MBSA is different than those presented in the FMEA example (Q.10).)

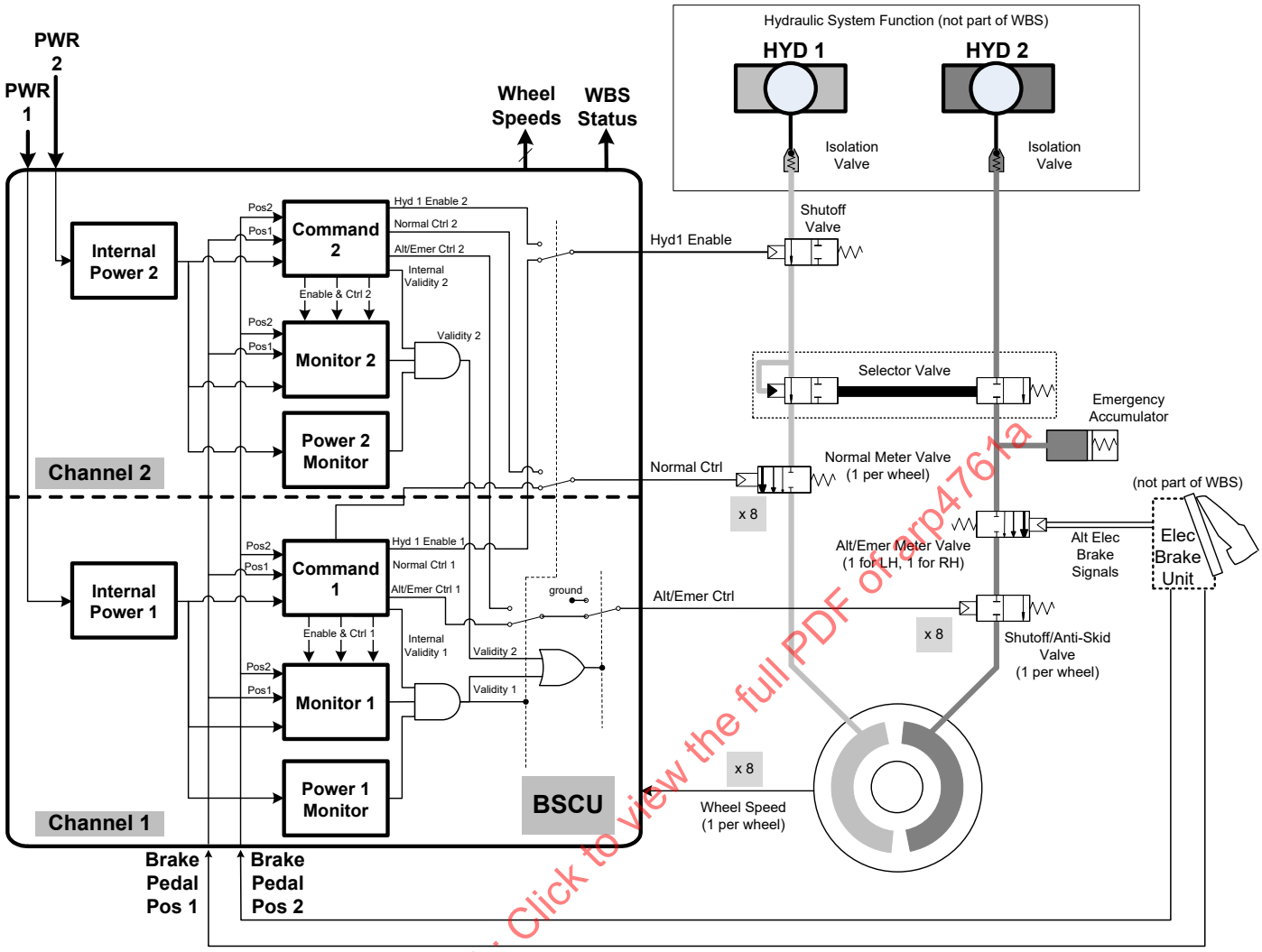


Figure Q.9-19 - (PSSA - WBS - MBSA)
WBS reviewed architecture second iteration

SAENORM.COM : Click to view the full PDF of arp4761a

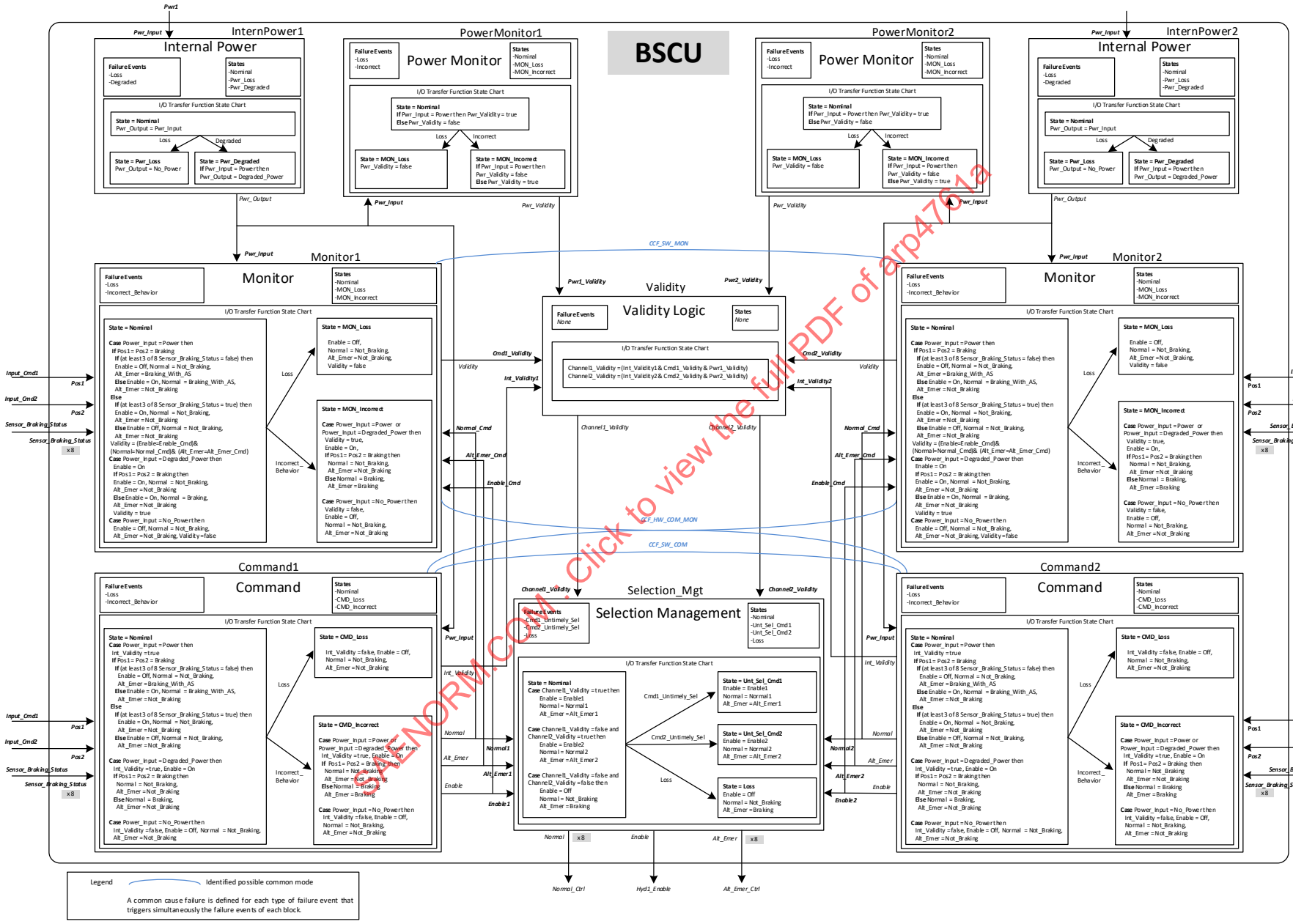
Q.9.9.2 Second Iteration Low-Level MBSA Model

In order to update the model, the following assumptions were considered:

MBSA-BSCU-R-06	Power Monitor If Power Monitor is lost, the output validity is false. This initiates a switch to the other channel. If Power Monitor is incorrect, the output validity is contrary to the real one.
MBSA-BSCU-R-07	Monitor If Monitor is lost or not powered, the output validity is false. This initiates a switch to the other channel. If Monitor is incorrect and powered, validity is always true (no detection)

These assumptions have to be confirmed/infirmed by the design organization for the next model iteration.

The updated second iteration low-level BSCU model was implemented as shown in Figure Q.9-20.



ARENORM.COM : Click to view the full PDF of arp4761a

Figure Q.9-20 - (PSSA - WBS - MBSA)
BSCU detailed low-level model second Iteration

Based on the development process plan captured in PSSA Q.6.4.3.1.2, the following electronic hardware and software common causes have been added to the Figure Q.9-20 model (highlighted as blue connections in Figure Q.9-20):

a. “CCF_HW_COM_MON”: potential COM/MON hardware development errors.

b. “CCF_SW_COM”: potential COM software development errors.

c. “CCF_SW_MON”: potential MON software development errors.

(Editor’s Note: In the scope of this example, only BSCU common error and failure causes have been considered. Other common causes could have been taken into account (e.g., internal power, power monitor, Shutoff/Anti-Skid Valves, Normal/Alt Emer Valves, wheel sensors).

Q.9.9.3 Second Iteration Low-Level Model MBSA Failure Condition Evaluation

Q.9.9.3.1 Loss of Wheel Braking Failure Condition

Table Q.9-7 presents the quantity of FFSs of the “Loss of wheel braking”, truncated to Order 3:

Table Q.9-7 - (PSSA - WBS - MBSA)
Quantity of “Loss of wheel braking” FFSs second iteration

Order of FFS	Number
Total	**119**
1	1
2	25
3	92

The FFSs, truncated to the Order 1 and 2, were the following:

a. {“CCF_HW_COM_MON_Incorrect”}

b. {“CCF_HW_COM_MON_LOSS”, “SELECTION_MGT.Cmd1_Untimely_sel”}

c. {“CCF_HW_COM_MON_LOSS”, “SELECTION_MGT.Cmd2_Untimely_sel”}

d. {“CCF_SW_COM_INCORRECT”, “CCF_SW_MON_Incorrect”}

e. {“CCF_SW_COM_INCORRECT”, “MONITOR1.Incorrect_Behavior”}

f. {“CCF_SW_COM_INCORRECT”, “MONITOR2.Incorrect_Behavior”}

g. {“CCF_SW_COM_INCORRECT”, “SELECTION_MGT.Cmd1_Untimely_sel”}

h. {“CCF_SW_COM_INCORRECT”, “SELECTION_MGT.Cmd2_Untimely_sel”}

i. {“CCF_SW_COM_LOSS”, “SELECTION_MGT.Cmd1_Untimely_sel”}

j. {“CCF_SW_COM_LOSS”, “SELECTION_MGT.Cmd2_Untimely_sel”}

k. {“CCF_SW_MON_INCORRECT”, “COMMAND1.Incorrect_Behavior”}

l. {“COMMAND1.Incorrect_Behavior”, “MONITOR1.Incorrect_Behavior”}

m. {“COMMAND1.Incorrect_Behavior”, “SELECTION_MGT.Cmd1_Untimely_sel”}

SAENORM.COM : Click to view the full PDF of arp4761a

n. {“COMMAND1.Loss”, “SELECTION_MGT.Cmd1_Untimely_sel”}

o. {“COMMAND2.Incorrect_Behavior”, “SELECTION_MGT.Cmd2_Untimely_sel”}

p. {“COMMAND2.Loss”, “SELECTION_MGT.Cmd2_Untimely_sel”}

q. {“INTERNALPOWER1.Degraded”, “POWERMONITOR1.Incorrect”}

r. {“INTERNALPOWER1.Degraded”, “SELECTION_MGT.Cmd1_Untimely_sel”}

s. {“INTERNALPOWER1.Loss”, “SELECTION_MGT.Cmd1_Untimely_sel”}

t. {“INTERNALPOWER2.Degraded”, “SELECTION_MGT.Cmd2_Untimely_sel”}

u. {“INTERNALPOWER2.Loss”, “SELECTION_MGT.Cmd2_Untimely_sel”}

v. {“PWR1.Degraded”, “POWERMONITOR1.Incorrect”}

w. {“PWR1.Degraded”, “SELECTION_MGT.Cmd1_Untimely_sel”}

x. {“PWR1.Loss”, “SELECTION_MGT.Cmd1_Untimely_sel”}

y. {“PWR2.Degraded”, “SELECTION_MGT.Cmd2_Untimely_sel”}

z. {“PWR2.Loss”, “SELECTION_MGT.Cmd2_Untimely_sel”}

(Editor’s Note: In this example, the notation for the FFS or for the MCS is the following: { “XXXX.yyyy” } represents an FFS or an MCS of Order 1, where XXXX represents a block and where yyyy is one of the failure events of the block (e.g., “COMMAND1.Incorrect_Behavior”); { “XXXX.yyyy”, “AAAA.bbbb” } represents an FFS or a MCS of Order 2 (e.g., “ACCUMULATOR.Failure”, “SELECTORVALVE.Stuck_Middle”).

