

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Root cause analysis (RCA)

Analyse de cause initiale (RCA)

IECNORM.COM : Click to view the full PDF of IEC 62740:2015



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2015 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

Plus de 60 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Root cause analysis (RCA)

Analyse de cause initiale (RCA)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.120.01

ISBN 978-2-8322-2246-1

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	9
3 Terms, definitions and abbreviations	9
3.1 Terms and definitions.....	9
3.2 Abbreviations	12
4 RCA – Overview	12
5 The RCA process	13
5.1 Overview.....	13
5.2 Initiation.....	14
5.3 Establishing facts.....	15
5.4 Analysis	17
5.4.1 Description	17
5.4.2 The analysis team	18
5.5 Validation.....	19
5.6 Presentation of results	19
6 Selection of techniques for analysing causes.....	20
6.1 General.....	20
6.2 Selection of analysis techniques	20
6.3 Useful tools to assist RCA.....	21
Annex A (informative) Summary and criteria of commonly used RCA techniques	22
A.1 General.....	22
A.2 RCA techniques	22
A.3 Criteria.....	23
Annex B (informative) RCA models	26
B.1 General.....	26
B.2 Barrier analysis.....	26
B.2.1 Overview	26
B.2.2 Strengths and limitations	27
B.3 Reason's model (Swiss cheese model)	27
B.3.1 Overview	27
B.3.2 Strengths and limitations	28
B.4 Systems models.....	28
B.5 Systems theoretic accident model and processes (STAMP)	29
B.5.1 Overview	29
B.5.2 Strengths and limitations	29
Annex C (informative) Detailed description of RCA techniques	30
C.1 General.....	30
C.2 Events and causal factors (ECF) charting	30
C.2.1 Overview	30
C.2.2 Process	31
C.2.3 Strengths and limitations	31
C.3 Multilinear events sequencing (MES) and sequentially timed events plotting (STEP).....	32

C.3.1	Overview	32
C.3.2	Process	32
C.3.3	Strengths and limitations	33
C.4	The 'why' method	35
C.4.1	Overview	35
C.4.2	Process	36
C.4.3	Strengths and limitations	36
C.5	Causes tree method (CTM)	36
C.5.1	Overview	36
C.5.2	Process	39
C.5.3	Strengths and limitations	39
C.6	Why-because analysis (WBA)	39
C.6.1	Overview	39
C.6.2	Process	42
C.6.3	Strengths and limitations	42
C.7	Fault tree and success tree method	42
C.7.1	Overview	42
C.7.2	Process	43
C.7.3	Strengths and limitations	44
C.8	Fishbone or Ishikawa diagram	44
C.8.1	Overview	44
C.8.2	Process	45
C.8.3	Strengths and limitations	46
C.9	Safety through organizational learning (SOL)	46
C.9.1	Overview	46
C.9.2	Process	46
C.9.3	Strengths and limitations	47
C.10	Management oversight and risk tree (MORT)	48
C.10.1	Overview	48
C.10.2	Process	48
C.10.3	Strengths and limitations	48
C.11	AcciMaps	49
C.11.1	Overview	49
C.11.2	Process	49
C.11.3	Strengths and limitations	51
C.12	Tripod Beta	51
C.12.1	Overview	51
C.12.2	Process	52
C.12.3	Strengths and limitations	52
C.13	Causal analysis using STAMP (CAST)	53
C.13.1	Overview	53
C.13.2	Process	56
C.13.3	Strengths and limitations	57
Annex D (informative)	Useful tools to assist root cause analysis (RCA)	58
D.1	General	58
D.2	Data mining and clustering techniques	58
D.2.1	Overview	58
D.2.2	Example 1	58
D.2.3	Example 2	58

D.2.4	Example 3	59
Annex E (informative)	Analysis of human performance	60
E.1	General.....	60
E.2	Analysis of human failure	60
E.3	Technique for retrospective and predictive analysis of cognitive errors (TRACEr).....	61
E.3.1	Overview	61
E.3.2	Process	62
E.4	Human factors analysis and classification scheme (HFACS)	63
E.4.1	Overview	63
E.4.2	Process	63
Bibliography		66
Figure 1	– RCA process	14
Figure B.1	– Broken, ineffective and missing barriers causing the focus event	26
Figure C.1	– Example of an ECF chart	31
Figure C.2	– Data in an event building block	32
Figure C.3	– Example of a time-actor matrix	34
Figure C.4	– Example of a why tree	35
Figure C.5	– Symbols and links used in CTM	37
Figure C.6	– Example of a cause tree	38
Figure C.7	– Example of a WBG	41
Figure C.8	– Example of a fault tree during the analysis	43
Figure C.9	– Example of a Fishbone diagram	45
Figure C.10	– Example of a MORT diagram	48
Figure C.11	– Example of an AcciMap	50
Figure C.12	– Example of a Tripod Beta tree diagram	52
Figure C.13	– Control structure for the water supply in a small town in Canada	55
Figure C.14	– Example CAST causal analysis for the local Department of health	56
Figure C.15	– Example CAST causal analysis for the local public utility operations management	56
Figure E.1	– Example of an TRACEr model [25]	61
Figure E.2	– Generation of internal error modes	62
Figure E.3	– Level 1: Unsafe acts	64
Figure E.4	– Level 2: Preconditions	64
Figure E.5	– Level 3: Supervision Issues	65
Figure E.6	– Level 4: Organizational Issues	65
Table 1	– Steps to RCA	13
Table A.1	– Brief description of RCA techniques	22
Table A.2	– Summary of RCA technique criteria	23
Table A.3	– Attributes of the generic RCA techniques	25
Table B.1	– Examples of barriers	27
Table B.2	– Example of the barrier analysis worksheet	27
Table C.1	– Direct and indirect causal factors	47

Table E.1 – External error modes.....	63
Table E.2 – Psychological error mechanisms	63

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ROOT CAUSE ANALYSIS (RCA)

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62740 has been prepared by IEC technical committee 56: Dependability

The text of this standard is based on the following documents:

FDIS	Report on voting
56/1590/FDIS	56/1608/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

INTRODUCTION

Root cause analysis (RCA) refers to any systematic process that identifies factors that contributed to a particular event of interest (focus event). RCA is performed with the understanding that events are addressed by understanding the root causes, rather than the immediately obvious symptoms. RCA aims to reveal root causes so that either the likelihood of them occurring, or their impact if they do occur, can be changed.

An important distinction to make is that RCA is used to analyse a focus event that has occurred and therefore analyses the past (a posteriori). However, knowledge of the root causes of past events can lead to actions that generate improvements in the future.

This International Standard is intended to reflect current good practices in the conduct of RCA. This standard is general in nature, so that it may give guidance across many industries and situations. There may be industry specific standards in existence that establish preferred methodologies for particular applications. If these standards are in harmony with this publication, the industry standards will generally be sufficient.

This standard is a generic standard and does not explicitly address safety or accident investigation although the methods described in this standard may be used for this purpose.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

ROOT CAUSE ANALYSIS (RCA)

1 Scope

This International Standard describes the basic principles of root cause analysis (RCA) and specifies the steps that a process for RCA should include.

This standard identifies a number of attributes for RCA techniques which assist with the selection of an appropriate technique. It describes each RCA technique and its relative strengths and weaknesses.

RCA is used to analyse the root causes of focus events with both positive and negative outcomes, but it is most commonly used for the analysis of failures and incidents. Causes for such events can be varied in nature, including design processes and techniques, organizational characteristics, human aspects and external events. RCA can be used for investigating the causes of non-conformances in quality (and other) management systems as well as for failure analysis, for example in maintenance or equipment testing.

RCA is used to analyse focus events that have occurred, therefore this standard only covers a posteriori analyses. It is recognized that some of the RCA techniques with adaptation can be used proactively in the design and development of items and for causal analysis during risk assessment; however, this standard focuses on the analysis of events which have occurred.

The intent of this standard is to describe a process for performing RCA and to explain the techniques for identifying root causes. These techniques are not designed to assign responsibility or liability, which is outside the scope of this standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050 (all parts), *International Electrotechnical Vocabulary*

3 Terms, definitions and abbreviations

For the purposes of this document, the definitions given in IEC 60050-192, as well as the following, apply.

3.1 Terms and definitions

3.1.1

cause

circumstance or set of circumstances that leads to failure or success

Note 1 to entry: A cause may originate during specification, design, manufacture, installation, operation or maintenance.

[SOURCE: IEC 60050-192:2014, 192-03-11 modified – addition of the words “circumstance or” and “or success” in the term]

3.1.2

causal factor

condition, action, event or state that was necessary or contributed to the occurrence of the focus event

3.1.3

contributory factor

condition, action, event or state regarded as secondary, according to the occurrence of the focus event

3.1.4

event

occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences, and can have several causes.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an "incident" or "accident".

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified – Deletion of Note 4 [1]]¹

3.1.5

failure <of an item>

loss of ability to perform as required

Note 1 to entry: A failure of an item is an event that results in a fault of that item.

Note 2 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, may be used to categorize failures according to the severity of consequences, the choice and definitions of severity criteria depending upon the field of application.

Note 3 to entry: Qualifiers, such as misuse, mishandling and weakness, may be used to categorize failures according to the cause of failure.

Note 4 to entry: This is failure of an item, not more generally of behaviour.

[SOURCE: IEC 60050-192:2014, 192-03-01, modified – Introduction of new Note 4]

3.1.6

failure mechanism

process that leads to failure

Note 1 to entry: The process may be physical, chemical, logical, psychological or a combination thereof.

[SOURCE: IEC 60050-192:2014, 192-03-12, modified – the word "psychological" has been added]

3.1.7

focus event

event which is intended to be explained causally

3.1.8

immediate causal factor

condition, action, event or state where there is no other causal factor between this causal factor and the focus event

¹ Numbers in square brackets refer to the Bibliography.

Note 1 to entry: There may be more than one immediate causal factor.

3.1.9

necessary causal factor <of an event or state>

condition, action, event or state, that resulted in the given event or state, without which the given event or state would not have occurred

3.1.10

human error

discrepancy between the human action taken or omitted, and that intended or required

Note 1 to entry: The first edition of IEC 60050-191:1990 identified "mistake" as a synonym for "human error", but a mistake is a type of human error.

Note 2 to entry: The term human error applies to any situation where the outcome is not as intended whether the intent of the person was correct or not.

[SOURCE: IEC 60050-192: 2014 192-03-14, modified – Omission of the example, addition of Note 1 and 2]

3.1.11

item

subject being considered

Note 1 to entry: The item may be an individual part, component, device, functional unit, equipment, subsystem, or system.

Note 2 to entry: The item may consist of hardware, software, people or any combination thereof.

Note 3 to entry: The item is often comprised of elements that may each be individually considered.

[SOURCE: IEC 60050-192: 2014, 192-01-01, modified – omission of internal references and Notes 4 and 5]

3.1.12

root cause

causal factor with no predecessor that is relevant for the purpose of the analysis

Note 1 to entry: A focus event normally has more than one root cause.

Note 2 to entry: In some languages, the term root cause refers to the combination of causal factors which have no causal predecessor (a cut set of causal factors).

3.1.13

root cause analysis

RCA

systematic process to identify the causes of a focus event

Note 1 to entry: IEC 60050-192:2014, definition 192-12-05 provides the following more restrictive definition "systematic process to identify the cause of a fault, failure or undesired event, so that it can be removed by design, process or procedure changes". This standard uses an extended definition to allow a wider applicability of the process.

Note 2 to entry: This note applies to the French language only.