The computation regarding the loss of braking was done for a whole flight (5 flight hours), with an average risk approach. Table Q.9-8 presents the summary of MCSs, truncated to the Order 3, with the respective probabilities.

Table Q.9-8 - (PSSA - WBS - MBSA)
“Loss of wheel braking” probability computation second iteration

Order of MCS	Number	Probability
Total	**69**	**4.0588E-08**
1	0	0
2	16	4.0584E-08
3	53	3.1833E-12

The MCSs, truncated to the Order 2, were the following:

a. {“ACCUMULATOR.Failure”, “SELECTORVALVE.Stuck_Middle”}

b. {“COMMAND1.Incorrect_Behavior”, “MONITOR1.Incorrect_Behavior”}

c. {“COMMAND1.Incorrect_Behavior”, “SELECTION_MGT.Cmd1_Untimely_sel”}

d. {“COMMAND1.Loss”, “SELECTION_MGT.Cmd1_Untimely_sel”}

e. {“COMMAND2.Incorrect_Behavior”, “SELECTION_MGT.Cmd2_Untimely_sel”}

f. {“COMMAND2.Loss”, “SELECTION_MGT.Cmd2_Untimely_sel”}

SAENORM.COM : Click to view the full PDF of arp4761a

g. {“INTERNALPOWER1.Degraded”, “POWERMONITOR1.Incorrect”}

h. {“INTERNALPOWER1.Degraded”, “SELECTION_MGT.Cmd1_Untimely_sel”}

i. {“INTERNALPOWER1.Loss”, “SELECTION_MGT.Cmd1_Untimely_sel”}

j. {“INTERNALPOWER2.Degraded”, “SELECTION_MGT.Cmd2_Untimely_sel”}

k. {“INTERNALPOWER2.Loss”, “SELECTION_MGT.Cmd2_Untimely_sel”}

l. {“PWR1.Degraded”, “POWERMONITOR1.Incorrect”}

m. {“PWR1.Degraded”, “SELECTION_MGT.Cmd1_Untimely_sel”}

n. {“PWR1.Loss”, “SELECTION_MGT.Cmd1_Untimely_sel”}

o. {“PWR2.Degraded”, “SELECTION_MGT.Cmd2_Untimely_sel”}

p. {“PWR2.Loss”, “SELECTION_MGT.Cmd2_Untimely_sel”}

Q.9.9.3.2 Uncommanded Wheel Braking Failure Condition

Table Q.9-9 presents the quantity of FFSs of the failure condition “Uncommanded wheel braking”, truncated to the Order 3:

Table Q.9-9 - (PSSA - WBS - MBSA)
Quantity of “Uncommanded wheel braking” FFSs second iteration

Order of FFS	Number
Total	**63**
1	1
2	15
3	47

SAENORM.COM : Click to view the full PDF of arp4761a

a. {“CCF_HW_COM_MON_INCORRECT”}

b. {“CCF_SW_COM_INCORRECT”, “CCF_SW_MON_INCORRECT”}

c. {“CCF_SW_COM_INCORRECT”, “MONITOR1.Incorrect_Behavior”}

d. {“CCF_SW_COM_INCORRECT”, “MONITOR2.Incorrect_Behavior”}

e. {“CCF_SW_COM_INCORRECT”, “SELECTION_MGT.Cmd1_Untimely_sel”}

f. {“CCF_SW_COM_INCORRECT”, “SELECTION_MGT.Cmd2_Untimely_sel”}

g. {“CCF_SW_MON_INCORRECT”, “COMMAND1.Incorrect_Behavior”}

h. {“COMMAND1.Incorrect_Behavior”, “MONITOR1.Incorrect_Behavior”}

i. {“COMMAND1.Incorrect_Behavior”, “SELECTION_MGT.Cmd1_Untimely_sel”}

j. {“COMMAND2.Incorrect_Behavior”, “SELECTION_MGT.Cmd2_Untimely_sel”}

k. {“INTERNALPOWER1.Degraded”, “POWERMONITOR1.Incorrect”}

l. {“INTERNALPOWER1.Degraded”, “SELECTION_MGT.Cmd1_Untimely_sel”}

m. {“INTERNALPOWER2.Degraded”, “SELECTION_MGT.Cmd2_Untimely_sel”}

n. {“PWR1.Degraded”, “POWERMONITOR1.Incorrect”}

o. {“PWR1.Degraded”, “SELECTION_MGT.Cmd1_Untimely_sel”}

p. {“PWR2.Degraded”, “SELECTION_MGT.Cmd2_Untimely_sel”}

A review of the FFS list indicates that assumption MBSA-SR-02 is confirmed:

MBSA-SR-02	Independence between the members of each Functional Failure Set shall be verified.

The Minimal Cut Sets, truncated to the Order 2, were the following:

a. {“COMMAND1.Incorrect_Behavior”, “MONITOR1.Incorrect_Behavior”}

b. {“COMMAND1.Incorrect_Behavior”, “SELECTION_MGT.Cmd1_Untimely_sel”}

c. {“COMMAND2.Incorrect_Behavior”, “SELECTION_MGT.Cmd2_Untimely_sel”}

d. {“INTERNALPOWER1.Degraded”, “POWERMONITOR1.Incorrect”}

e. {“INTERNALPOWER1.Degraded”, “SELECTION_MGT.Cmd1_Untimely_sel”}

f. {“INTERNALPOWER2.Degraded”, “SELECTION_MGT.Cmd2_Untimely_sel”}

g. {“PWR1.Degraded”, “POWERMONITOR1.Incorrect”}

h. {“PWR1.Degraded”, “SELECTION_MGT.Cmd1_Untimely_sel”}

i. {“PWR2.Degraded”, “SELECTION_MGT.Cmd2_Untimely_sel”}

Q.9.9.4 PASA and Proposed Safety Requirement Satisfaction

Q.9.9.4.1 PASA-SR-01

The functional decomposition of Decelerate Wheels Function within the model identified two separate sub-functions; a “Control Wheel Braking Function” and an “Actuate Wheel Braking Command Function”. Each are assigned a development assurance of FDAL A in refined requirement MBSA-SR-01.

PASA-SR-01	Decelerate Wheels Function shall be developed FDAL A.
MBSA-SR-01	The Control Wheel Braking function and the Actuate Wheel Braking Command function shall be developed to FDAL A.

SAENORM.COM : Click to view the full PDF of arp4761a

The following items require IDAL assignment for the Control Wheel Braking function of the BSCU:

- Command hardware.
- Command software.
- Monitor hardware.
- Monitor software.
- Selection management.
- Internal Power 1 and 2.
- Power Monitor 1 and 2.

Whereas PWR1 and PWR2 are external to the system, their IDAL assignments may have an impact on BSCU items IDAL assignment. Thus, different possible assignments have been taken into account.

(Editor's Note: The MBSA example used different assumptions than those postulated in the PSSA "IDAL Assignment for Braking System Control Function," Section Q.6.4.3.1.2 which resulted in different MBSA FFS than those captured in PSSA Q.6 Table Q.6-9.)

The BSCU IDAL will now be assigned. The design organization IDAL allocation proposal is:

IDAL(HW_COM_MON) = A

IDAL(SW_COM) = B and IDAL(SW_MON) = B

(Editor's Note: Other choices could have been IDAL(SW_COM) = A and IDAL(SW_MON) = C or IDAL(SW_MON) = C and IDAL(SW_COM) = A).

A review of the model generated FFS is accomplished to substantiate that the proposed IDAL assignments satisfy the safety criteria.

Review of the FFSs for the Uncommanded Wheel Braking failure condition:

IDAL(HW_COM_MON) = A. This assignment is compatible with FFS #01

IDAL(SW_COM) = B and IDAL(SW_MON) = B. This assignment is compatible with FFS #02

FFS #05 and #06 imply an IDAL assignment for Selection_Mgt ≥ B:

MBSA-SR-03	Selection_Mgt IDAL shall be at a minimum of Level B.

SAENORM.COM : Click to view the full PDF of arp4761a

Then, two options are possible for IDAL assignment:

Option1:

If IDAL(Selection_Mgt) = A

FFS #12 and #13 imply IDAL(InternalPoweri) ≥ C

FFS #15 and #16 imply IDAL(PWRi) ≥ C

If IDAL(InternalPoweri) = IDAL(PWRi) = C

FFS #11 and #14 imply IDAL(PowerMonitor1) = A

Option 2:

If IDAL(Selection_Mgt) = B

FFS #12 and #13 imply IDAL(InternalPoweri) ≥ B

FFS #15 and #16 imply IDAL(PWRi) ≥ B

If IDAL(InternalPoweri) = IDAL(PWRi) = B

FFS #11 and #14 imply IDAL(PowerMonitor1) ≥ B

MBSA-SR-04	According to Selection_Mgt IDAL choice, two minimal IDAL allocations shall be considered (Table Q.9-11).

These two minimal IDAL allocations, among various different possible ones, are gathered in Table Q.9-11:

Table Q.9-11 - (PSSA - WBS - MBSA)
Minimal IDAL allocations

Item	Option 1	Option 2
HW COM/MON	A	A
SW COM	B	B
SW MON	B	B
Selection_Mgt	**A**	**B**
PWR1	C	B
PWR2	C	B
InternalPower1	C	B
InternalPower2	C	B
PowerMonitor1	A	B

As per the PSSA Q.6 assignment example:

A single hardware requirement specification is envisaged for BSCU hardware. It gathers the following items:

- COM
- MON
- InternalPower
- PowerMonitor

SAENORM.COM : Click to view the full PDF of arp4761a

Two separate software requirement specifications are envisaged for COM software and MON software. Thus, the COM software includes the Selection_Mgt, whose IDAL becomes B.

As a result, only Option 2 described above satisfies the safety requirements. It implies a new requirement for PWR 1 and 2 assignment (see MBSA-SR-05):

MBSA-SR-05	PWR1 and PWR2 IDAL shall be developed to a minimum of Level B. (To be confirmed at the airplane level.)

The final minimal IDAL allocations are summarized in Table Q.9-12.

Table Q.9-12 - (PSSA - WBS - MBSA)
Final minimal IDAL allocations

Item	Option 2
HW COM/MON	A
SW COM	B
SW MON	B
PWR1	**B**
PWR2	**B**

Q.9.9.4.2 PASA-SR-05

PASA-SR-05	Complete loss of wheel brake shall be less than 1.0E-07 for a landing.

This requirement was fulfilled, as the computed probability of the complete loss was 4.0588E-08 for a landing (see Table Q.9-8).

Q.9.9.4.3 PASA-SR-XX

PASA-SR-XX	No single failure shall result in an uncommanded full symmetric wheel deceleration during a takeoff roll.

This requirement was fulfilled, as there was no minimal cut set of Order 1 for the uncommanded failure condition.

Q.9.9.4.4 PASA-SR-XY

PASA-SR-XY	Uncommanded full symmetric wheel deceleration shall be less than 1.0E-09 for a takeoff.

This requirement was fulfilled, as the computed probability of the uncommanded failure condition was 1.8088E-10 for a takeoff (see Table Q.9-10).

Q.9.9.4.5 PASA-SR-12

PASA-SR-12	Loss of power from both hydraulic subsystems powered by the engines shall not lead to complete loss of wheel braking.

This requirement was fulfilled due to the emergency accumulator integration.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.9.9.4.6 PASA-SR-14

PASA-SR-14	Two redundant control lanes shall be provided between the Electric Brake Unit (EBU) and each of the two Alternate/Emergency Meter Valves.

This requirement was fulfilled by design.

Q.9.9.5 Second Iteration MBSA Outputs

The second iteration design satisfies the quantitative and the qualitative safety objectives regarding the two failures conditions.

Building the second iteration MBSA Model led the safety team to raise several questions (a non-exhaustive list):

- How does the BSCU know HYD1 status or the SelectorValve position? Adding a sensor on the SelectorValve would allow the BSCU to quickly detect the presence of the HYD1 and the position of the Selector Valve.
- What is the consequence of one (or several) untimely wheel braking (Tire burst, impact on the nearby tire)?
- When addressing the common causes, is there a need for two different types of speed sensor?
- Are there enough pedal sensors to satisfy the safety objectives?
- What is the internal architecture of the Electric Brake Unit?
- How are the pedal sensors electrically powered?

Reminder: Some assumptions were made and are presented to the design organization for confirmation. These assumptions are captured in Table Q.9-13.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.9-13 - (PSSA - WBS - MBSA)
Safety assumptions for confirmation

Assumption ID	Assumption
MBSA-BSCU-R-01	If Braking is commanded, the loss of braking on at least three wheels triggers the switch from NORMAL Mode to ALTERNATE Mode and a switch from the HYD 1 path to HYD 2 path.
MBSA-BSCU-R-02	The Shutoff Valve is used to control the Selector Valve in order to: - Fill the emergency accumulator in flight (main landing gears retracted) - Avoid unstable commutations between HYD 1/HYD 2 - Provide a mitigation means for a Normal Meter Valve failure which leads to an uncommanded braking of one wheel (risk of tire burst).* *Not in the frame of the study.
MBSA-BSCU-R-03	Electric Brake Unit (EBU) As the internal architecture of the EBU (e.g., number of sensors, number of pedals, electrical power supply) was unknown, the EBU was considered a monolithic block which provides the three position data. As a consequence, only two failure modes were retained, one leading to a Not_Braking state, the other one leading to an Untimely_Braking state.
MBSA-BSCU-R-04	BSCU/EBU interface The two signals coming from the EBU were used inside the BSCU with the following logic: both signals shall be consistent to execute the braking command.
MBSA-BSCU-R-05	BSCU Command In case of degraded power, the worst-case was considered: the Internal Validity is still true and the output command is the opposite of the input command request.
MBSA-BSCU-R-06	Power Monitor If Power Monitor is lost, the output validity is false. This initiates a switch to the other channel. If Power Monitor is incorrect, the output validity is contrary to the real one.
MBSA-BSCU-R-07	Monitor If Monitor is lost or not powered, the output validity is false. This initiates a switch to the other channel. If Monitor is incorrect and powered, validity is always true (no detection).

The different iterations raised some refined requirements. The refined proposed safety requirements are presented in Table Q.9-14.

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.9-14 - (PSSA - WBS - MBSA)
Proposed MBSA Safety Requirements

MBSA-SR-01	The Control Wheel Braking function and the Actuate Wheel Braking Command function shall be developed to FDAL A.
MBSA-SR-02	Independence between the members of each Functional Failure Set shall be verified.
MBSA-SR-03	Selection_Mgt IDAL shall be at a minimum of Level B
MBSA-SR-04	According to Selection_Mgt IDAL choice, two minimal IDAL allocations shall be considered (Table Q.9-11).
MBSA-SR-05	PWR1 and PWR2 IDAL shall be developed to a minimum of Level B. To be confirmed at the airplane level.

Q.9.10 Conclusion

Performing a model based analysis identifies the necessity to formalize the functional and the dysfunctional system behaviors. In accomplishing these activities, a clear identification and capturing hypotheses which have been made is also essential. All hypotheses are be validated by the design organization.

This example shows that:

- A model based analysis can handle multi-physics system (Hydraulic, electrical, mechanical, and electronic hardware/software).
- An MBSA model can be used at different stages of the development process.
- Several failure conditions can be studied using the same model.
- Several types of analyses can be done using the same model using post-treatment (e.g., FFS, MCS).
- Using a single model can insure consistency between several failure conditions (in the framework of an update of a system. This feature reduces considerably the necessary time to update one system safety analysis).
- A MBSA model makes it possible to verify top-level safety requirements at each iteration.
- A MBSA model raises a lot of questions about system behavior, enables all stakeholders (e.g., design and safety teams) to share common understanding of the system and helps to formalize hypotheses made.
- Finally, a MBSA model highly facilitates the communication between development and safety teams.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.10 S18 AIRPLANE - BSCU FAILURE MODES AND EFFECTS ANALYSIS AND SUMMARY (FMEA/FMES) EXAMPLE

FMEA/FMES Example

Q.10.1 BSCU Power Supply FMEA Introduction

(Editor's Note: This Failure Modes and Effects Analysis (FMEA) example is simplified by limiting the FMEA to the BSCU power supply. On any specific project, an FMEA may be requested at any level from an entire system to a small portion of circuitry performing one function inside an LRU.)

(Editor's Note: For the purpose of this example, it is assumed that the FMEA was chosen to support an SSA FTA. The process and format of the FMEA may require minor alterations to support DD or MA methodologies; however, the basic steps and principles carry forward. The FMEA/FMES checklist defined in J.4.3. was used to ensure that the correct steps were accomplished throughout the FMEA and FMES development. In each step of this section, the applicable checklist element was observed. The first step was to obtain a definition of FMEA goals and expectations, including the expected final report format.)

This FMEA addresses the BSCU power supply in support of the basic events and safety objectives identified in the following fault tree analyses as requested:

- "1.1.MF1 - Uncommanded Full Symmetrical Wheel Deceleration at Takeoff" (FTA not developed in the example).
- FTA branch "3_BSCU-NMV-ERR BSCU provides unannunciated erroneous output to NMV- inadvertent" preliminary FTA.

This FMEA report provides support of the final FTA by providing updated failure rates for the basic events. The FTA basic events supported by this FMEA are:

- "BSCU-CH1-PS-ERR BSCU Channel #1 Power Supply Fails outside voltage limits"
- "BSCU-CH1-PSM-LOSS-PUP BSCU Ch#1 PS Monitor fails to mitigate erroneous PS operation- LATENT"
- The power supply contribution to "Undetected BSCU Failure Causes Inadvertent Braking"

This analysis was performed against released and final documentation of the BSCU design and production drawings. This FMEA is part of the supporting documentation for both the BSCU and WBS SSAs.

The requested FMEA was performed in two parts. A functional FMEA was performed on the power supply and a Piece-Part FMEA was performed on the power supply monitor portion of the power supply. The Piece-Part FMEA was performed after the conservative results of the functional FMEA did not meet the needs of the FTA to support the safety objectives.

(Editor's Note: Table Q.10-1 provides a cross reference linkage from the example sections herein to the applicable FMEA appendix section.)

Table Q.10-1 - (SSA - BSCU - FMEA)
Cross reference to FMEA process appendix

Example FMEA Section No.	*Appendix J Section No.*
Q.10.2 & Q.10.3	*J.3.1*
Q.10.3.1	*J.3.2.1*
Q.10.3.2	*J.3.2.2*

(Editor's Note: The information contained in these references provides a substantial portion of the documentation required before beginning an FMEA. See J.3.1.)

SAENORM.COM : Click to view the full PDF of arp4761a

1. ARP4761A/ED-135 “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment”.

2. Internal memo requesting FMEA support for “1.1.MF1 - Uncommanded Full Symmetrical Wheel Deceleration at Takeoff” fault tree for the S18 airplane incorporating the BSCU system.

   (Editor’s Note: FTA not developed in the example.)

3. BSCU released design and production documentation

4. MIL-HDBK-217F “Reliability Prediction of Electronic Equipment”.

5. Internal memo stating component failure modes to be used for BSCU FMEA.

6. Results of lab analysis of “Loss of or Reduced Filtering.”

7. BSCU Power Supply Reliability Prediction.

Q.10.2 Power Supply Description

(Editor’s Note: Part of the preparation for an FMEA includes understanding the operation of the function. A brief overview of the operation should be included in the report as outlined in J.3.1)

The implementation of the BSCU power supply, as documented in design documentation (Reference 3) was reviewed. The design and implementation of the BSCU 1 and 2 power supplies were found to be identical. Implementation is through identical power supply designs, located on physically separated areas of the BSCU circuit card assembly as depicted in architectural diagram of the BSCU in Figure Q.10-1. Within each BSCU Channel, the power supply and power supply monitor functions are physically independently located.

The power supply design is depicted in the block diagram provided in Figure Q.10-2. A detailed schematic of the +5V monitor design is provided in Figure Q.10-3.

The BSCU power supply is of standard design and is described in the BSCU Hardware Description document.

The power supply monitors are window comparators. Both +5V and ±15V are monitored for over and under voltage conditions. The outputs are ANDed together so that if any voltage exceeds the trip point, high or low, the monitor output is pulled low.