3.1.14

stakeholder

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[SOURCE: IEC 60300-1:2014, 3.1.15] [2]

3.1.15

stopping rule

reasoned and explicit means of determining when a causal factor is defined as being a root cause

3.2 Abbreviations

BGA	Ball grid array
CAST	Causal analysis using STAMP
CCT	Causal completeness test
CT	Counterfactual test
CTM	Causes tree method
ECF	Events and causal factors
EEM	External error mode
FTA	Fault tree analysis
GEMS	Generic error modelling system
HFACS	Human factor analysis and classification scheme
IEM	Internal error mode
MES	Multilinear events sequencing
MORT	Management oversight and risk tree
PEM	Psychological error mechanism
PSF	Performance shaping factors
RCA	Root cause analysis
SOL	Safety through organizational learning
STAMP	Systems theoretic accident model and processes
STEP	Sequentially timed events plotting
TRACer	Technique for retrospective and predictive analysis of cognitive errors
WBA	Why-because analysis

4 RCA – Overview

RCA refers to any systematic process that identifies the cause or causes that contribute to a focus event. The immediate or obvious cause of a focus event is often a symptom of underlying causes and may not truly identify the root cause or causes that should be identified and addressed. RCA provides a greater understanding about why events have occurred. RCA may identify the following:

- a single root cause;
- multiple root causes in which the elimination of any cause will prevent the focus event from occurring;
- root causes which are contributory factors where elimination will change the likelihood of the focus event occurring but may not directly prevent it;
- root causes of successes.

By addressing the root cause or causes it is possible to make decisions regarding appropriate actions that will generate better outcomes in the future; implementing appropriate actions based on RCA are more effective at preventing the same or similar events with negative

outcomes occurring or increasing the probability of repeating events with positive outcomes, when compared with just addressing the immediately obvious symptoms.

RCA can be applied to any focus event whether success or failure, for example:

- 1) investigation for technological, medical and occupational focus events;
- 2) failure analysis of technological systems, to determine why an item failed to perform as and when required;
- 3) analysis of quality control and business processes;
- 4) analysis of successful outcomes.

RCA can be carried out at various levels of decomposition, for example, from system to component level or by selecting different events or outcomes as a starting point. The level appropriate to conduct the analysis will be dependent on the focus event.

RCA is used to analyse focus events which have actually occurred and is therefore applicable during the testing and operational phases of a project or product life cycle. RCA can identify problems of process including design, quality control, dependability management and project management.

The benefits of performing RCA include:

- obtaining a greater understanding into what has happened;
- finding the source of problems so corrective action can prevent future events;
- identifying the causes of events with beneficial outcomes so they can be repeated;
- identifying more effective actions to address the causes of focus events;
- achieving the objectives of focus event investigations more effectively;
- supporting traceability between focus event investigation evidence and conclusions;
- increasing consistency between investigations of similar focus events;
- increasing objectivity of focus event analysis.

5 The RCA process

5.1 Overview

To be effective, RCA should be performed systematically as an investigation, with the root causes and conclusions backed up by documented evidence. To achieve this, RCA should include the five steps shown in Table 1 and illustrated in Figure 1.

Table 1 – Steps to RCA

Step	Concepts and tasks to be performed
Initiation	Based on the knowledge available on the focus event, determine the need to carry out RCA and define the purpose and scope
Establishing facts	Collect data and establish the facts of what happened, where, when and by whom
Analysis	Use RCA tools and techniques to ascertain how and why the focus event occurred
Validation	Distinguish and resolve the different possibilities as to how and why the focus event was caused
Presentation of results	Present the results of the focus event analysis

RCA is iterative in nature, especially for data collection and analysis, in that data is collected on 'what' happened, which is then analysed in order to determine what other data needs to be collected. Once gathered, further analysis is conducted and any gaps identified, for which

further data is collected. This process is repeated until the purpose of the analysis is fulfilled and the root causes identified. The outputs of the RCA will be dependent on its purpose and scope.

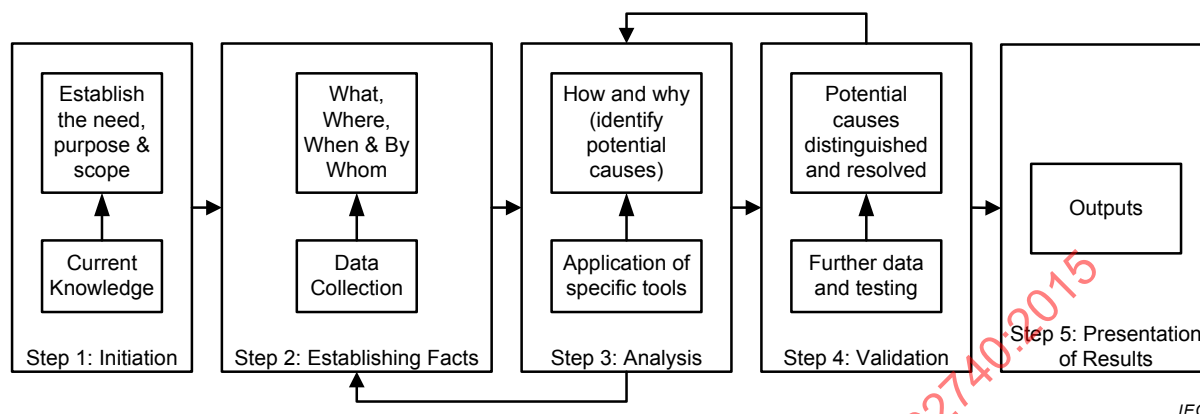


Figure 1 – RCA process

5.2 Initiation

The first step initiates the RCA process by evaluating the need to carry out RCA. It defines the purpose and scope of the analysis, in response to the focus event, and establishes a team and resources to carry out the RCA.

There is usually some criterion which is used to determine when an RCA is required, which may include:

- any single event with a large effect;
- multiple similar undesirable events;
- a parameter moving out of a defined tolerance level;
- failures or successes (whatever the level of effect) that involve critical items of equipment or activities.

When defining the type of events that require the conduct of RCA, it is important to consider that an event with a large effect may have common root causes to events with minor effects. Analysing and addressing root causes for events with minor effects may prevent a large effect event occurring. Examples of events where RCA may be required include: completion of a project (successes and failures), failures that result in unacceptable costs, injury or fatality, unacceptable performance or delays, large contractual consequences and equipment breakdown.

If a RCA is required, the focus event(s) to be analysed is/are described and an appropriate team appointed for the analysis. The description should include the background and context in which the focus event(s) occurred. A good description of a focus event is short, simple and easy to understand and should not be biased towards a specific solution. This description is used to identify appropriate members of the analysis team and ascertain where to start collecting data.

The purpose and scope of the RCA should be determined, taking into account knowledge of system, functions, interfaces etc. In some cases, the purpose of the analysis is to identify the causes of the focus event. In others, the purpose may be broader, for example, to also identify matters of concern outside those that led to the focus event.

There are in general two different types of RCA that have different objectives and should not be mixed up. These two types can be described as follows:

- 1) analysing a focus event using only verifiable factual information;
- 2) analysing a focus event to obtain hypotheses of sequences of events and cause.

The first version focuses on observed facts only. It may be an analysis "per se" according to the purpose of the study and no hypothesis about event occurrence is acceptable for this analysis. The second can be implemented when sufficient factual information is not available and hypotheses of potential causes are acceptable for the purpose of the analysis.

The outputs required of the RCA should also be identified. Examples are as follows:

- provide a description of each root cause along with sufficient background information to allow the identification of suitable actions;
- recommend actions that, taken together, prevent further occurrences of similar events with adverse consequences and improve the likelihood of successes;
- identify, implement and review actions to address root causes.

RCA can include the analysis of systems in which the boundaries continually evolve and interact with their environment; this interaction can take the form of information, energy, or material transfer. Therefore, the scope should specify the boundary of the analysis (what is included and what is excluded).

The scope of the analysis should where possible include a definition of the 'stopping rule', which is the point at which action can be defined or additional proof of cause is no longer necessary for the purpose of the analysis. For example, the last point where corrective action can be identified, before factors that cannot be influenced e.g. weather. It may however be more appropriate to ascertain the stopping rule at review points that determine whether further analysis is required.

RCA can be effectively carried out by one person provided that person is experienced with the causal analysis technique, is a domain expert (or has immediate access to domain experts) and has access to all the data required. However, it is more common to conduct RCA as a team. The team members for the analysis should be selected based on the specific expertise needed to analyse the focus event. The team should include:

- a person or persons who among them can provide a complete systems overview and knowledge of the programme or project and focus event;
- a facilitator skilled in the causal analysis technique, desirably trained or experienced in the facilitation of the causal analysis technique.

Team members can change depending on the activity being conducted, e.g. team members responsible for data collection will not necessarily be the same as those conducting the analysis. Team members can include engineers, technicians, operators, sales representatives and managers. The use of external parties should be considered to provide an independent perspective and avoid blind spots that may exist in the organization. Additional team members should be included for specific activities during the investigation to either bring expertise into the team or to increase the influence of the team. The role of these additional team members is to support the investigation so that it is not halted for technical or organizational boundary reasons. It is not appropriate for persons who may have had a role in causation of the focus event to be part of the team. Their input should be collected during the first two steps.

5.3 Establishing facts

This step includes all the activities necessary to prepare for the analysis. Establishing the facts is usually the largest part of the RCA. Facts should be determined on 'what' happened, 'where', 'when' and 'by whom'.

Data should be collected, before it is lost (e.g. before evidence is disturbed or removed, or memories fade). In general data collected would include:

- a) the context in which the focus event occurred;
- b) the conditions before, during and after the focus event;
- c) personnel involvement including actions taken (or not taken) and decisions made;
- d) context data about the surroundings, including environmental data;
- e) how the organization operates including organization charts, processes and procedures, training and skills;
- f) historical data relating to similar events or precursors;
- g) deviations from the expected;
- h) interactions with other items and personnel;
- i) equipment involved, its operating state and compliance with requirements.

The following lists examples of data that may be relevant:

- 1) Inspection of physical evidence such as failed components and failure reports. Generally, it is experience that will determine what physical evidence is required. If there is doubt, the evidence should be retained. It is also important to preserve the evidence.
- 2) Photographs and videos taken by monitoring cameras. Photographing the area of the occurrence from several views will also be useful in the analysis phase.
- 3) Operational data, recorded by monitoring systems, control systems, alarm and event loggers etc. Operator logs can be critical to understanding the operating conditions at the time of failure and since they are typically dated (or clocked), they are ideal for generating a timeline of events.
- 4) Personal testimony gathered by conducting interviews. Interviews should concentrate on data collection, e.g. building a consistent timeline etc; any premature discussion of the causes of the failure may adversely impact the interview process. Questions should be prepared before the interview to ensure that all necessary information is obtained. Interviews should be conducted with those people, who are the most familiar with the focus event, however, consider interviewing other personnel e.g. people who have performed the job in the past. All interviews should be documented.
- 5) Documentary evidence of relevant procedures, operating environment and regulatory environment.

This step can include failure analysis which examines failed components using a wide array of methods including microscopy, spectroscopy and non-destructive testing or models on the development of failure such as fire modelling or crash modelling.

Once all the data associated with the focus event has been collected, the data should be reviewed for correctness and suitability, missing data should be obtained and any inconsistencies should be resolved to ensure a clear and consistent picture of the focus event is determined.

The outcome of this step is information and understanding, supported by physical evidence and witness statements, concerning

- what happened including the circumstances that lead to the focus event,
- the time sequence of events which lead to the focus event,
- the location of the focus event,
- actions of people associated with the focus event,
- any necessary conditions for the focus event,
- the consequences of the focus event.

5.4 Analysis

5.4.1 Description

Having determined 'what' happened, 'where', 'when' and 'by whom', this step establishes 'how' and 'why' the focus event occurred. The objective of this step is to understand the focus event and its causes by structuring the data that has been collected into a form that allows root causes to be systematically derived.

RCA normally analyses facts to identify the causes that were necessary for the focus event to occur, referred to as "necessary causal factors". However, in some cases, for example where sufficient facts are not available, the analysis may propose one or more hypotheses for cause and may also identify contributory factors and prevailing conditions which were possibly associated with the focus event, but cannot be proven to be necessary causal factors.

Analysis involves the following:

- organizing the physical evidence and witness statements concerning actions, events, conditions and outcomes;
- seeking how and why the focus event occurred using the data collected to justify conclusions. Models of causation, laboratory testing, check lists and taxonomies or statistical analysis of data may be used to assist this process;
- looking beyond the immediate causal factors to why they occurred. The aim is to seek all causal factors that contributed, not only the obvious causes;
- continuing this process until the stopping rule is invoked and root causes identified. There may be multiple root causes which can be independent or correlated.