SAENORM.COM : Click to view the full PDF of arp4761a

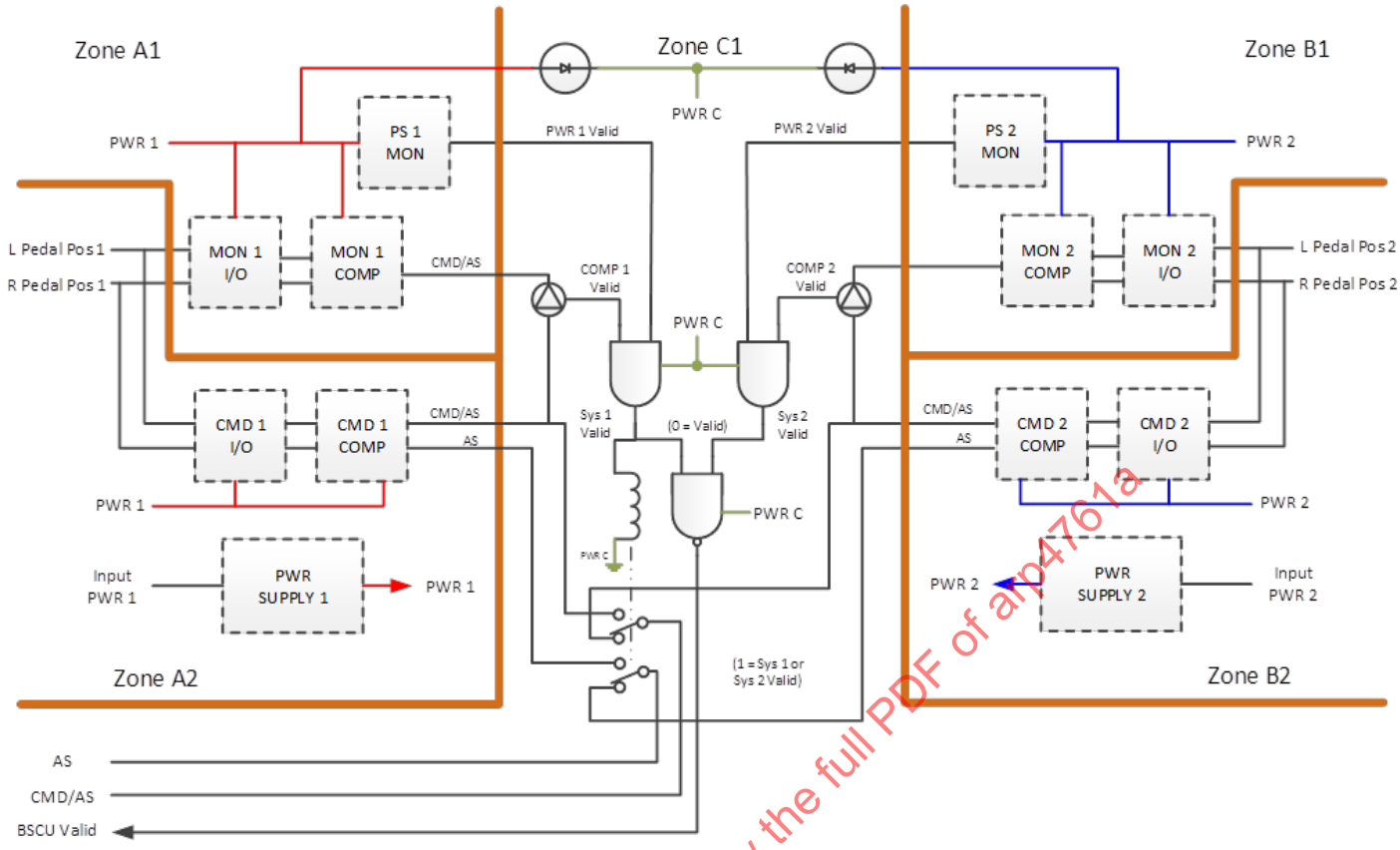


Figure Q.10-1 - (SSA - BSCU - FMEA)
BSCU physical implementation

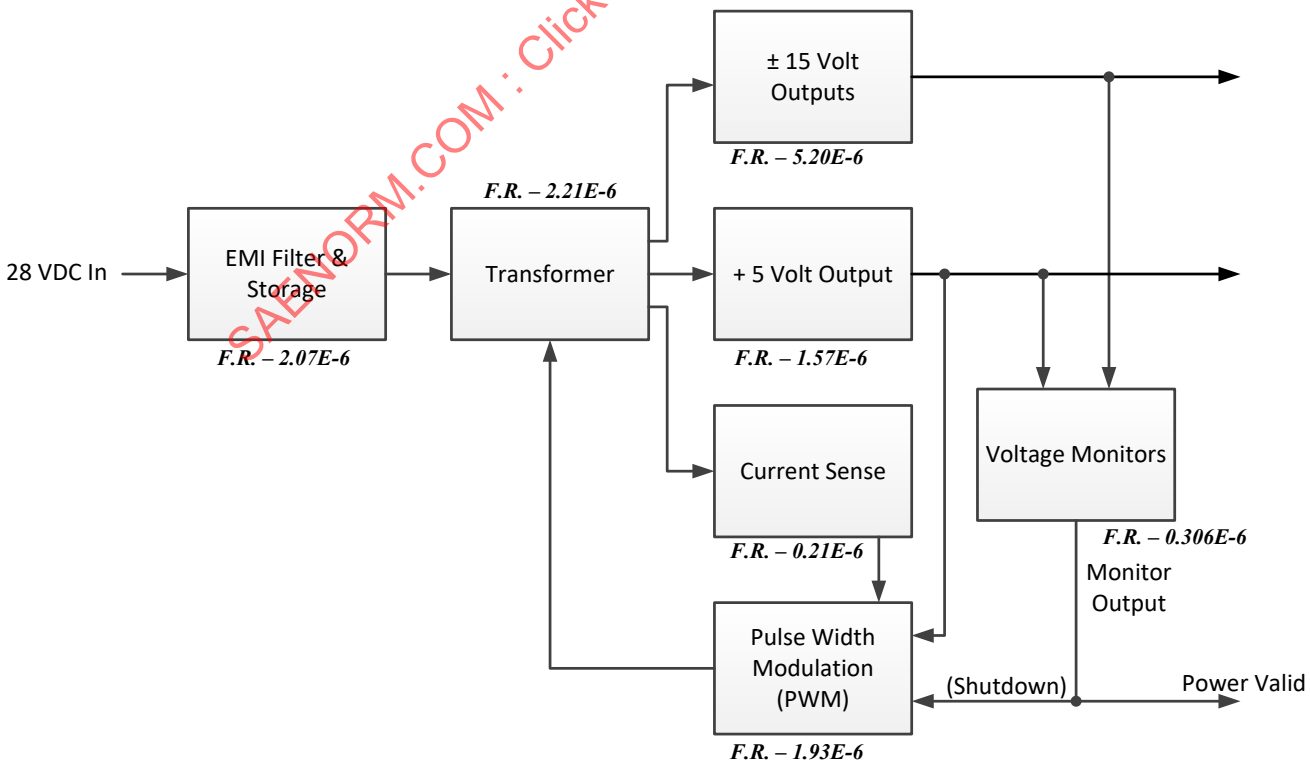


Figure Q.10-2 - (SSA - BSCU - FMEA)
Power supply block diagram

SAENORM.COM : Click to view the full PDF of arp4761a

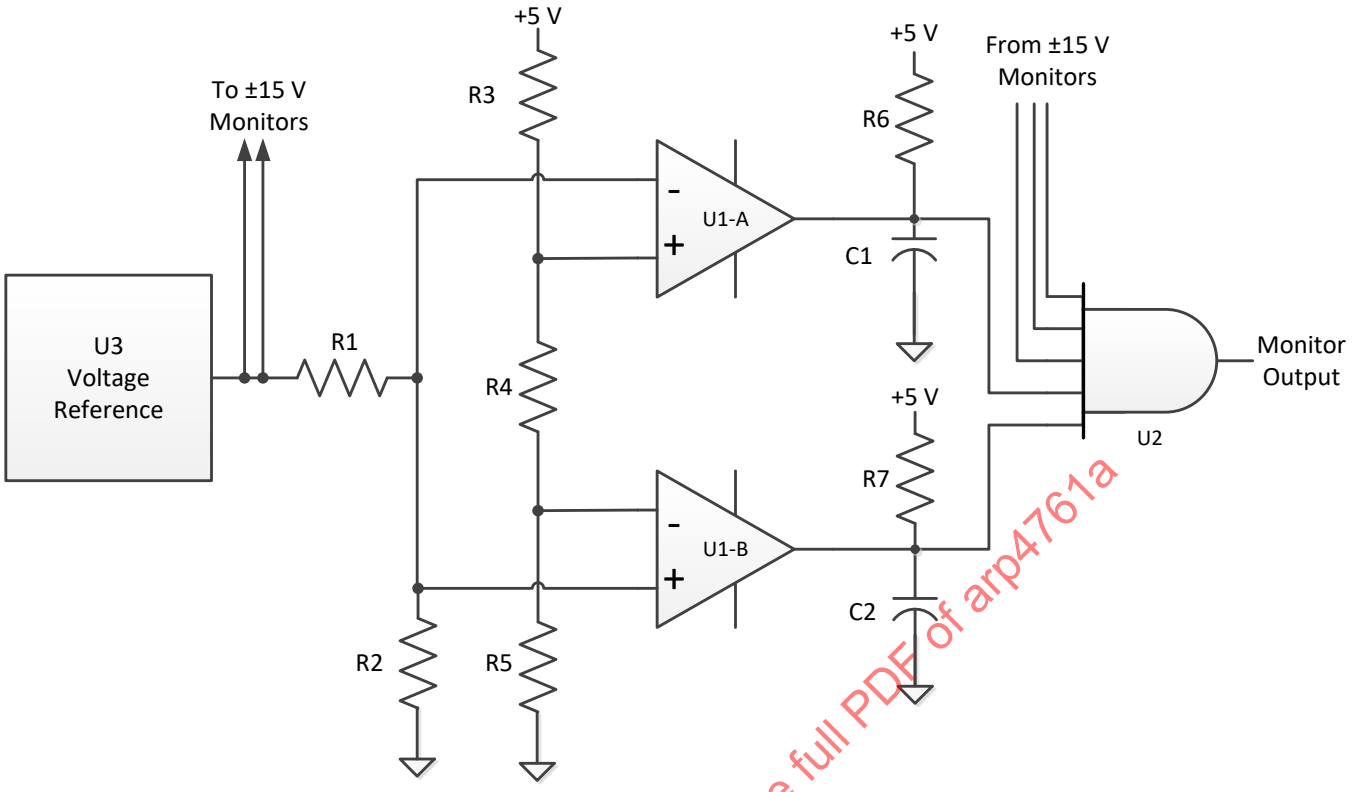


Figure Q.10-3 - (SSA - BSCU - FMEA)
Schematic of power supply monitor

It should be noted that the ±15V monitor uses same reference voltage source and comparator monitoring scheme.

Q.10.3 Power Supply Detailed Analysis and Results

This FMEA contains two sections. Q.10.3.1 is the functional FMEA performed on the entire power supply. The functional FMEA on the power supply monitor has been deleted from the functional FMEA section since it is superseded by the Piece-Part FMEA found in Q.10.3.2.

Q.10.3.1 Power Supply Functional FMEA

Initial analysis of the power supply was conducted by computing the total power supply failure rate based on parts counts and failure rates. Conservative analysis did not meet the budget for “Undetectable power supply failure causes inadvertent braking.” Therefore, a functional FMEA was performed to provide better resolution into the failure rates of the various failure modes. The only failure that may cause bad data and may not be detected by a properly functioning power supply monitor is “Loss of/reduced filtering.” This failure mode may cause increased ripple on the output voltages that may be at such a level and frequency that it is not detected by the monitor. Table Q.10-2 captures the Functional FMEA results.

(Editor’s Note: Only the analysis of the “+5V output” functional block is shown in detail. The results of an FMEA on the remainder of the power supply are included in the summary. This is done to remove pages of tables unnecessary to give a representative example of a functional FMEA.)

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.10-2 - (SSA - BSCU - FMEA)
Functional FMEA for BSCU power supply

Function Name	Failure Mode	Failure Rate (E-06)	Failure Effect	Detection Method	Comments
+5 Volt	+5V out of spec.	0.2143	Possible P/S shutdown	Power Supply Monitor trips, shuts down supply and passes “invalid power supply (P/S)” to other BSCU channel	BSCU channel fails
	+5V short to ground	0.2857	P/S shutdown	Power supply monitor passes invalid P/S to other BSCU channel	BSCU channel fails
	Loss of/reduced filtering	0.3571	Increase Ripple	May pass out of spec voltage to rest of BSCU if ripple is such that it is not detected by the P/S monitor	May cause spurious P/S monitor trip
	+5V open	0.5714	P/S shutdown	Power supply monitor passes invalid P/S to other BSCU channel	BSCU channel fails
	No Effect	0.1429	No effect.	None / No Effect	No Effects
Total Failure Rate of +5V Supply		1.5713			

Q.10.3.2 Power Supply Monitor Piece-Part FMEA

Initial analysis of the power supply monitor was conducted by computing the total power supply monitor failure rate based on parts counts and failure rates. It was found that the total failure rate of the power supply monitor was 3.06E-07 failures per hour thus not complying with the budgeted failure rate of 2.0E-07 for monitor fails valid. A detailed Piece-Part FMEA was conducted to provide better resolution into the probability of a “Monitor Fails Valid” condition. Table Q.10-4 documents this Piece-Part FMEA. Five general failure code categories were included to enhance summary failure classification. These Failure Effect Codes are defined in Table Q.10-3.

Table Q.10-3 - (SSA - BSCU - FMEA)
Failure effect categories

Failure Effect Code	Failure Effect Category
1.	Monitor Stuck Valid
2.	Nuisance Monitor Trip
3.	Monitor Stuck Tripped/Supply Shutdown
4.	Monitor Sensitivity Shifts
5.	No Effect

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.10-4 - (SSA - BSCU - FMEA)
Piece-Part FMEA for BSCU power supply monitor

Component Identifier	Component Type	Failure Mode	Failure Mode Rate (E-06)	Failure Effect Code	Failure Effect	Detection Method
C1	Ceramic Capacitor	short	0.0073	3	Under voltage monitor stuck tripped	P/S shut down by monitor
		open	0.0013	2	Loss of delay, spurious monitor trips	P/S shutdown
		low cap.	0.0019	2	Decrease delay to trip	
C2	Ceramic Capacitor	short	0.0073	3	Over voltage monitor stuck tripped	P/S shut down by monitor
		open	0.0013	2	Loss of delay, spurious monitor trips	P/S shutdown
		low cap	0.0019	2	Decrease delay to trip	
U1A	Comparator IC	output open	0.0124	1	Under voltage monitor stuck valid	Bench test
		output grounded	0.0056	3	Under voltage monitor trips	P/S shutdown
		high offset voltage	0.0062	4	Loss of monitor sensitivity	Bench test
U1B	Comparator IC	output open	0.0124	1	Over voltage monitor stuck valid	Bench test
		output grounded	0.0056	3	Over voltage monitor trips	P/S shutdown
		high offset voltage	0.0062	4	Loss of monitor sensitivity	Bench test
R1	Film Resistor	open	0.0009	3	Over voltage monitor trips	P/S shutdown
		increase resistance	0.0005	4	Trip window shifts down	
		decrease resistance	0.0004	4	Trip window shifts up	
R2	Film Resistor	open	0.0009	3	Under voltage monitor trips	P/S shutdown
		increase resistance	0.0005	4	Trip window shifts up	
		decrease resistance	0.0004	4	Trip window shifts down	
R3	Film Resistor	open	0.0009	3	Under voltage monitor trips	P/S shutdown
		increase resistance	0.0005	4	Trip window shifts up	
		decrease resistance	0.0004	4	Trip window shifts down	
R4	Film Resistor	open	0.0009	1	Monitor stuck valid	Bench test
		increase resistance	0.0005	2	Trip window tightens	Bench test
		decrease resistance	0.0004	1	Trip window widens, may cause monitor stuck valid	Bench test
R5	Film Resistor	open	0.0009	3	Over voltage monitor trips	P/S shutdown
		increase resistance	0.0005	4	Trip window shifts down	
		decrease resistance	0.0004	4	Trip window shifts up	
R6	Film Resistor	open	0.0009	3	Under voltage monitor stuck tripped	P/S shutdown
		increase resistance	0.0005	5	No effect	
		decrease resistance	0.0004	5	No effect	
R7	Film Resistor	open	0.0009	3	Over voltage monitor stuck tripped	P/S shutdown
		increase resistance	0.0005	5	No effect	
		decrease resistance	0.0004	5	No effect	
U2	AND gate	stuck high	0.0108	1	Monitor stuck valid	Bench test
		stuck Low	0.0054	3	Monitor stuck tripped	P/S shutdown
U3	Voltage Reference	inop	0.0110	3	Over voltage monitor trip	P/S shutdown
		out of spec	0.0058	4	Window shift	
		short	0.0026	3	Monitor trip	P/S shutdown
		open	0.0245	3	Over voltage monitor trip	P/S shutdown
…						

It should be noted that failures in failure effect category 4 may cause monitor effectiveness to be reduced

(Editor's Note: For the purposes of this example, failure modes and failure rates for the ±15V monitors are assumed to be identical to the +5V monitor. In an actual FMEA, the same detailed analysis would be completed on the ±15V monitors to determine the actual failure modes and rates.)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.10.3.3 FMEA Summary

The BSCU level effect of “Loss of/reduced filtering” was unknown and might have contributed to “Undetectable BSCU failure causes inadvertent braking.” It is extremely conservative to assume that all failures in this category will be undetectable and capable of causing “Undetectable BSCU failure causes inadvertent braking.” Therefore, a separate laboratory analysis of the effect on the system was performed. This analysis (reference 6) shows that none of the failures in the “Loss of/reduced filtering” effect category can cause inadvertent braking.

(Editor’s Note: Laboratory analysis may be required in some instances to determine the actual effect of a failure mode. See J.3.2.3)

All other failure effect categories except “No effect” may contribute to “BSCU power supply failure causes bad data.” These failures will be detected by a properly functioning power supply monitor. Table Q.10-5 summarizes the results of the power supply and power supply monitor FMEAs.

Table Q.10-5 - (SSA - BSCU - FMEA)
BSCU power supply and power supply monitor FMEA summary

Failure Modes	Failure Rate (E-06)	BSCU Effect	Potential Failure Cause	Detection Method	Comments
Power Supply (P/S) Shutdown	8.21	BSCU channel fails	+5V out of spec +5V short to ground +5V open +15V out of spec ...	“Power valid” to other BSCU set invalid	BSCU Channel 2 provides braking command
Increased Ripple from P/S	1.86	Unknown	Loss/reduced filtering: +5V +15V -15V ...	Possibly undetected	Laboratory analysis was performed that indicates this mode does not cause inadvertent braking.
Properly Operating P/S Monitor cannot shut down P/S	0.57	P/S does not shut down following P/S failure	PWM input from voltage monitor stuck valid	Card level test only	Power valid signal shuts down BSCU CH 1 outputs. No obvious BSCU effect.
P/S Monitor Fails Valid	0.1429	Possible erroneous operation following P/S failure	U1A open U1B open R4 Open R4 decreased Res U2 high ...	Bench test	Latent failure
P/S Monitor Tripped	0.1578	BSCU channel fails	C1 short C1 open C2 short C2 open ...	“Power valid” to other BSCU set invalid	
No Effect (NE)	2.5554	None	+5V output NE R6 increase Res R6 decrease Res ...	None	None

SAENORM.COM : Click to view the full PDF of arp4761a

Q.10.4 FMES for the BSCU Introduction

This FMES provides a summary of the results of all BSCU FMEAs.

(Editor’s Note: Results of other FMEAs that may have been performed are also included to provide a more extensive list of failure effects.)

(Editor’s Note: For details on FMES process, see J.4.2.)

Q.10.5 References

The following references were utilized in performing this analysis.

1. ARP4761A/ED-135 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

2. Internal memo documenting FMEAs results relative to the BSCU system.

3. BSCU released design and production documentation.

Q.10.6 BSCU Description

(Editor's Note: Normally a system description would be included here. However, since it's included elsewhere in Appendix Q, it is not repeated here for brevity.)

Q.10.7 FMES Data

The failure effects from the FMEAs from Reference 2 were examined and summarized as shown in Table Q.10-6.

Table Q.10-6 - (SSA - BSCU - FMEA)
Failure effects summary

Failure Mode	Failure Rate	Potential Failure Cause (Source of Failure)	Detectability	Comments
Loss of braking command from channel 1	3.10E-05	- Channel 1 P/S shutdown - Channel 1 P/S monitor trips - Channel 1 command failed	- Signal to crew alerting system	Channel 2 provides braking command
Loss of braking command from channel 2	3.10E-05	- Channel 2 P/S shutdown - Channel 2 P/S monitor trips - Channel 2 command failed	- Signal to crew alerting system	Channel 1 provides braking command
Loss of Braking command from both channel 1 and 2	1.60E-09	- BSCU validity monitor stuck invalid - BSCU switch failed in intermediate position	- Indication on system display "Loss of normal braking"	Discrete provided
Inadvertent brake command from channel 1 or 2	0.85E-09	- Failures 3, 5, 9 of CMD1 I/O, CMD2 I/O (FMEA BSCU)	Obvious by effect	
Asymmetrical brake command from channel 1 or 2	1.60E-08	- Failures 6, 11, 12 of CMD1COMP,CMD2COMP (FMEA BSCU)	Obvious by effect	

(Editor's Note: Not all failures mentioned in the "Potential Failure Cause" column can be found in the FMEA in this example appendix, but it shows the principle of the FMES to summarize all failures with the same effect to get one failure mode for the next higher level of analysis.)

(Editor's Note: The Failure Mode has been used as the FMEA reference designation in this example.)

SAENORM.COM : Click to view the full PDF of arp4761a

Q.11 S18 AIRPLANE - BSCU COMMON MODE ANALYSIS (CMA) FOR THE BSCU EXAMPLE

CMA Example

Q.11.1 CMA Example Introduction

This section provides an example of a CMA as part of a system safety assessment (SSA). In this case, the CMA example is supporting a Brake System Control Unit (BSCU) SSA (not included in Appendix Q). This example illustrates the processes and methods described in Appendix M to develop an CMA. The reporting format of the analysis is left to the analyst; however, the specific content should reflect the expected content as described in Appendix M and this example. This example depicts one format of a completed CMA. This example may be incorporated into the BSCU SSA or managed as an independent artifact.

This analysis provides an evaluation of the Independence Principles for the BSCU. This CMA evaluates the areas where the safety assessment has identified a need for independence, describes any identified co-dependence characteristics and elaborates on mitigations for the co-dependencies. The BSCU provides dual redundant high integrity braking and anti-skid control for the S18 airplane.

(Editor's Note: Table Q.11-1 provides linkage from each example paragraph to the applicable CMA appendix paragraph.)