In general, causal factors may involve technical issues, human aspects and factors relating to the physical or psycho-social environment in which the focus event occurred. All of these should be considered in seeking root causes. People with expertise in these areas should therefore be involved in the analysis.

Causal factors should be described clearly and unambiguously. Where a human action, omission or decision is identified as a causal factor, the nature of the act or decision should be specified, e.g. "the operator switched off the wrong power switch" and not just "human error".

The analysis of the causes (depending on the purpose and scope of the analysis) can consider:

- how the focus event occurred, i.e. the physical, chemical, psychological or logical process that was involved;
- preceding events or conditions that were necessary for the focus event to occur;
- relationships between causal factors including how they combined to cause the focus event and how a root cause leads to the focus event;
- organizational and management influences and human factors that were involved in the focus event or in the events and conditions leading up to it;
- prevailing conditions that may have contributed to the event occurring but were not necessary causal factors;
- matters of concern that could lead to other focus events (these are not strictly causal factors but may be an outcome of the analysis).

A structured analysis technique should be used to perform the analysis. Several formal techniques exist ranging from those that are based on a checklist of causes to techniques that guide the analyst through consideration of causes and graphically present the results. The techniques range from simple to complex and require suitably skilled practitioners or facilitators to conduct the analysis. Some techniques are based on particular models of how a

focus event occurs and hence give a particular emphasis to the results. The different models are based on different hypotheses with regard to the causation therefore they tend to lead the investigator to identify different contributory factors.

In some cases it is appropriate to use more than one technique or to take into account considerations of more than one model to identify all root causes.

Models of causation are described in Annex B and analysis techniques are described in Annex C. The most appropriate technique will be dependent on the focus event and the purpose and scope of the analysis (see Clause 6).

The analysis may indicate that further data is required. Requests for such data should be expected to occur throughout the analysis to resolve inconsistencies or complete gaps in the analysis. The analysis should continue until a 'stopping rule' is invoked.

5.4.2 The analysis team

A leader should be appointed for the analysis step, who is responsible for the following preparatory work:

- a) obtaining copies of the agreed role and responsibilities of the team, and purpose and scope of the analysis;
- b) obtaining copies of the focus event description and the facts established;
- c) deciding the analysis technique(s) to be used;
- d) converting the focus event description and facts established into a suitable format for use in the analysis technique selected;
- e) developing an analysis plan;
- f) forming the analysis team;
- g) facilitating or arranging for training of team members in the analysis technique selected;
- h) selecting software tools or other templates for use during the analysis;
- i) arranging for a search to be made of databases, media, legal proceedings, etc. to identify focus events of a similar nature, or which may have occurred with the same or similar technologies.

The leader should review the information available to determine what analysis technique(s) should be applied and what skills are required. Expert advice in the field of RCA may need to be obtained regarding the selection of the analysis technique. The leader may also require an expert RCA facilitator for all or part of the analysis, depending on the complexity of the focus event, the complexity or volume of evidence and data or analysis technique selected.

The analysis is usually carried out by a team, with each team member being chosen for their experience and skills. The analysis team should be as small as possible, consistent with the relevant technical and operating skills and experience being available. Where input will be required from multiple parties, stakeholders or entities, the analysis team should contain representatives of each. It is the leader's responsibility to ensure the relevant stakeholders are informed, so that adequate stakeholder representation is available during the analysis.

The role and responsibilities of the analysis team members should be determined and milestones established at the outset of the analysis. A programme of meetings should be developed which reflects the objectives and milestones provided to the analysis team. This will ultimately enable any recommendations to be carried out in a timely fashion.

The leader should develop an analysis plan, which should contain the following:

- 1) focus event description;
- 2) agreed roles and responsibilities of the team, and the purpose and scope of the analysis;

- 3) a list of team members and the stakeholders to be represented;
- 4) time, date and location of the analysis meetings;
- 5) a summary of the data available;
- 6) analysis technique(s) to be used;
- 7) arrangements for training the analysis team in the selected analysis technique (if required);
- 8) the form of recording of the analysis and the analysis results, including reference to any templates or software tools to be used.

Adequate room facilities with visual and recording aids should be arranged by the leader for the efficient conduct of the analysis meetings. A briefing package consisting of the analysis plan and any essential pre-meeting reading or references should be sent to the analysis team members in advance of the first meeting, to allow them to familiarize themselves with the information available and the selected analysis technique.

The leader should ensure that an appropriate communication system is in place for informing and transferring the results of the analysis to those responsible for the next step of the RCA process (see 5.5).

5.5 Validation

A number of review activities are conducted throughout the RCA process to determine whether data collected is relevant and the analysis is representative of the data collected. This step tests whether the causes identified in the analysis can be substantiated and may be interleaved with the analysis or conducted as a separate activity.

An independent review can be carried out to assess whether the analysis is complete and correct and to determine whether the purpose of the analysis has been fulfilled. The review method will be dependent on the analysis technique used and on the focus event. In some cases experiments can be performed to repeat the occurrence of the focus event; where appropriate, statistical methods should be used to assess the degree of confirmation of the hypothesis of cause. If the causes are validated with the help of simulation, care should be taken to ensure the simulation is representative.

During the analysis there may be several alternative hypotheses of how the event could have happened. If the objective is to produce a factual report of the causes then at the completion of the analysis the causes should be validated and only a single conclusion should remain.

This step may require further data collection to seek direct evidence to support or refute the causes identified. Evidence may not always be available to fully validate all potential causes.

5.6 Presentation of results

The results of the analysis will depend on the purpose of the analysis. For example, if the purpose of the analysis is to identify the actions that, taken together, prevent further occurrences of similar events, the analysis results should identify corrective actions which break the causal network and prevent the focus event occurring again. If the purpose of the analysis is to repeat successes, then actions that enhance the likelihood or the consequences of the focus event should be proposed. The effectiveness of the analysis results is dependent on the quality of the analysis.

An agreed format for presenting the results of the RCA should be developed that summarizes the analysis and captures the required outcomes from the analysis, e.g. recommended actions. If the expected outcome of the RCA is to produce recommended actions, the summary should include the following as a minimum:

- a) a general description of each cause requiring action along with sufficient background information and detail, to ensure the need to address each cause is understood and actions to be taken can be identified;
- b) a set of options for treatment actions and, where practicable, and within the scope, a summary of the benefits and costs of each;
- c) recommended actions to address each of the causes identified.

Recommended corrective actions should be evaluated for effectiveness and realism. In general, corrective actions aim to achieve the following:

- change the likelihood of the focus event and/or its consequences (i.e. reduce the likelihood or consequence of undesirable events or increase the likelihood or consequence of successful events);
- not to introduce new unacceptable risks, e.g. the safety of other systems must not be degraded by the proposed corrective action.

Where actions are identified they should be reviewed prior to implementation to determine whether they have not only addressed the root causes, but also not introduced new unexpected consequences and will therefore function as intended. Also reoccurrence of the same or a similar event should be monitored in order to evaluate the effectiveness of actions taken.

6 Selection of techniques for analysing causes

6.1 General

Formal techniques have been devised to help analysts identify causal factors and eventually root causes. Analysis techniques may perform one or more of the following functions:

- organize data and provide structure to the analysis and identify where further evidence is needed;
- provide a visual display of the evidence relating to the focus event, for example the time sequence of events or causal chains;
- conduct statistical analysis of the data, particularly from multiple similar events, to identify common causal factors;
- provide guidance to identify possible causal factors for further investigation and comparison with data (such methods include check lists and methods based on models of causation);
- guide the analysts through the causal chain to a set of root causes.

6.2 Selection of analysis techniques

RCA is undertaken in varying degrees of depth and may use one or several analysis techniques ranging from simple to complex. The depth of the analysis and technique(s) used should exhibit the following characteristics:

- be justifiable and appropriate to the focus event under analysis and the scope and the purpose of the analysis;
- provide results that enhance the understanding of the root causes of the focus event;
- be capable of use in a manner that is traceable, repeatable and verifiable.

The analysis techniques to be used are selected based on the applicable factors such as

- characteristics of the analysis technique,
- characteristics of the focus event e.g. severity or potential severity or complexity,

- characteristics of the organization, e.g. industry/sector approved techniques or cost benefit evaluation,
- purpose of the analysis e.g. outputs required or stakeholder expectations,
- the causation model or models most appropriate to the objectives of the analysis.

The attributes of the most commonly used analysis techniques are described at Annex A. The criteria used to characterize the techniques, described in Annex A, are as follows:

- expertise required;
- tool support;
- scalability;
- graphical representation;
- modularity;
- reproducibility;
- plausibility checks;
- intellectual rigour;
- time sequence;
- specificity.

Detailed descriptions of the RCA techniques are described in Annex C, which includes the methods and process used for each technique along with their strengths and weaknesses.

6.3 Useful tools to assist RCA

Modern data mining techniques enable a search for specific properties and conditions. Clustering analysis selects data that are closely related, and thereby identify deviating data (outliers). Modern cluster analysis can detect data that are closely related in one, two or more dimensions and thereby analyse products or processes that are closely related and identify deviating data points (outliers). An overview of these techniques is provided in Annex D.

Many focus events and analysis techniques involve human factors and several taxonomies have been developed to assist in finding root causes where human behaviour is involved. Two examples are given in Annex E.

Annex A (informative)

Summary and criteria of commonly used RCA techniques

A.1 General

Annex A lists the most commonly used RCA techniques, with a brief description, and provides a reference list of criteria which can be used to compare different RCA techniques. The list is not comprehensive but covers examples of the different types of techniques used.

A.2 RCA techniques

Table A.1 provides a list and brief description of the most commonly used RCA techniques.

Table A.1 – Brief description of RCA techniques

Technique	Description
Events and causal factors (ECF) charting	ECF analysis identifies the time sequence of a series of tasks and/or actions and the surrounding conditions leading to a focus event. These are displayed in a cause-effects diagram
Multilinear events sequencing (MES) and sequentially timed events plotting (STEP)	MES and STEP are methods of data-gathering and tracking for the analysis of complex focus events. The results are displayed as a time-actor matrix of events
The 'why' method	The 'why' method guides the analysis through the causal chain by asking the question why a number of times.
Causes tree method (CTM)	CTM is a systematic technique for analysing and graphically depicting the events and conditions that contributed to a focus event. CTM is similar to the 'why' method in concept, but builds a more complex tree and explicitly considers technical, organizational, human and environmental causes
Why-because analysis (WBA)	WBA establishes the network of causal factors responsible for a focus event using a two-factor comparison, the counterfactual test. The network of factors is displayed in a "why-because" graph
Fault tree and success tree method	Fault or success tree is a graphic display of information to aid the user in conducting a deductive analysis to determine critical paths to success or failure, which are displayed graphically in a logic tree diagram
Fishbone or Ishikawa diagram	The Fishbone or Ishikawa diagram is a technique that helps identify, analyse and present the possible causes of a focus event. The technique illustrates the relationship between the focus event and all the factors that may influence it
Safety through organizational learning (SOL)	SOL is a checklist-driven analysis tool, oriented towards focus events in nuclear power stations. Results are in the visual form of a time-actor diagram, derived from the MES/STEP method
Management oversight and risk tree (MORT)	The MORT chart is a pre-populated fault tree with events, usually faults or oversights, expressed in generic terms. The MORT tree contains two main branches and many sub-branches giving a high level of detail. One main branch identifies about 130 specific control factors while the other main branch identifies over 100 management system factors. The chart also contains a further 30 information system factors common to both main branches of the tree
AcciMaps	AcciMaps is primarily a technique for displaying the results of a causal analysis. It requires an organizational model to separate factors into layers and to elicit factors in the layers; applies a version of the counterfactual test (see WBA) to determine the causal relations amongst the factors
Tripod Beta	Tripod Beta is a tree diagram representation of the causal network, focusing on human factors and looking for failures in the organization that can cause human errors

Technique	Description
Causal analysis for systems theoretic accident model and process (STAMP) (CAST)	CAST is a technique that examines the entire socio-technical process involved in a focus event. CAST documents the dynamic process leading to the focus event including the socio-technical control structure as well as the constraints that were violated at each level of the control structure

A.3 Criteria

Table A.2 provides a list and describes the criteria used to characterize the RCA techniques listed in Table A.1. Each criterion has three levels indicated by a (+), (o) or a (–), where the different levels indicate the range.

The attributes for each RCA technique using the criteria in Table A.2 are shown in Table A.3.

Table A.2 – Summary of RCA technique criteria

Criteria	Description	Levels
Expertise required	Is the method targeted towards the "sophisticated user" (does it require use of techniques such as theorem proving which requires specific expertise)? Is it suitable for use by domain experts only?	• Intuitive, little training necessary (+) • Limited training required e.g. one day (o) • Considerable training effort necessary, e.g. one week (–)
Tool support	Is tool support necessary?	• Can be well applied without dedicated tool support (+) • Tool support not required but usually needed for effective application (o) • Tool support necessary, can be applied only with dedicated tool support (–)
Scalability	Is the method scalable? Can the method be used cost effectively for simple as well as complex focus events? Can a subset of the method be applied to small, or to less-significant focus events and the full capability applied to large, or to significant focus events? So the question of scalability asks whether the complexity of analysis using the method scales with the complexity of the focus event	• Scales well with complexity (+) • Limited scalability, considerable overhead with every application (o) • Not scalable, the full method has to be applied (–)
Graphical representation	What is the nature of the method's graphical representation? The motivating principle is that a picture is better than a thousand words. It is often more comprehensible to display results of an analysis method as an image, a graph, or other form of illustration, than as purely written text. The desirable properties of a graphical representation are • to display clearly the semantics of causality (including denotation of causal factors, and taxonomy of factors), • to be cognitively (relatively) easily evaluated by a single person, • ideally, a graphical representation could also display the history of the analysis	• Graphical representation with clearly defined semantics and cognitively easy to understand (+) • Graphical representation, but without semantics (o) • No graphical representation defined (–)

Criteria	Description	Levels
Reproducibility	Are the results of the method reproducible? Would different analysts obtain similar results for the same focus event?	- The results can be reproduced, differences are only observed on the representation of the results, wording etc. (+) - A significant amount of the results can be reproduced, but some differences will be observed (o) - The results will depend on the analyst's expertise (–)
Plausibility checks	Are there reasonable, quick plausibility checks on the results obtained which are independent of the tool? What ways are there of checking the "correctness" of the results? One example would be checklists	- There are plausibility checks for almost all aspects (+) - There are plausibility checks, e.g. checklists, but they do not necessarily cover all aspects (o) - There exist only limited means supporting plausibility checks (–)
Intellectual rigour	How rigorous is the method? Rigour has two relevant aspects: - Does the method have a rigorous meaning, formal semantics, for the key notions of causal factor and root cause? Are the semantics easy to apply? - Are the results of the method amenable to formal (mathematical) verification? To what extent is an application of the method so amenable?	- Formally defined and can be formally verified (+) - Semi-formal definition (o) - Informal definition (–)
Time sequence	Does the method contain a representation of time sequence of events?	- Yes (+) - Only indirectly (o) - No (–)
Specificity	The extent to which the method limits analysis to necessary causal factors of the focus event rather than exploring a range of general problems with the system that existed at the time of the focus event and may have contributed	- Method only analyses necessary causal factors of the focus event (+) - Method can be used to analyse contributory factors as well as necessary causal factors of the focus event (o) - Method seeks problems in general whether or not they were necessary causal factors of the focus event (–)

Table A.3 – Attributes of the generic RCA techniques

	Expertise required	Tool support	Scalability	Graphical representation	Reproducibility	Plausibility checks	Intellectual rigour	Time sequence	Specificity
ECF	0	0	0	+	0	0	0	+	+
MES and STEP	-	0	0	+	+	0	0	+	+
The 'Why' Method	+	+	-	0	-	-	-	-	+
CTM	0	0	+	+	0	0	0	-	+
WBA	0	+	0	+	+	+	+	0	+
Fault tree and success tree method	0	0	0	+	0	0	0	-	0
Fishbone or Ishikawa Diagram	+	+	-	0		0	-	-	0
SOL	0	-	+	0	+	+	0	+	0
MORT	+	-	-	0	+	0	0	-	-
AcciMaps	0	0	0	+	-	0	-	-	0
Tripod Beta	-	+	0	*	0	0	0	0	0
CAST	+	+	+	0	0	0	0	+	+

NOTE The criteria for each attribute are described in Table A.2.

Annex B (informative)

RCA models

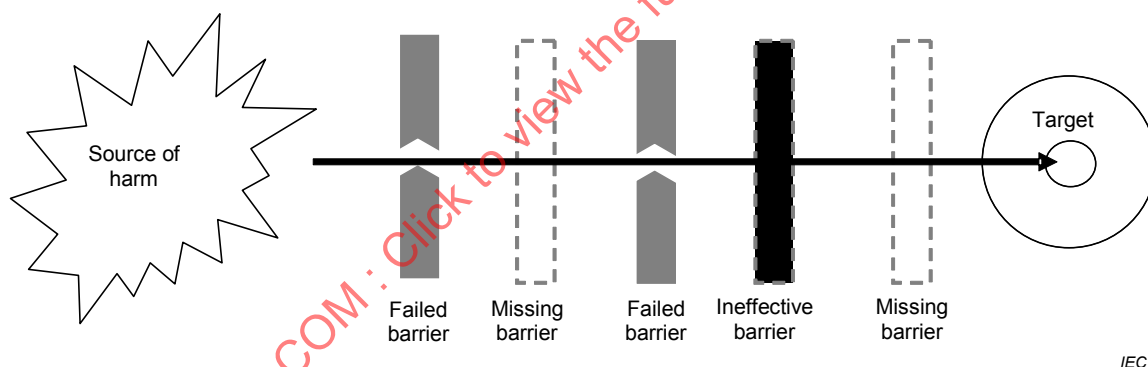
B.1 General

This annex describes the most commonly used RCA models which provide different ways of thinking about focus events. The different models are based on certain hypothesis with regard to the focus event, e.g. barrier analysis assumes the focus event has occurred as a result of missing, failed or ineffective barriers. Therefore, the different models tend to lead the investigator to identify different causal factors. Models are used to direct thinking in conjunction with the techniques of Annex C, or simply to identify a set of causal factors.

B.2 Barrier analysis

B.2.1 Overview

Barrier analysis is based on the hypothesis that a focus event occurs as a result of the interaction of a source of harm on a target and that this can be prevented by the use of barriers [3]. An undesirable event occurs when the barriers are missing, failed or ineffective (see Figure B.1).



IEC

Figure B.1 – Broken, ineffective and missing barriers causing the focus event

Haddon [3] considered focus events where the source of harm is physical energy and barriers relate to how the energy can be modified or prevented from impinging on the target. The model has been extended in various ways [4], for example barriers are often divided into physical barriers and administrative barriers (see Table B.1 for some examples). Barriers may also be considered in terms of prevention, protection and detection (for example in the context where the focus event is a fire, these would be using non-flammable materials, providing fire extinguishers and installing smoke alarms).

The output of the analysis generally includes a barrier analysis worksheet (see Table B.2), which identifies those barriers that either were available but ineffective or were not in place during the occurrence of the focus event.

Table B.1 – Examples of barriers

Physical or energy barriers	Administrative barriers
Engineered safety features	Plant operating and maintenance procedures
Safety and relief devices	Regulations, policies and practices
Conservative design allowances	Training and education
Redundant equipment	Work protection
Locked doors and valves	Work permits
Ground fault protection devices	Skilled people
Shielding and guards	Methods of communication (3-way communication)
Alarms	Supervisory practices
Automatic fire containment systems	

Table B.2 – Example of the barrier analysis worksheet

Undesired outcome (what happened?)	Source of harm	Barrier(s) that should have precluded the undesired event	Barrier failure mechanism (how the barrier failed)	Barrier assessment (why the barrier(s) failed)
List one at a time, need not be in sequential order		List all physical and administrative barriers for each undesired outcome		Identify if the barrier was missing, weak or ineffective; and why
Maintenance worker loosened nuts on flange of the pipe line that was pressurized	Pressurized liquid	Procedure to switch off pump and release pressure before commencing work	Pressure released on wrong system	Unclear labelling

B.2.2 Strengths and limitations

The strengths of barrier analysis are as follows:

- identifies what corrective actions are required to ensure adequate barriers (number and effectiveness) are in place.

The limitations of barrier analysis are as follows:

- may not recognize all failed or missing barriers, or the effect of the rate or frequency with which the barriers are challenged;
- addresses immediate causal factors rather than root causes, i.e. it seeks what barrier failed and how, but does not explore why in any depth.

B.3 Reason's model (Swiss cheese model)

B.3.1 Overview

Reason's model [5] is based on the premise that the basic required elements of any productive system are

- appropriate decisions from plant and corporate management,
- line management activities, operations-maintenance training, etc.,
- reliable and fit for use equipment,
- motivated workforce,

- integration of human and mechanical elements,
- safeguards against foreseeable risks.

There are inevitably weaknesses in these elements that can be considered to be latent failures. If these come together to form a triggering event, which may be unimportant in other circumstances, this results in failure.

The weaknesses in the elements of the productive system are pictured as holes in slices of Swiss cheese. An event will result when all individual weaknesses align. Reason's model is not strictly a barrier model as the layers are normal operating systems with weaknesses rather than failed barriers or controls.

Human error taxonomies based on Reason's model have been developed for a number of different industries.

B.3.2 Strengths and limitations

The strengths of Reason's model are as follows:

- encourages the analyst to explore causal factors of operator error and hence possible means of reducing it.

The limitations of Reason's model are as follows:

- superficial analysis of technical or environmental causal factors which considers technical aspects only in terms of failed barriers;
- assumes the core problem is operator error (errors at other levels and organizational failures are explored primarily in terms of how they influence operator error);
- does not supply a taxonomy to assist with the identification of motivations and psychological precursors of human error or in identification of latent failures and hence requires expertise in individual and organizational psychology to use properly.

B.4 Systems models

Systems theory [6] was developed in the 1940s and 1950s to handle the increase in complexity of systems after WWII and to consider the social and technical aspects of systems together as a whole.

In system models it is assumed that human interaction with technology in complex social structures is influenced by the organization's goals, policy and culture and by internal and external economic, legal, political and environmental elements. This system is stressed by the fast pace of technological change, by an increasingly aggressive, competitive environment, and by factors such as changing regulatory practices and public pressure. In this context focus events are due to multiple factors and are typically 'waiting for release' and not due to any one act or event.

Failures arise due to the complex interactions between system components that may lead to degradation of system performance. Two or more discrete events within system elements can interact in unexpected ways which designers could not have predicted and operators cannot comprehend or control without exhaustive modelling or test. Factors contributing to the focus event may include effects of decisions which are normal in the circumstances in which they were made, but produce an unwanted outcome.

Methods based on a systems model do not seek a causal chain or look for individual error or technical failures but consider the system as a whole, its interactions and its weaknesses. Individual human or hardware failures may be recognized but the focus is on interactions and systemic issues.

B.5 Systems theoretic accident model and processes (STAMP)

B.5.1 Overview

STAMP [7] is a causality model based on systems theory [6] that extends the traditional model (chains of directly related failure events) to include both the technical and social contributors to focus events and their relationships. It also captures focus events involving interactions among non-failing system components and processes, indirect and systemic causal mechanisms, complex operator and managerial decision making, advanced technology such as digital systems and software and system design flaws.

STAMP assumes incidents arise from interactions among humans, machines and the environment; it treats systems as dynamic control problems in which the controls aim to manage the interactions among the system components and its environment. The goal of the control is to enforce constraints on the behaviour of the system components, for example, aircraft in an air traffic control system have to always maintain a minimum separation distance. Focus events result from inadequate control or enforcement of constraints on the development, design and operation of the system. In the space shuttle "Challenger" loss, for example, the O-rings did not control propellant gas release through the field joint of the space shuttle. In STAMP, the cause of a focus event is a flawed control structure.