Table Q.11-1 - (SSA - CMA - BSCU)
Example to Appendix M cross reference

Example CMA Section No.	Appendix M Section No.
Q.11.3.2	M.3.3.2.1
Q.11.3.1	M.3.3.2.2
Q.11.3.3	M.3.3.2.3
Q.11.3.4	M.3.3.2.4

Q.11.1.1 References

The following references were utilized in performing this analysis:

Ref No.	Document Number	Document Title
1	ARP4761A/ED-135	Guidelines and Methods for Conducting the Safety Assessment Process for Civil Airborne Systems and Equipment
2	BSCU SSA Appendix A	FTA Analysis for the S18 Airplane Incorporating the BSCU System - Loss of All Wheel Braking
3	BSCU SSA Appendix A	FTA Analysis for the S18 Airplane Incorporating the BSCU System - Inadvertent Wheel Braking
4	S18 SFHA	System Functional Hazard Assessment (SFHA) for the S18 Wheel Braking System
5	BSCU PSSA	Preliminary System Safety Assessment (PSSA) for the S18 Airplane WBS BSCU
6		BSCU design and production documentation
7		Safety Segregation Design Guidelines for LRUs in Safety Critical Systems
8	BSCU V&V Report	Validation and Verification Summary (containing BSCU validation and verification evidence references)
9	BSCU HAS	BSCU Hardware Accomplishment Summary
10	BSCU SAS	BSCU Software Accomplishment Summary
11	BSCU Test Report	BSCU Environmental Test Report Summary
12		BSCU Manufacturing Quality Plan
13		BSCU Return to Service Test
14		BSCU Installation and Service Manual

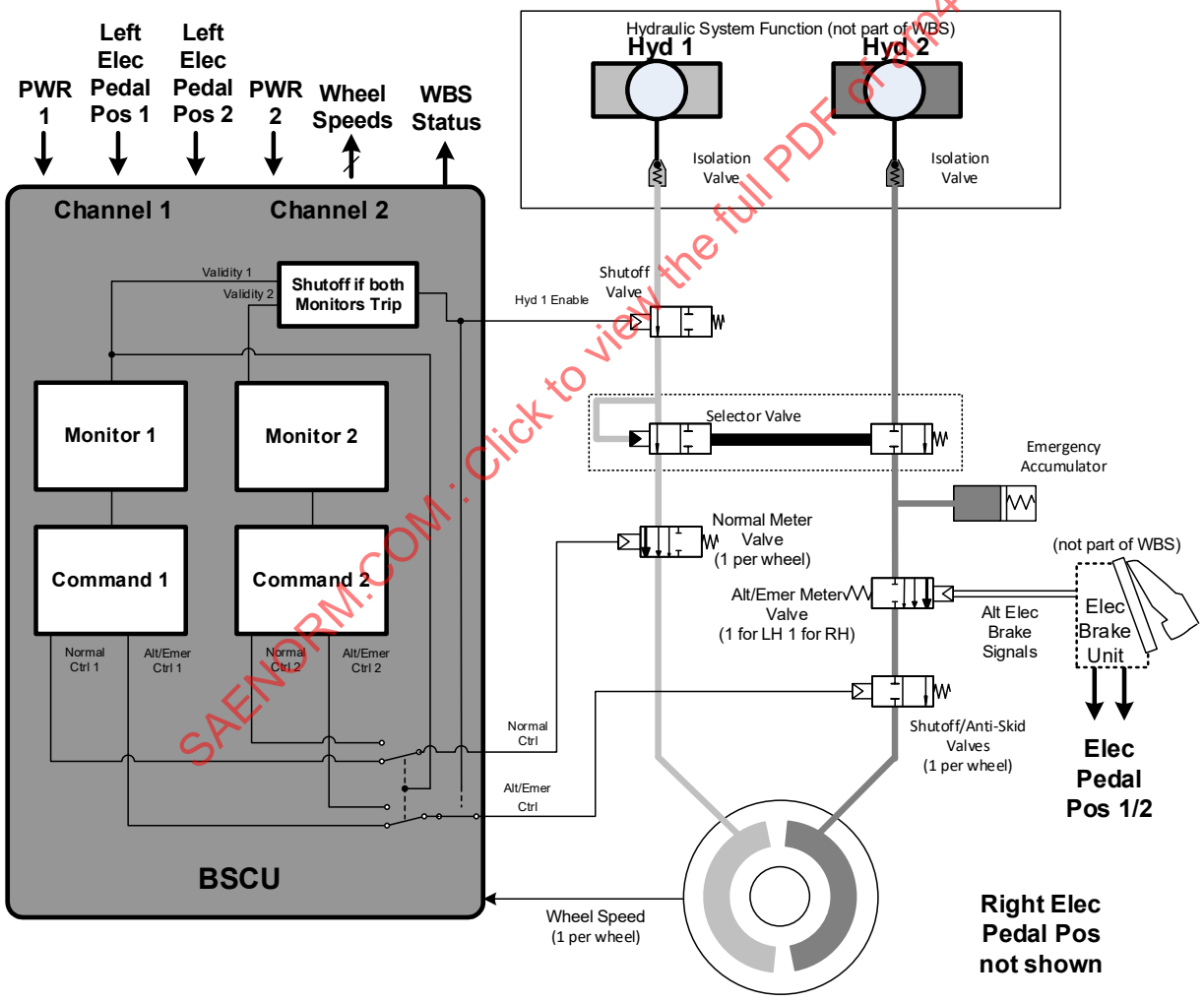
SAENORM.COM : Click to view the full PDF of arp4761a

Q.11.2 Function/System Description

The BSCU LRU provides the normal brake system commands and the anti-skid commands as part of the NORMAL Mode and ALTERNATE Mode brake capabilities of the S18 airplane Wheel Brake System (WBS). Braking on the ground is commanded manually, via brake pedals, or automatically (autobrake) without the need for pedal application. The Autobrake function allows the pilot to pre-arm the deceleration rate prior to takeoff or landing. Autobrake is only available with the NORMAL Mode.

The architecture for the BSCU is a Dual-Dual configuration consisting of two independent channels (Channel 1 and 2), each having two independent computation channels (command and monitor) as shown in Figure Q.11-1. Each channel interfaces through dedicated LRU connectors (P1 or P2). The BSCU operates as an active/standby device where Channel 1 is normally active and Channel 2 is a standby system which is automatically switched on-line upon Channel 1 failures detected by the System 1 in-line monitoring. In-line monitoring of both Channel 1 and Channel 2 combine to provide a NORMAL Mode shutdown and automatic reversion to ALTERNATE Mode when both BSCU systems are inoperative.

The BSCU provides Normal brake commands activating the wheel mounted hydraulic powered brakes. The BSCU Anti-Skid commands remove the Normal brake commands under sensed environmental conditions.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.11-1 - (SSA - BSCU - CMA)
BSCU architecture diagram

Q.11.3 BSCU CMA Detail

The following CMA activities are captured in this analysis:

- Identify CMA checklist elements.
- Identify independence requirements needing evaluation.
- Evaluate each independence requirement against the checklist.
- Summarize results of independence requirement evaluations.

Q.11.3.1 CMA Checklist

(Editor's Note: Appendix M, M.3.1 provides guidelines for establishing the CMA checklist types, sources, and failures/errors)

The CMA questionnaire used in the BSCU PSSA was extracted for review and transitioned to a checklist as part of the SSA CMA activities.

The design implementation was reviewed against the independence requirements to ensure that the independence requirements that were identified during the PSSA process were satisfied. The implementation was also reviewed to ensure that design updates, that may have occurred during development, did not result in any new independence concerns.

(Editor's Note: In a case of finding a lack of independence, the finding(s) would be captured and addressed by the SSA and/or perhaps the ASA.)

In addition to the development error sources captured during the BSCU PSSA CMA development, the following error/failure sources are identified as relevant concerns for the BSCU SSA CMA:

a. Design considerations:
    1. Common external sources to redundant functions.
    2. Common electrical interfaces (connectors) within the redundant systems.
    3. Common failures effecting computation and monitoring functions.
b. Manufacturing considerations:
    1. Inappropriate electronic component substitution.
    2. Improper assembly.
    3. Common manufacturer of electronic components.
    4. Installation considerations.
    5. Incomplete installation (connectors not mated).
    6. Incorrect installation (connectors interchanged).
c. Environmental considerations:
    1. Mechanical/thermal conditions.
    2. Electromagnetic environment/high intensity radiated field conditions.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.11.3.2 Independence Requirement Inputs to CMA

The independence requirements developed in the BSCU PSSA were extracted for review and update as part of the SSA CMA activities. The BSCU SSA Independence Principles were reviewed and no design updates, that may have occurred during development, resulted in new independence requirement concerns.

The following BSCU independence requirements were established for the BSCU by the system development process:

a. BSCU-001: Channel #1 shall have physical independence from Channel #2. (BSCU Channel 1 is independent of BSCU Channel 2 (Loss of Wheel Braking FTA))

b. BSCU-002: Within each channel, the command function shall have physical independence from the monitor function; i.e., BSCU Channel 1 command lane is independent of BSCU Channel 1 monitor lane (Inadvertent wheel braking FTA).

(Editor's Note: There are more independence requirements associated with the S18 BSCU when all airplane wheel brake failure conditions are considered. This example highlights just the evaluation of the sample requirements above.)

Q.11.3.3 Common Mode Analysis

The revised CMA checklist was captured in tabular fashion using the typical format provided in ARP4761A/ED-135, Appendix M. Each of the independence requirements identified in Q.11.3.2 were evaluated against the CMA checklist. This evaluation was performed by adding a narrative discussion of the concern, potential effects, and the mitigation to the tables for each independence requirement.

Tables Q.11-2 through Q.11-4 present the results of each independence requirement evaluation.

(Editor's Note: The independence evaluation tables reference documentation which would normally have unique project configuration control identification characteristics which has been removed in this example for brevity.)

SAENORM.COM : Click to view the full PDF of arp4761a

Table Q.11-2 - (SSA - CMA - BSCU)
Channels 1 and 2 independence evaluation

1 BSCU Channel 1 is physically independent of BSCU Channel 2)		
Common Failure or Error Source Concern	**Description of Effect on Principle**	**Description of Mitigating Factors or Lack of Independence**
BSCU Channel 1 and 2 have common specification? BSCU Channel 1 and Channel 2 common specification contains requirement error(s)?	- Erroneous BSCU specification due to human error, omission or commission causes operational effect - Erroneous BSCU specification interpretation causes operational effect	The BSCU specification is common to both Channel 1 and Channel 2. The BSCU was successfully developed per ARP4754B/ED-79B to FDAL A objectives as evidenced by the BSCU Validation and Verification Summary mitigating common source concern.
BSCU Channel 1 and 2 common hardware specification, common hardware error, or hardware tool error?	- Erroneous hardware specification due to human error, omission or commission causes operational effect - Erroneous electronic component usage in circuit design causes operational effect - Erroneous hardware function (e.g., control equations) causes operational effect - Error in Very High-Speed Integration Circuit Hardware Description Language coder or layout tool causes operational effect	The BSCU command and monitor lane hardware configuration Items are common to both BSCU Channel 1 and Channel 2. The BSCU Command Lane and Monitor Lane hardware requirements were established as implementing identical designs with identical requirements. Each lane has been developed and rigorously verified to Item Development Assurance Level A using RTCA DO-254/ED-80 process objectives, thus mitigating the common source concern. [see BSCU Hardware Accomplishment Summary]
BSCU Channel 1 and 2 common software specification, common software error or error in common software function?	- Erroneous software specification due to human error, omission or commission causes operational effect - Software error due to implementation tools (e.g., compilers, linker, relocate, loader, etc.) causes operational effect - Errors in common software library function causes operational effect - Errors in software function (e.g., control equations) causes operational effect	The BSCU command and monitor lane software configuration Items are common to both BSCU Channel 1 and Channel 2. The BSCU Command Lane and Monitor Lane software requirements were established as implementing different designs with different requirements. Each lane has been developed and rigorously verified to software level B (IDAL B) using RTCA DO-178C/ED-12C process objectives, thus mitigating the common source concern. [see BSCU Software Accomplishment Summary]

SAENORM.COM : Click to view the full PDF of arp4761a

1 BSCU Channel 1 is physically independent of BSCU Channel 2)		
Common Failure or Error Source Concern	**Description of Effect on Principle**	**Description of Mitigating Factors or Lack of Independence**
BSCU Channel 1 and Channel 2 have common electrical and mechanical components, hardware implementation errors or erroneous component applications?	- Erroneous application of new or sensitive technology causes operational effect - Electronic components used outside of data sheet operating ranges causes operational effect	BSCU implemented using common and simple industry electronic components with wide application and usage. All BSCU electronic components used per company derating guidelines [See BSCU Hardware Accomplishment Summary].
	- Failure due to common electrical or mechanical component operation causes operational effect	BSCU Channel 1 and Channel 2 are housed in common enclosure. Channel 1 and Channel 2 are physically separated and electrically isolated to prevent failure propagation. Channel interfaces are isolated between Channel 1 and Channel 2 through separate connectors and wiring. See detailed separation analysis provided in CMA Q.11.3.3.1. Channel 1 and Channel 2 are sufficiently isolated mitigating the common source concern.
	- Failure due to common implementation features (e.g., power supply voltages, ground paths, isolation mechanisms, Incorrect analog-to-digital (A/D) or digital-to-analog (D/A) conversion) causes operational effect	BSCU design uses proven circuit implementations from previous company electronics applications. BSCU implementation verified against system, hardware and software requirements. Based on the extensive industry experience with these designs, no adverse failure modes are anticipated.
BSCU Channel 1 and Channel 2 have common manufacturer? - Use the same manufacturing procedure? - Use the same manufacturing process? - Use the same manufacturing tools?	- An error or failure in the manufacturing of the BSCU could cause operational effect	Manufacturing mistakes/errors, which could invalidate independence of the BSCU functions, are controlled by a combination of controlled manufacturing processes, inspection of sequential assembly processes, and end product pre-delivery testing of each unit produced. [see BSCU Manufacturing Quality Plan]
Channel 1 and Channel 2 common maintenance or installation procedure? Channel 1 and Channel 2 are installed incorrectly	- Erroneous or defective repair or installation procedure, missing repair or installation procedure, inadequate calibration/tools adjustments, failure to follow calibration procedures, lack of calibration procedure could cause operation effect - Lack of connector keying results in Channel 1 and Channel 2 interfaces being connected incorrectly causing operation effect	Installation and maintenance related common cause sources are controlled by reviewed and established maintenance procedures backed up by specific return to service testing. [See BSCU Return to Service Test and BSCU Installation and Service Manual]. Additionally, unique connector keying eliminates reversing BSCU connections. [See BSCU design and production data].