STAMP also incorporates the concept that incidents often arise from a slow migration of the whole system toward a state of high risk [8] so that financial and other pressures that lead to changing behaviour over time can be accounted for in the causal analysis process.

B.5.2 Strengths and limitations

The strengths of STAMP are as follows:

- considers the role of the entire socio-technical system in causation;
- includes indirect and systemic factors in the causal explanation;
- provides a model to explain accidents in very complex systems;
- identifies the causes back to the process with which a system was developed.

The limitations of STAMP are as follows:

- requires focus events to be analysed in a way that is often unfamiliar to engineers, therefore may take more time to learn how to analyse focus events using causal analysis processes based on STAMP.

Annex C (informative)

Detailed description of RCA techniques

C.1 General

Annex C describes a range of techniques used during a RCA. The list is not comprehensive but covers examples of the different types of techniques used. Many of these techniques are supported by software tools. Some of the methodologies and software tools have elements that are proprietary, which may impact on the cost of implementing the technique.

Some techniques aim to identify causal factors that can be shown to be necessary if the focus event is to occur. Other methods seek general weaknesses of the system as a whole that probably contributed to the focus event but where the focus event could have occurred in their absence. In some terminologies a “causal factor” cannot be so described unless it is necessary to the focus event. In this annex such causal factors are referred to as “necessary causal factors”. Identified weaknesses that may have played a part in the focus event but may not be necessary to it are referred to as “contributory factors”.

In general, identification of necessary causal factors will be repeatable and based on evidence. There may be a higher level of subjectivity in identifying contributory factors and different analysis techniques with a different focus may identify different factors.

C.2 Events and causal factors (ECF) charting

C.2.1 Overview

The ECF chart [9] records events in chronological order from left to right in rectangles, with events characterized by single subjects and active verbs. Each event is derived strictly from the one before. Conditions necessary for the events are displayed in ovals above and below the sequence of events (conditions are states or circumstances rather than happenings). Events are connected by solid lines and conditions by dashed lines. Events and conditions based on evidence have a solid outline, whereas those that are presumptive have a dashed outline. There may be multiple or branching sequences of events, each with their own conditions.

Figure C.1 illustrates an example of an ECF chart in which a maintenance activity was incorrectly carried out due to the maintainer turning up late, resulting in an emergency landing carried out by an aircraft.

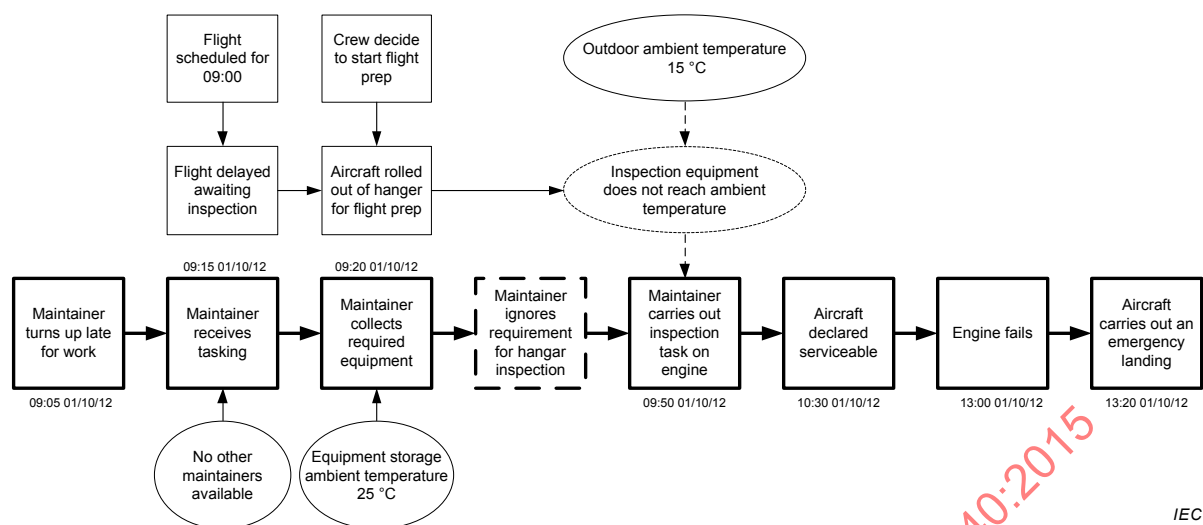


Figure C.1 – Example of an ECF chart

C.2.2 Process

The following describes the process for developing an ECF chart:

- Identify the focus event and record it in a box on the right hand side.
- Record the primary chain of events that led to the focus event where each event in the chain is both immediate and necessary to the event on the right hand side. Therefore, the consequence is recorded on the right hand side of each event (causal factor). Also, the consequence of a previous event may be the causal factor of the next event. The events are displayed in rectangles linked by arrows to the right of the focus event.
- Determine what conditions led to these events. State each of them in an oval above the relevant event.
- Add any secondary chains of events that may be relevant to the focus event and their conditions.
- Check the validity of the causal factors by obtaining evidence that determines whether the conditions and events are true.
- Develop the ECF chart until the event at the start of the sequence is identified and all conditions which can be verified by evidence are added.

In general, the exact chronology of events is not known at the beginning of the investigation but becomes clearer as the investigation proceeds. A method should therefore be used that allows investigators to easily change the sequence of events and conditions as more information is gained.

C.2.3 Strengths and limitations

The strengths of ECF are as follows:

- assists the verification of causal chains and event sequences;
- provides a structure for collecting, organizing and integrating evidence;
- identifies information gaps;
- assists communication by providing an effective visual aid that summarizes key information regarding the focus event and its causes.

The limitations of ECF are as follows:

- identifies some causal factors but may not necessarily determine the root causes;

- can be overcomplicated for simple problems.

C.3 Multilinear events sequencing (MES) and sequentially timed events plotting (STEP)

C.3.1 Overview

MES [10] and STEP [11] are methods developed to analyse focus events in complex systems, where STEP is a successor to MES.

As with ECF charting, MES/STEP conceives a focus event as arising from an interlinked succession of events with events characterized by a single subject and an active verb. In MES and STEP, the subject is called an actor (which may be a human, a machine or even a property).

Events are represented as event building blocks (BBs), which consist of (partial or full) data records as described in Figure C.2. These are arranged during the analysis in a time-actor matrix where the vertical axis of the matrix represents the different actors, and the horizontal axis represents time.

The time-actor matrix also contains:

- conditions necessary for enabling an event along with precursor events;
- annotations for further tasks in an investigation, such as a note indicating a deficit of information, or an incomplete explanation of an event.

An example showing part of the representation of a tank maintenance event is given in Figure C.3.

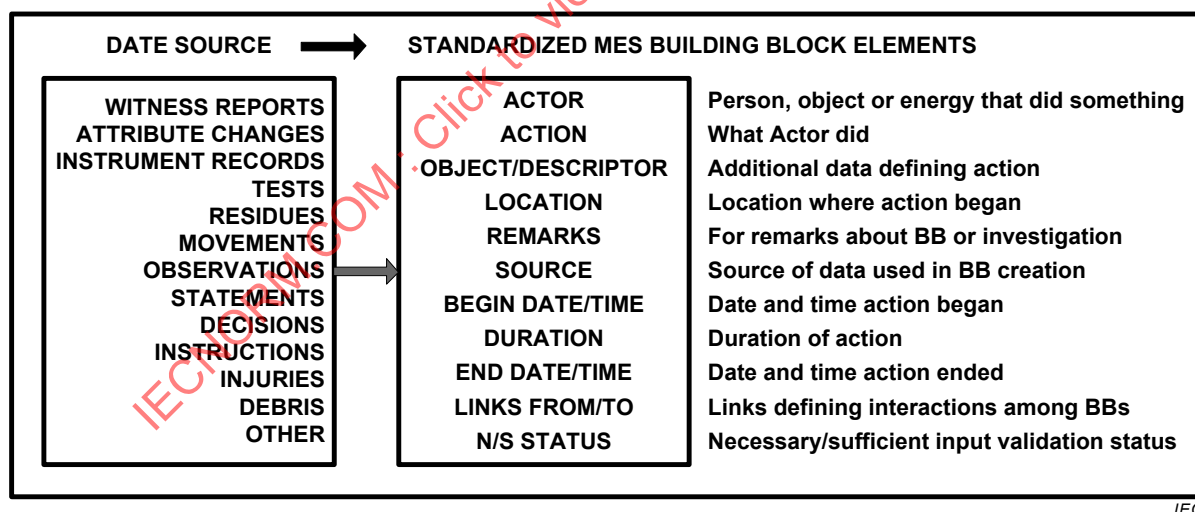


Figure C.2 – Data in an event building block

C.3.2 Process

MES/STEP has the following steps:

- Gather information for the initial series of building blocks, and identify and track missing information.
- Arrange the initial building blocks in an initial time-actor matrix.
- Identify and generate hypotheses to "fill" the gaps with events (in the form of further building blocks).

- d) Terminate the process when an analyst considers that sufficient information is available in the time-actor matrix.

C.3.3 Strengths and limitations

MES/STEP has the same strengths and limitations as ECF. Data formatting is relatively more elaborate, and there are explicit mechanisms for determining and tracking missing data and attempts to determine those data. Some such “bookkeeping” mechanisms are necessary for managing complex investigations with multiple investigators. The time-actor matrix also has explicit notation for recording the state of an on-going inquiry along with data-acquisition and explanatory tasks yet to be performed. This means that a comprehensible visual representation of the state of an investigation is available at all points in an investigation.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