SAENORM.COM : Click to view the full PDF of arp4761a

1 BSCU Channel 1 is physically independent of BSCU Channel 2)		
Common Failure or Error Source Concern	**Description of Effect on Principle**	**Description of Mitigating Factors or Lack of Independence**
BSCU Channel 1 and Channel 2 have common response to mechanical, environmental or electromagnetic effects?	- Channel 1 and Channel 2 respond in the same manner to environmental conditions cause operation effect	The BSCU has been designed to meet the environmental (mechanical, thermal, electromagnetic) characteristics expected when installed on the airplane. Environmental considerations relative to common failure modes are eliminated through successful qualification and certification testing conducted in accordance with DO-160 Environmental Standards [See BSCU Environmental Test Summary].

Table Q.11-3 - (SSA - CMA - BSCU)
Command-monitor independence evaluation

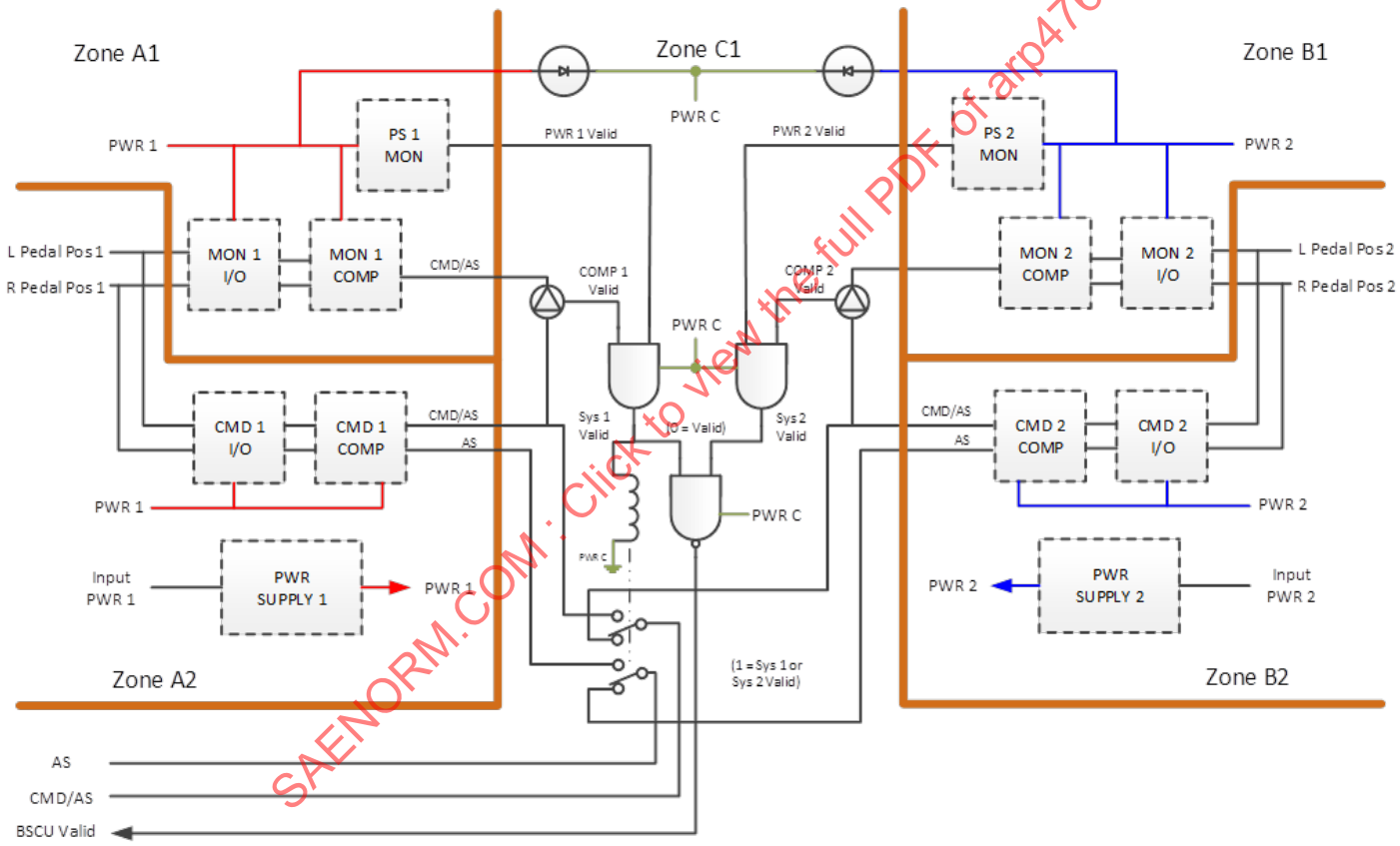
2 BSCU Channel 1 command function is physically independent from the BSCU Channel 1 monitor function. 2 BSCU Channel 2 command function is physically independent from the BSCU Channel 2 monitor function.		
Common Failure or Error Source Concern	**Description of Effect on Principle**	**Description of Mitigating Factors or Lack of Independence**
(Editor's Note: Independence requirement captured in CMA but not fully developed for brevity).		
Continue question/evaluations until Tailored Checklist is complete for the independence requirement under evaluation		

SAENORM.COM : Click to view the full PDF of arp4761a

Q.11.3.3.1 BSCU Channel 1 - Channel 2 Physical Separation Analysis

The BSCU implementation was reviewed relative to the independence requirements identified in Q.11.3.2 and the segregation guidelines established in the safety segregation design guidelines for LRUs in safety critical systems per the BSCU development plan. A number of factors were considered and are addressed individually in the following analysis.

Figure Q.11-2 summarizes the physical BSCU segregation zones that implement the Channel 1 and Channel 2 independent functions. Analysis was conducted by reviewing printed circuit wiring board documentation and other production assembly documentation (see BSCU design and production data). The design intent is that BSCU Channel 1 be entirely constrained within Zone A while BSCU Channel 2 is constrained within Zone B, assuring independence of Channel 1 and Channel 2. Each channel is further sub-divided into additional Zones 1 and 2. This division provides independence of the monitor computation and the power supply monitor functions in Zone 1 from the command computation and the power supply functions in Zone 2, respectively. The “VALIDITY” and “SWITCHING” functions are within a unique zone, Zone C1, to provide independence from common element of both Channel 1 and 2. This segregation design assures independence of the elements within each of these functions. The actual implemented design was reviewed to assure that the intent of the segregation was satisfied.



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.11-2 - (SSA - BSCU CMA)
BSCU physical implementation

The segregation analysis began at the inputs to the BSCU and proceeded through each segregation zone to identify any unintended violations of the function segregation. A list of signals which violated the segregation zones was created and summarized in Table Q.11-4. The identified signals were further analyzed to assure they were acceptable and that appropriate buffering or circuit isolation to prevent fault propagation was provided.

Table Q.11-4 - (SSA - CMA - BSCU)
Signals violating segregation zone evaluation

Signal Description	Signal Evaluation
Power supply voltages	Power supply voltages were common to all elements in each channel (however each channel's power supply voltages were found to be independent). This is acceptable given the independent power monitor input to channel validity.
Command and monitor command/anti-skid outputs	The monitor and command computation channel command/anti-skid outputs and the command computation channel anti-skid output passed from their respective segregation zones into the validity/monitor zone. The comparison and command switching between systems functions is implemented within the validity/monitor segregation zone. The command signals must pass into that zone to be switched to the output as appropriate. Adequate buffering is provided to prevent fault propagation between zones. Thus, these violations are acceptable.
Channel 2 validity, anti-skid and command/anti-skid outputs	Channel 2 BSCU validity, anti-skid, and command/anti-skid outputs passed from Channel 2 into Channel 1's validity/monitor channel. As with the similar violations of the Channel 1 commands, this is an anticipated violation given that the selection of which of the two channels is directed to the output is functionally implemented within Channel 1's validity/monitor zone. Again, adequate buffering for fault propagation was present in the design.
External power and pilot command inputs	Power and pedal inputs for Channel 1 and Channel 2 were routed through independent channel oriented connectors, keyed differently to preclude inadvertent interchanges of inputs to the two channels. All command outputs from the BSCU are routed through the Channel 1 connector. Output functions and Channel 1 input functions are separated by grounded connectors pins, eliminating undetectable inadvertent shorts between input or power and brake command or validity outputs. The validity and command outputs are also isolated from each other within the connector.

Q.11.3.4 BSCU CMA Conclusion

No BSCU common failures or errors, which could result in the loss of wheel braking or inadvertent wheel braking, remain unmitigated. Identified BSCU independence requirements are found acceptably satisfied for common cause concerns.

SAENORM.COM : Click to view the full PDF of arp4761a

Q.12 S18 AIRPLANE - BSCU SYSTEM SAFETY ASSESSMENT (SSA) FAULT TREE ANALYSIS (FTA) EXAMPLE

BSCU FTA Example

Q.12.1 BSCU FTA Example Introduction

This section comprises the Brake System Control Unit (BSCU) Fault Tree Analysis (FTA) example for the S18 airplane. The results from the BSCU FTA are used in the WBS SSA - Section Q.13.

(*Editor's Note: For the sake of brevity, only the requirements needed to support the WBS SSA example - Section Q.13 are developed in detail for this BSCU FTA example. Other requirements could be assessed by the same method shown here.)*

(Editor's Note: This example is not intended to dictate the format of an FTA report. The intent of this example is to show example FTAs that are part of the BSCU SSA process.)