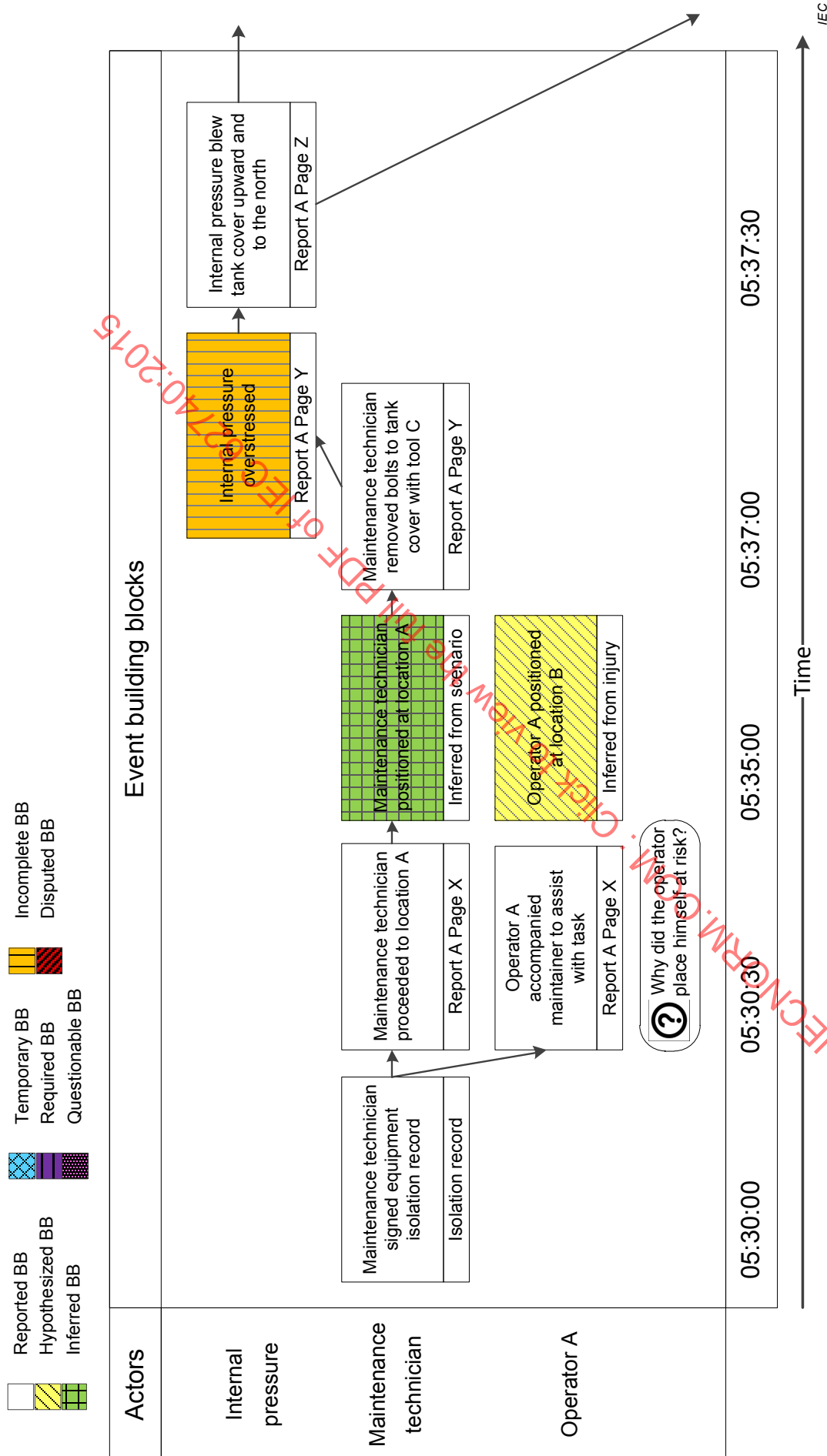


Figure C.3 – Example of a time-actor matrix

C.4 The 'why' method

C.4.1 Overview

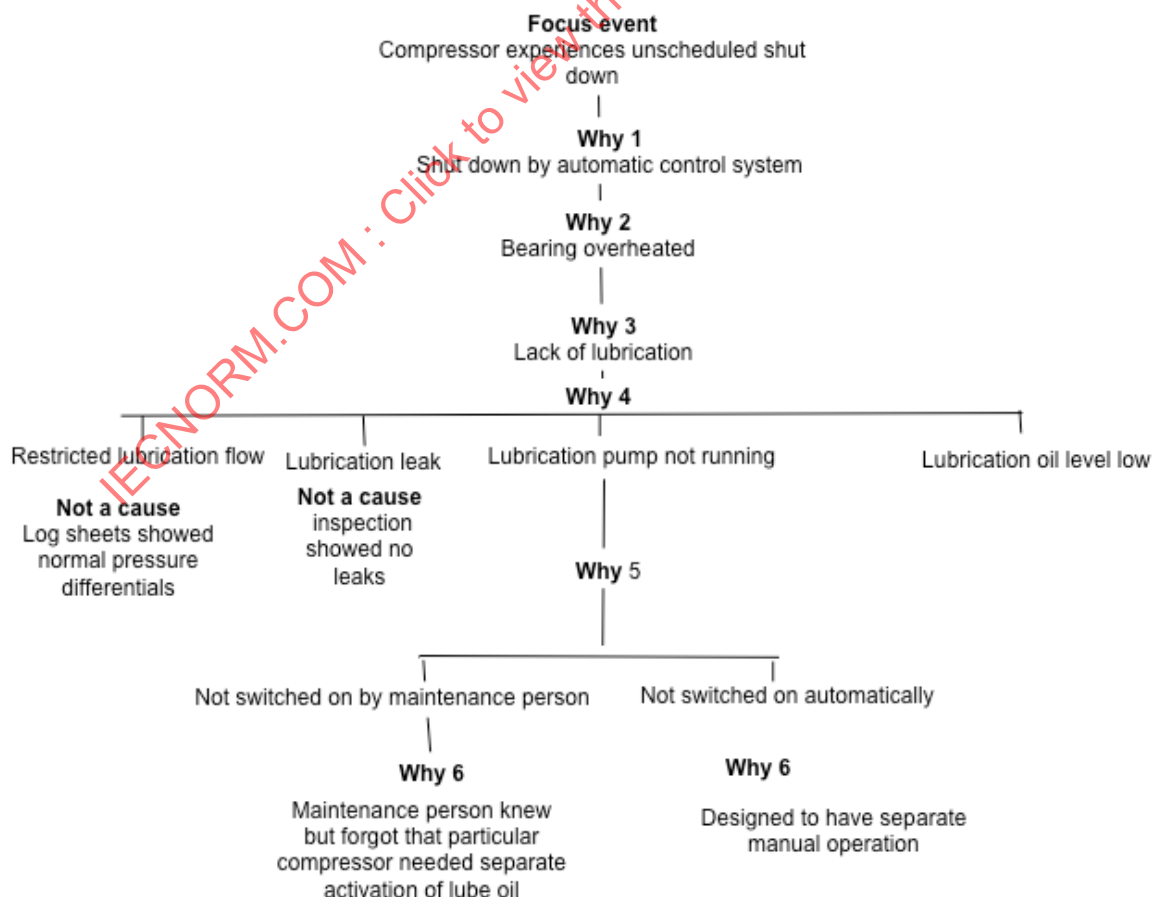
The 'why' method uses a straightforward questioning process to arrive at the root causes.

Questioning starts with a statement of the situation and asks why it occurred. The answer to this question is turned into a second why question and the answer to this into a third question. Questioning ceases when the stopping rule is reached. Generally this requires approximately 5 levels of questions hence the method is sometimes known as the 5 whys.

Where a why question provides several causal factors, each is explored and the method produces a why tree.

The why method is used alone for simple situations but is also inherent in more complex tree methods such as the causes tree method (CTM) (see Clause C.5). It can be useful for eliciting information from witnesses on how and why an event occurred because the simple question 'why' does not make assumptions about cause or lead the witness.

Figure C.4 illustrates an example of a compressor that has experienced an unscheduled shutdown. In the example the fourth why suggested a number of potential causal factors for lack of lubrication and evidence was sought to define which in fact occurred. Although a human error was involved in that a person did not follow specified start up procedures, the recommendation is to improve the design so the compressor and pump motors are linked. Further analysis of why the error occurred, in this case, is not useful.



IEC

Figure C.4 – Example of a why tree

C.4.2 Process

The 'why' method has the following steps:

- Identify and record the focus event as the start of a 'why' diagram.
- Ask why the focus event occurred, seeking only the immediate causal factors.
- Ask "why" successively with respect to the previous answer. In each case the answer to the question "why" should be an immediate causal factor of the previous answer.

The question 'why' is asked as many times as is needed to lead to a root cause, which is normally five questions but this is only a guideline. Each time the question is asked, there may be multiple answers and some analysis will be needed to eliminate those possible answers that are not applicable. It may be more effective to ask 'why did the process fail?' instead of just asking 'why'?

It can be useful to consider a set of categories of cause such as from the Ishikawa method and to involve a team of people. This will help ensure that all relevant areas are considered by the investigators.

C.4.3 Strengths and limitations

The strengths of the 'why' method are as follows:

- simple to apply by those involved in the problem;
- easy to understand by others;
- quick process to achieve results for simple problems;
- does not require extensive knowledge from the person asking the questions;
- does not require a lot of training from the person asking the questions.

The limitations of the 'why' method are as follows:

- only suitable for simple situations;
- heavily dependent on the knowledge and expertise of the people answering the questions, with expertise in both technical failure modes and human error often required to reach the root causes;
- root causes are likely to be missed if outside the knowledge base of those involved;
- possible uncertainty about when the appropriate root causes have been identified;
- can be developed to the level where reasons for people's actions are being considered, where evidence is often not available and results are therefore not always repeatable.

C.5 Causes tree method (CTM)

C.5.1 Overview

CTM [12] is a systematic technique for analysing and graphically depicting the events and conditions that contributed to a focus event.

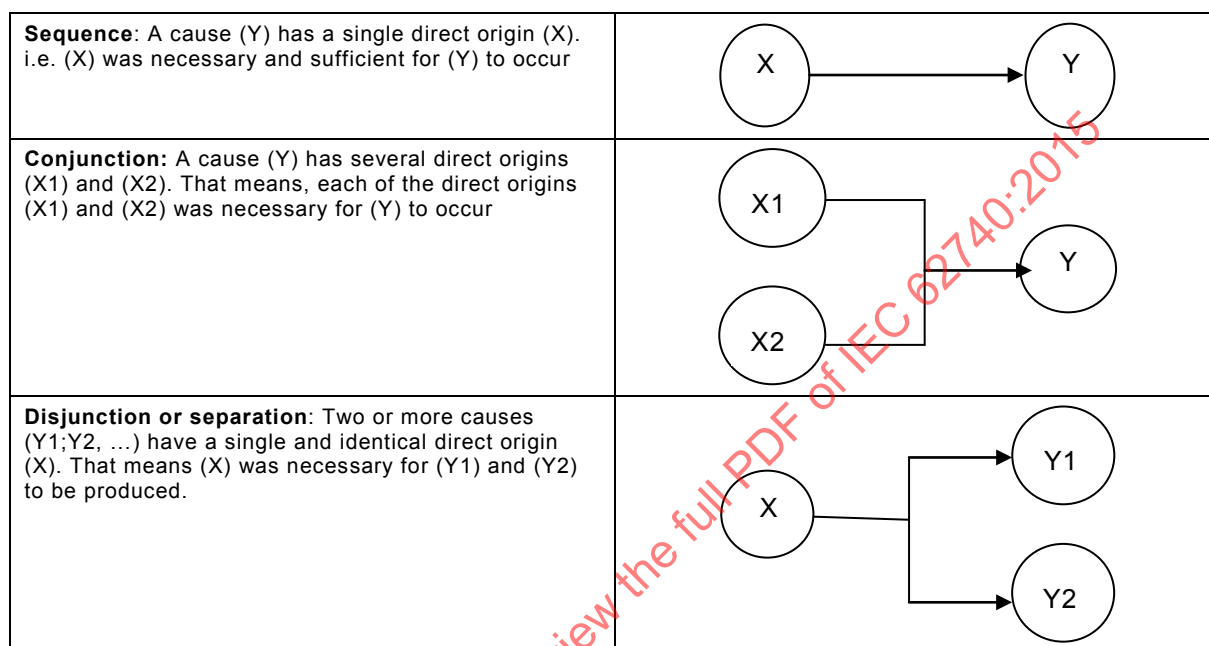
The method examines all the system components associated with the focus event. The investigation starts by establishing the tangible facts, taking care, in this phase, not to interpret them or to express an opinion about them.

CTM is similar to the why method in concept but builds a more complex tree and explicitly considers technical, organizational, human and environmental causal factors. Each antecedent (identified causal factor) is tested to check it is an immediate and necessary causal factor of the previous one, whereas the why method is less rigorous. Therefore, CTM is suitable for more complex situations.

CTM is also similar to a fault tree but, whereas a fault tree is used prior to an event to explore all possible causal factors and strict logic relationship(s) between faults are specified, the cause tree includes only those causal factors which apply to a specific event that has already occurred and does not develop the logical relationships in detail.

A cause tree may be used to explore successes as well as failures.

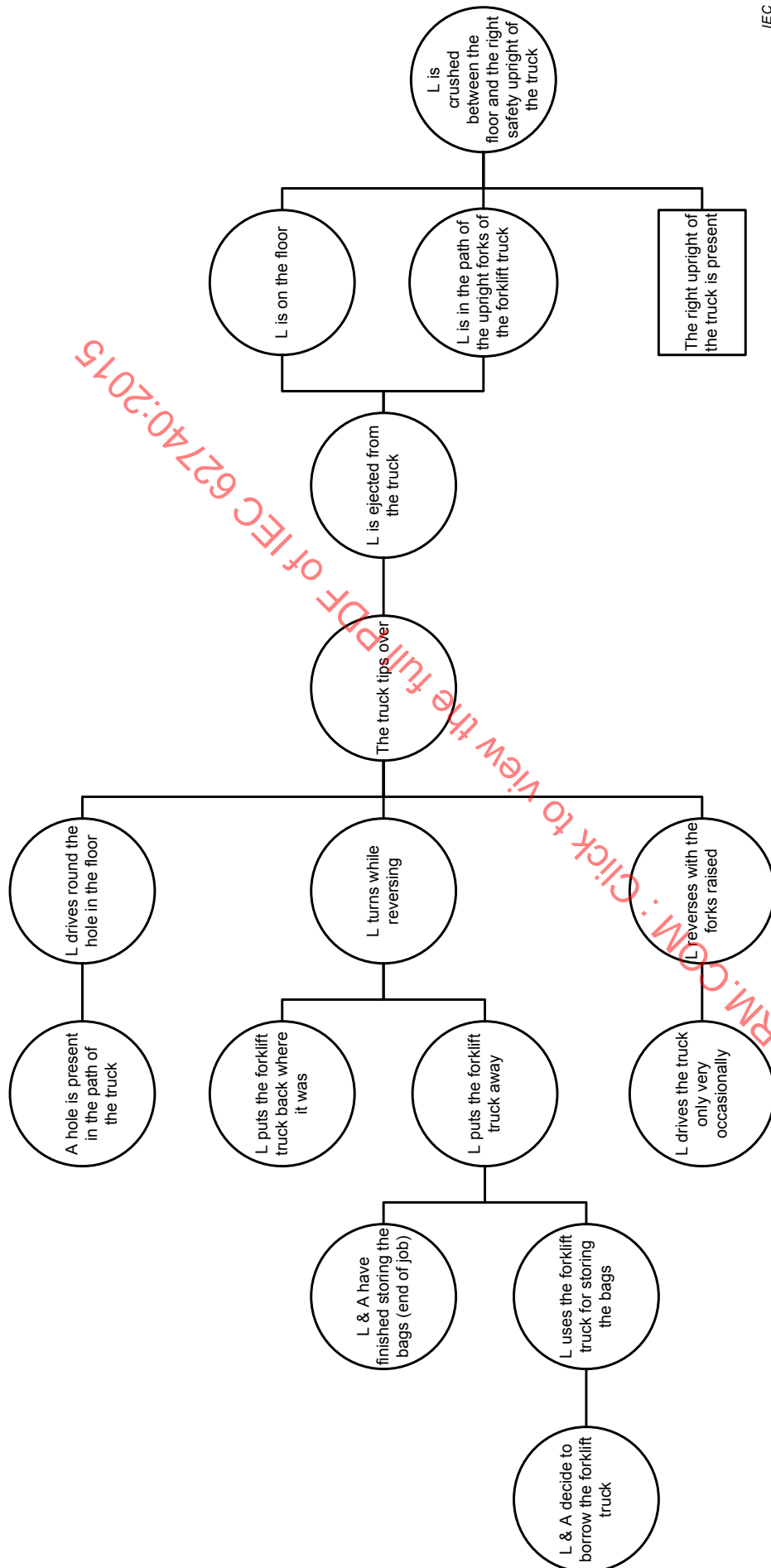
The cause tree forms a network of the causes which have directly or indirectly caused the focus event, using the three logical relations shown in Figure C.5.



IEC

Figure C.5 – Symbols and links used in CTM

Figure C.6 shows an example tree, in which Mr L (the victim) and Mr A are working nights, as an exception, to store a surplus of stock. In accordance with the handbook, Mr L and Mr A were required to load the crusher with "flour" which is then bagged and stored. Normally this activity is under the responsibility of a head of team whose presence had not been considered essential by the management for this night. Of his own initiative to save time, Mr L took a forklift truck (the ignition key had remained on the dashboard as usual) to store the bags. At the end of the task, Mr L set about returning the forklift truck. Mr L carried out a sharp bend in reverse, forks raised, and while seeking to avoid a hole on the ground the forklift tipped over, crushing Mr L between the ground and the right safety upright of the truck.



IEC

Figure C.6 – Example of a cause tree

C.5.2 Process

CTM has the following steps:

- a) Identify the focus event to be analysed and record it as the starting point for the tree.
- b) Collect and record all relevant data including people, their activities and actions, materials and equipment and factors relating to the physical and psychosocial environment.
- c) Make a list of the causal factors to the focus event. These should be supported by evidence and be expressed as precisely as possible. Subjective opinions and judgements are not included. Causal factors include those which are unusual or change the normal course of events and those which are normal but played an active part in the occurrence of the event.
- d) Work backwards towards the root causes by asking the following questions systematically for each antecedent that has been gathered:
 - 1) what antecedent X has directly caused the antecedent Y?;
 - 2) was X in itself necessary to give rise to Y?;
 - 3) If not, what are the other antecedents (X1, X2...) that were equally necessary in order to give rise directly to Y?
- e) Display these immediate necessary causal factors in a box linked by an arrow to the focus event. The tree may be drawn horizontally or vertically but is normally drawn horizontally starting from the right, so that left to right corresponds to the chronology of events.
- f) Continue asking the same questions with respect to each necessary causal factor found until the team agrees that there is no value in continuing further.
- g) Check the validity of the tree by obtaining further evidence that determines whether it is true.

C.5.3 Strengths and limitations

The strengths of CTM are as follows:

- provides a method for structuring investigation of complex events;
- facilitates easy to read format;
- can be used to encourage group participation;
- identifies areas for collecting data as the investigation proceeds;
- can be used to analyse success or failure events;
- can be used for technical and non-technical events.

The limitations of CTM are as follows:

- many human and organizational factors may contribute to the occurrence of the focus event and it is often difficult to establish which in a particular instance were the necessary causal factors;
- there is no guidance on how to seek causal factors; therefore, expertise in human error and organizational systems is needed when the tree involves human and organizational failures, where evidence is often difficult to obtain;
- it is difficult to apply when an event occurs as a result in a change of quality in several areas, where no single causal factor is a necessary causal factor.

C.6 Why-because analysis (WBA)

C.6.1 Overview

WBA [13] is a causal-analytical technique for establishing which of a given collection of events and situations are necessary causal factors. Given two events or situations, A and B

say, a condition called the counterfactual test (CT) is used to establish whether A is a necessary causal factor of B. Suppose two events or situations A and B have been observed. The CT asks whether, had A not occurred, B would also not have occurred. (Since A did occur, a supposition that A had not occurred is contrary to fact, hence the word “counterfactual”.) In asking this question, all other conditions are assumed to have remained the same. If the answer is yes: B would not have occurred then A is a necessary causal factor of B. If the answer is no: B could have happened anyway even if A had not happened (the CT fails) then A is not a necessary causal factor of B.

The network of causal factors is displayed as a Why-because graph (WBG), a collection of “nodes”, boxes, diamonds and other shapes, containing a brief description of the fact, joined by “edges”, or arrows, where the node at the tail of an arrow is a necessary causal factor of the node at its head, as determined by the CT.

A WBA is acyclic (contains no loops), so is usually drawn with arrows pointing in the generally upwards direction, as shown in Figure C.7, or horizontally with arrows pointing generally left-to-right, or right-to-left.

In order to determine whether sufficient causal factors are present in the collection of events and situations presented, the causal completeness test (CCT) is used. The CCT is applied to a given event or situation and its collection of necessary causal factors as determined by the CT. If the CCT is not passed, then the collection of events and situations has to be extended by further factors until it is passed. Suppose $A_1, A_2, \dots, A_n$ have been determined to be necessary causal factors of B by the CT. Then the CCT is deemed to be passed if, had B not occurred, one of $A_1, A_2, \dots, A_n$ would not have occurred either (formally, NOT-B is a necessary causal factor of NOT(A_1 AND A_2 AND...AND A_n) as determined by the CT).

When a WBG has been constructed and the CCT is passed for all the events and situations therein, then the WBG is complete and is deemed to represent a sufficient causal explanation of the focus event.

Figure C.7 illustrates an example of a WBG for a commercial-aviation runway-overrun accident.

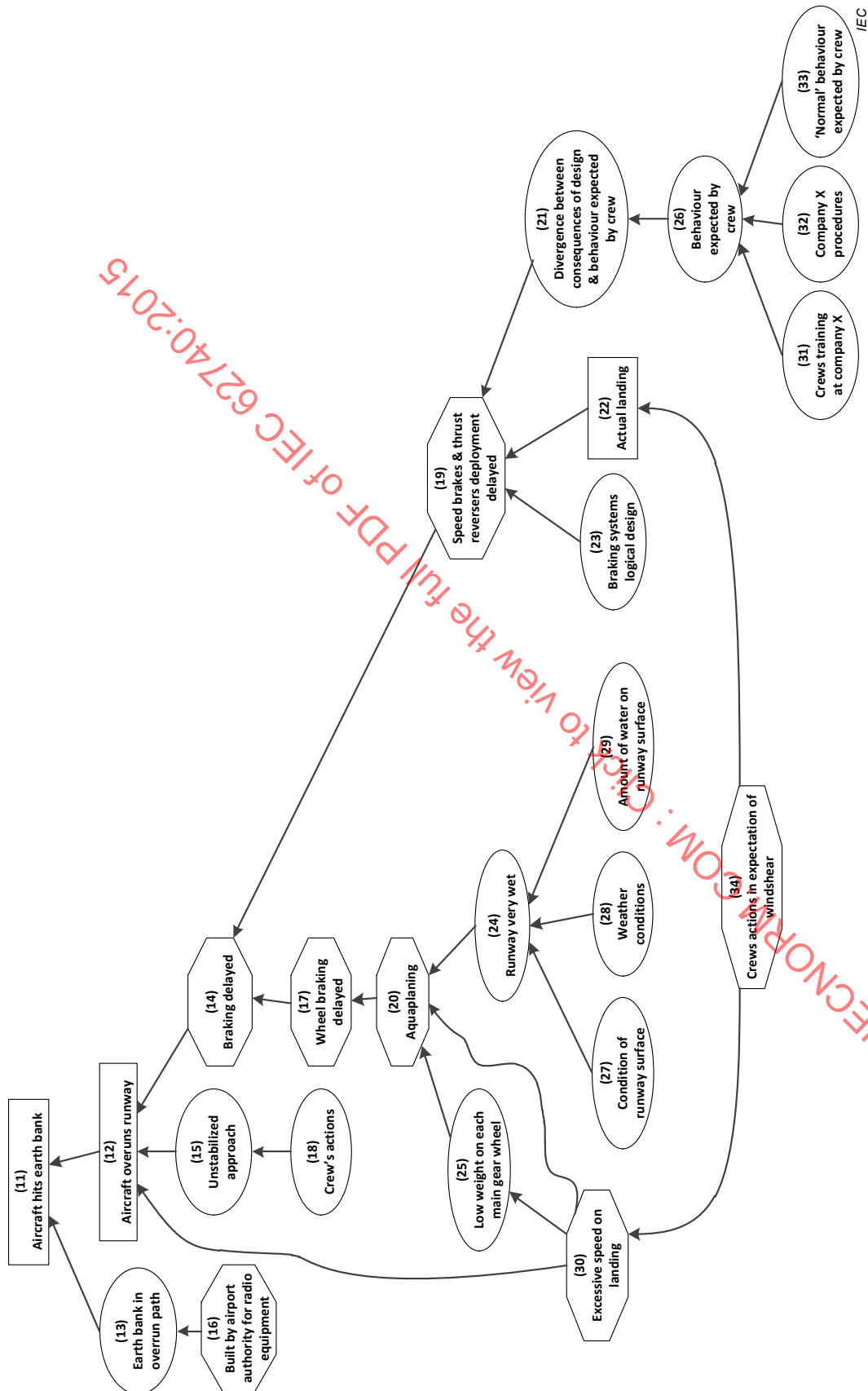


Figure C.7 – Example of a WBG

C.6.2 Process

WBA has the following steps:

- a) Determine a collection of facts deemed to be relevant, under guidance of a stopping rule. This gives an initial collection C of facts, divided into events, states and situations.
- b) Select the focus event (called in WBA the accident event).
- c) Determine intuitively the immediate necessary causal factors of the focus event from amongst the collection C; check using the CT. Display the results visually as a partial WBG.
- d) Determine intuitively the necessary causal factors of those immediate factors; check using the CT. Extend the WBG with these factors.
- e) Proceed to fill out the analysis (to extend the WBG) by testing each fact in C against the factors already in the WBG.
- f) Apply the CCT to determine whether the WBG is complete, or whether factors are missing from the collection C.
- g) Extend C if necessary; incorporate the new facts into the WBG using the CT. If insufficient information is available, assumptions may be included, providing they are clearly labelled as such.
- h) Finish when the CCT shows sufficient causal factors for each fact, in conformity with the stopping rule. If insufficient facts are available, assumptions have to be included in order to allow the CCT to succeed, but clearly labelled as such.