Q.12.2 Summary of BSCU FTA Results

Table Q.12-1 - (SSA - BSCU - FTA)
BSCU FTA Results Summary

ID	BSCU Allocated Requirement	Allocation (/flight)	Result (/flight)
S18-WBS-R-6104	The probability of BSCU failure resulting in loss of a valid braking command output to the NMV shall not exceed 2.0E-04 per flight.	2.0E-04	7.06E-06
S18-WBS-R-6105	The probability of BSCU failure resulting in unannunciated erroneous braking command to the NMV shall not exceed 2.0E-04 per flight.	2.0E-04	2.66E-09
S18-WBS-R-6106	The probability of BSCU failure resulting in the loss of command to open the SOV shall not exceed 2.0E-04 per flight.	2.0E-04	5.02E-06
S18-WBS-R-6107	The probability of BSCU failure resulting in unintended closure of the S/ASV shall not exceed 2.0E-04 per flight.	2.0E-04	5.02E-06 (See Note 1)

Note 1: The fault tree for S18-WBS-R-6107 will be identical to that generated for S18-WBS-R-6106, since unintended closure of the S/ASV requires either failure of both Channel #1 and #2, or a failure of the BSCU switching circuitry.

Q.12.3 BSCU FTA Detail

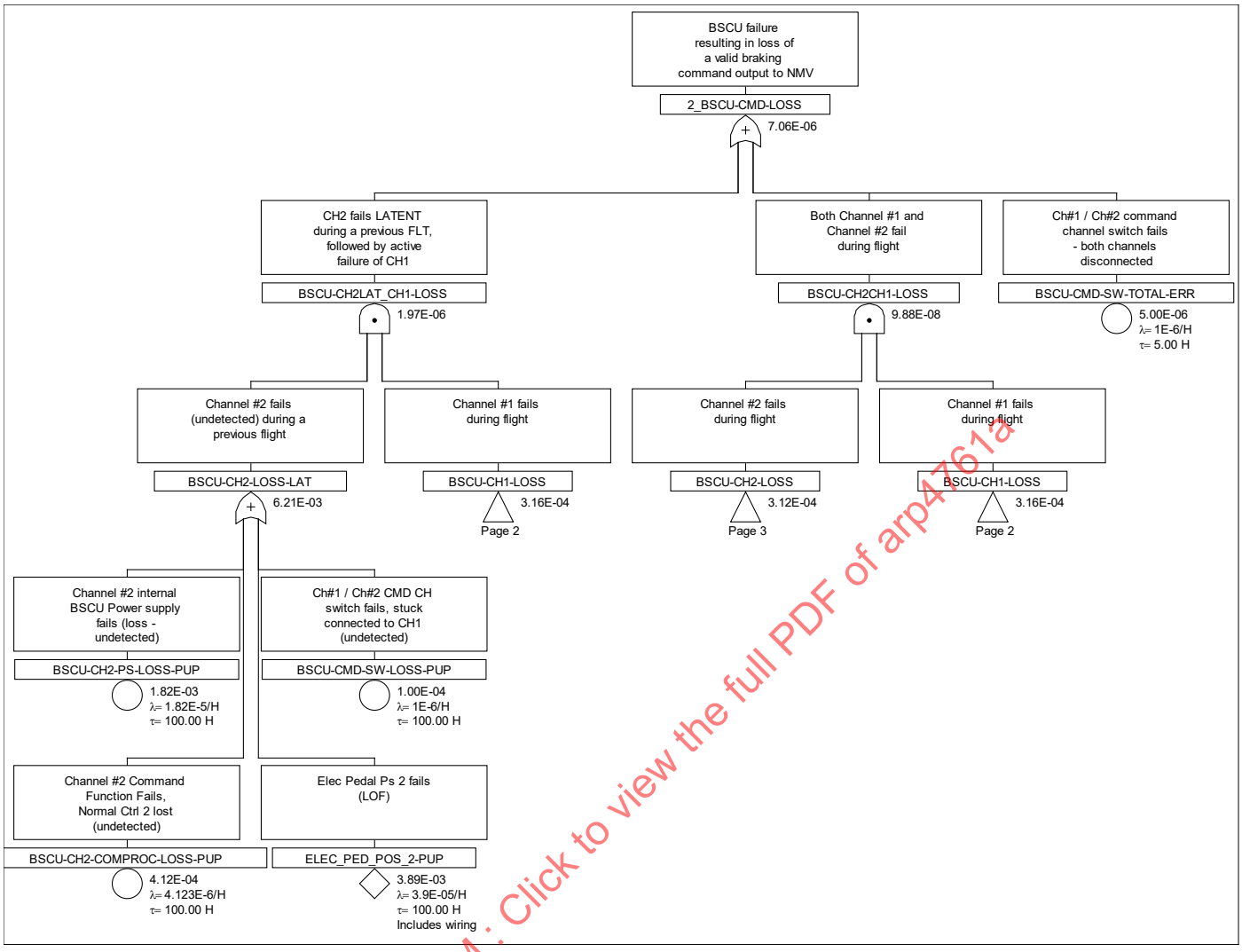
The following sub-sections detail the FTA performed for the BSCU. Failure rates for each event in the FTAs were sourced from Reliability Predictions and the BSCU FMEA.

(Editor's Note: For brevity, not all the failure rates shown in the FTAs have an identifiable source within this example.)

Q.12.3.1 BSCU Loss of Normal Braking Command to NMV

Figures Q.12-1 through Q.12-3 show the FTA for S18-WBS-R-6104, loss of a valid braking command output to the Normal Meter Valve (NMV). This analysis uses a 100-hour check time based on the power-on test that checks Channel #2 is working.

SAENORM.COM : Click to view the full PDF of arp4761a



SAENORM.COM : Click to view the full PDF of arp4761a

Figure Q.12-1 - (SSA - BSCU - FTA)
Loss of normal braking command to NMV from BSCU (page 1)

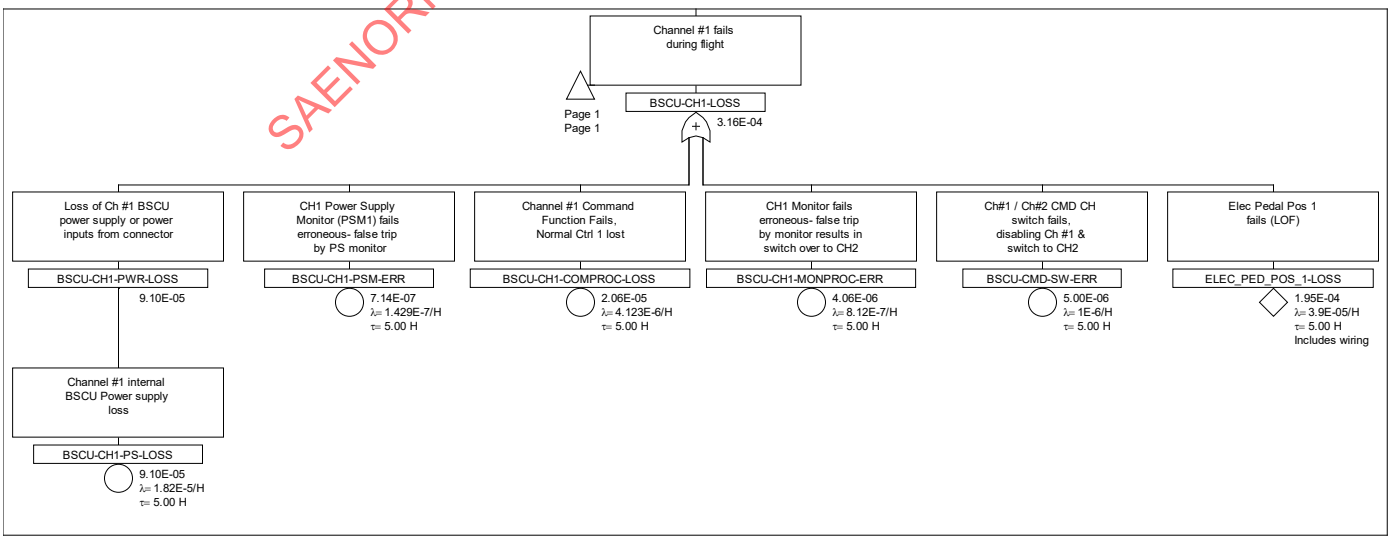


Figure Q.12-2 - (SSA - BSCU - FTA)
Loss of normal braking command to NMV from BSCU (page 2)

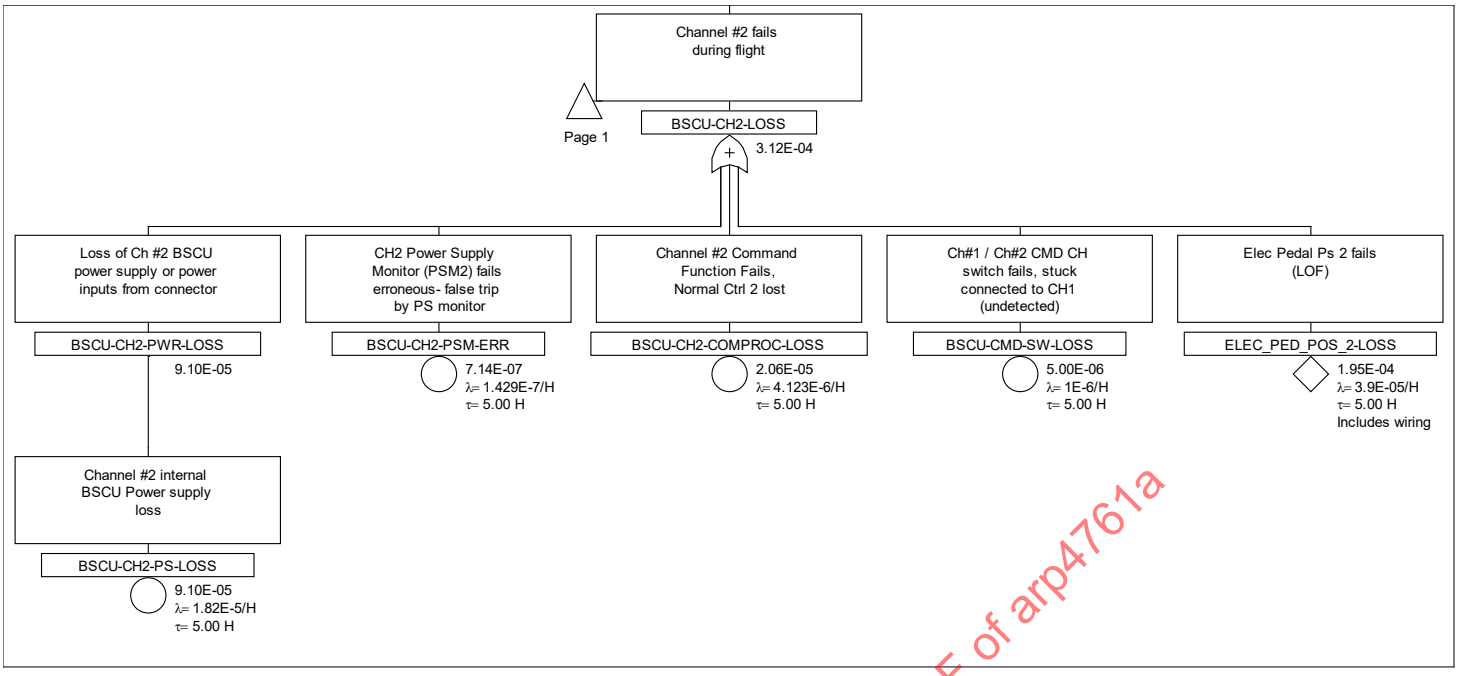


Figure Q.12-3 - (SSA - BSCU - FTA)
Loss of normal braking command to NMV from BSCU (page 3)

Q.12.3.2 BSCU Provides Erroneous Output to NMV

Figures Q.12-4 through Q.12-7 show the FTA for S18-WBS-R-6105, BSCU provides an erroneous braking command to the NMV. This analysis uses a 100-hour check time for the power supply monitor based on the power-on test that verifies the monitor is working.

SAENORM.COM : Click to view the full PDF of arp4761a