C.6.3 Strengths and limitations

The strengths of WBA are as follows:

- may be performed with a minimum of training (with the use of suitable tools that provide help on extracting facts from narrative descriptions, an inexperienced analyst can typically perform a first pass WBA inside two hours);
- the analysis results are easily understandable by third parties;
- the conceptual background required to perform a WBA is limited (an analyst must be able to apply the CT, and then the CCT);
- any network of causally-related phenomena may be analysed with a WBA;
- the reasoning behind a WBA may be formally checked using a formal logic;
- can be used together with other methods, e.g. those providing more structure to the collection of facts.

The limitations of WBA are as follows:

- the method provides no guidance on the collection of facts to which the tests are applied e.g. there is no structuring of facts into categories such as technical, procedural, human-factors, organizational and legal;
- because facts are not structured, WBA provides limited guidance on corrective action in the case where recurrence needs to be prevented.

C.7 Fault tree and success tree method

C.7.1 Overview

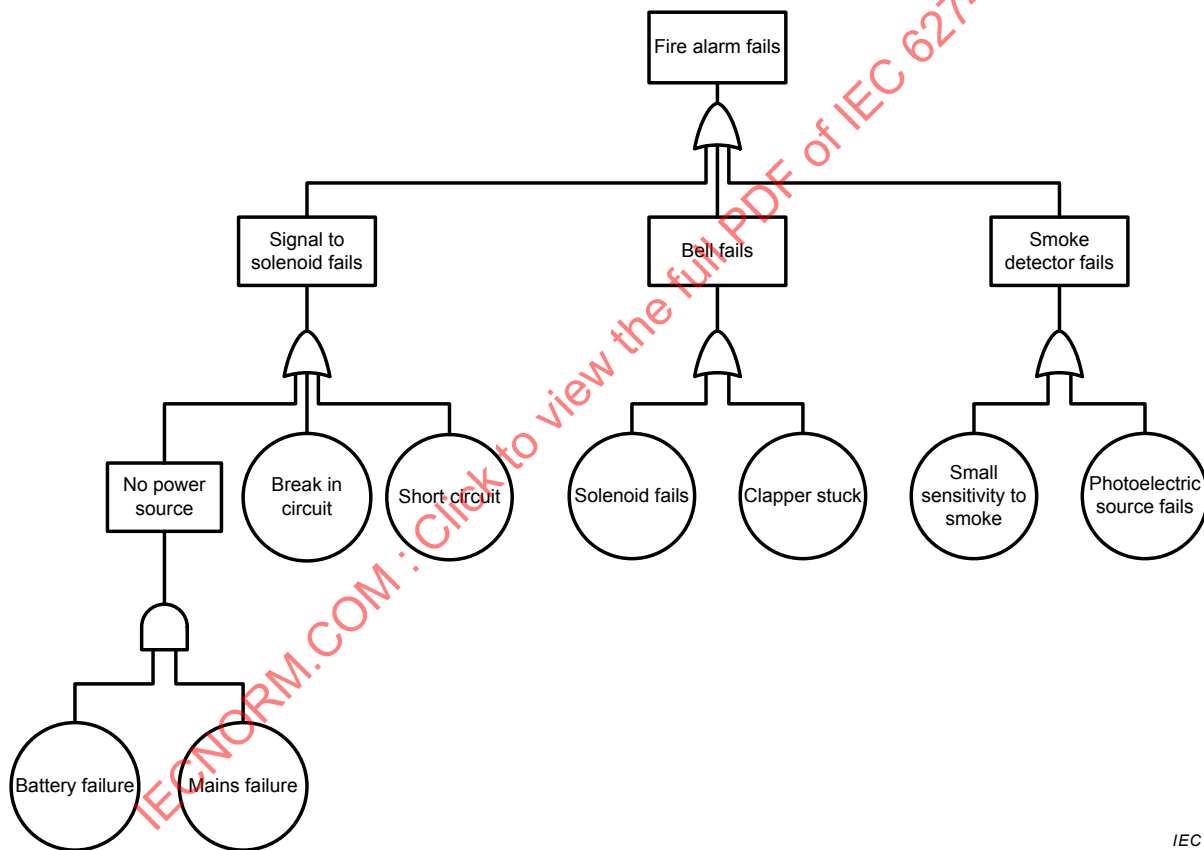
A fault tree [14] displays the immediate necessary causal factors of a focus event, their causal predecessors and the logic relationships between them. Fault tree analysis (FTA) [15] is normally used as a priori method of identifying and analysing potential failure modes, particularly of equipment. The fault tree diagram can be used in RCA by building a tree following the same logic but including in the tree only those events which actually occurred.

OR gates may be used during the analysis to describe alternative causal factors that need to be evaluated, but when all facts are clearly established only AND gates should remain, unless the purpose of the investigation is to prevent other related events. Therefore, as the investigation proceeds, potential causal factors that do not fit the evidence are gradually ruled out and removed from the tree. By closing out each branch of the tree, the causal factors of the focus event become apparent.

Strictly a fault tree represents binary events where a statement is true or false, e.g. a component failed or not. In RCA, the fault tree structure is often applied to a tree of causal factors where the logic rules are not strictly obeyed and changes in quality are included as well as binary events.

A similar logic can be applied where the focus event is a success. In this case the tree is referred to as a success tree.

Figure C.8 shows an example of a fault tree.



IEC

Figure C.8 – Example of a fault tree during the analysis

C.7.2 Process

The process for developing a fault/success tree is as follows:

- Define the focus event to be analysed and record it as the starting point for the tree.
- Establish the immediate necessary causal factors of the focus event and display them in a box linked by an arrow to the focus event. The tree may be drawn horizontally or vertically. These are the first level causal factors of the focus event.
- Establish the logic relationships between the immediate causal factors using AND and OR Gates. The events at inputs of an AND gate have to be both necessary and sufficient to

cause the event above. OR gates may be used during the analysis to describe potential causal factors that require investigation.

- d) Examine each causal factor to decide whether it is a root cause or the result of underlying causal factors.
- e) Validate potential causal factors and update the tree accordingly.
- f) Continue down the tree until the stopping rule is reached.

When the tree is developed, the possibility of causal factors relating to people, equipment and the environment is considered for each causal factor at each level. These should not be separated out at the top of the tree.

C.7.3 Strengths and limitations

The strengths of the fault/success tree method are as follows:

- provides a method for dividing up the analysis for large complex focus events;
- supported by many commercial software packages which assist in the development of the fault tree structure;
- encourages group participation;
- uses an orderly, easy-to-read format;
- identifies areas for collecting data.

The limitations of the fault/success tree method are as following:

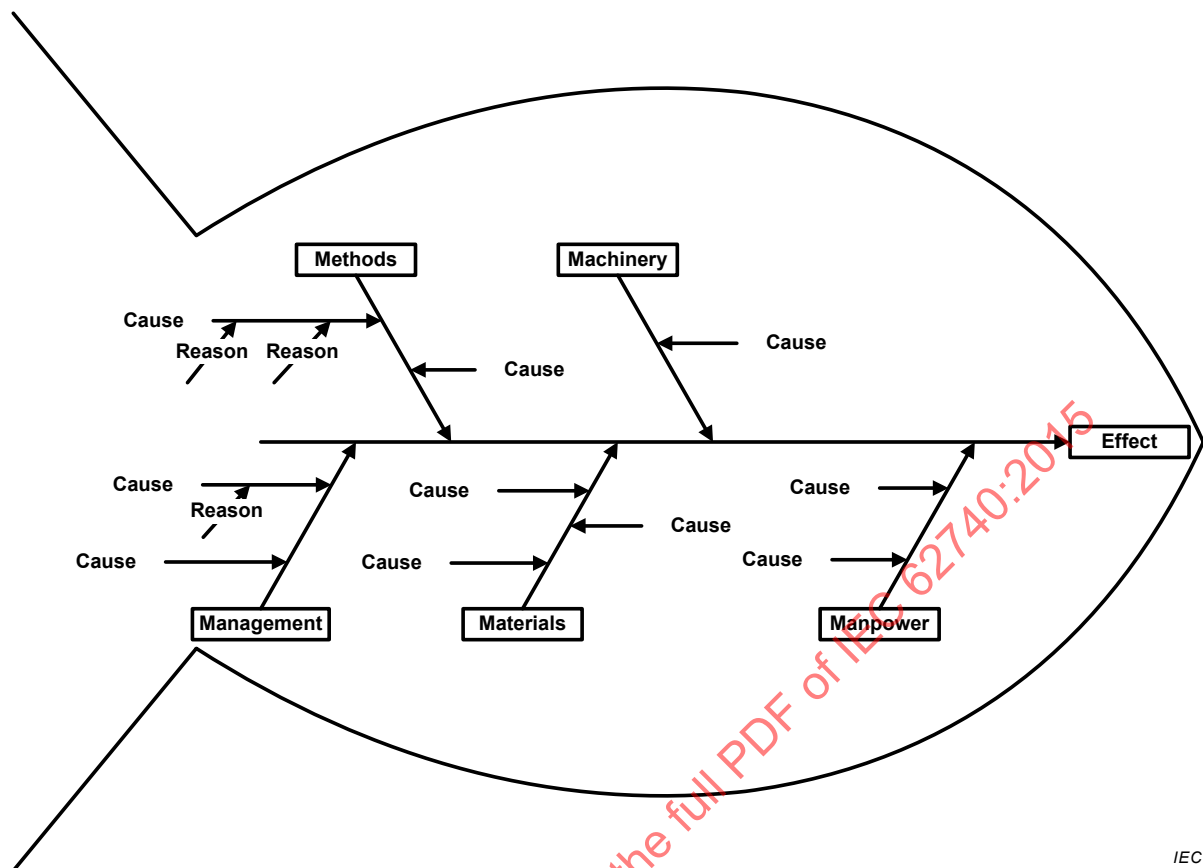
- requires an experienced practitioner;
- has no underlying model of causation and provides no guidance on how to seek causal factors;
- does not easily represent situations where an event occurs as a result of a general changing of quality that affects for example adherence to procedures or tolerances of physical components.

C.8 Fishbone or Ishikawa diagram

C.8.1 Overview

The Fishbone or Ishikawa diagram [16] is a technique that helps identify, analyse and present the possible causes of a focus event. It may be used to structure a brainstorming session and to suggest ideas where further evidence may be sought. The technique was invented by Kaoru Ishikawa and graphically illustrates the relationship between an event and all the factors that influence it. This technique is also referred to as a "fishbone diagram" because of its appearance.

Figure C.9 shows an example of a Fishbone or Ishikawa diagram.



IEC

Figure C.9 – Example of a Fishbone diagram

C.8.2 Process

The process for developing a Fishbone or Ishikawa diagram is as follows:

- a) Identify the focus event and record it on the right hand side and draw a line horizontally from it. This forms the head and spine of a fish.
- b) Establish the main categories of causes to be considered and draw lines off the spine to represent each category. Categories commonly used include:
 - 1) 5Ms: methods, machinery, management, materials, manpower;
 - 2) 4Ps: place, procedures, people, policies;
 - 3) 4Ss: surroundings, suppliers, systems, skills.
- c) For each category identify the possible causal factors of the focus event. These are presented as smaller lines coming off the 'bones' of the fish. Increasingly more detailed levels of causal factors can be shown as sub-branches coming off each cause line. It may be necessary to break the diagram into smaller diagrams if one branch has too many sub-branches.
- d) Analyse the diagram: The diagram now shows all the possible causal factors of the focus event. The final step is to investigate the most likely causal factors which tests whether the analysis is correct. Analysis includes:
 - 1) reviewing the "balance" of the diagram, checking for comparable levels of detail to identify the need for further identification of causal factors;
 - 2) identifying causal factors that appear repeatedly as these may represent root causes;
 - 3) assessing what can be measured in each cause in order to quantify the effects of any changes made;
 - 4) highlighting the causal factors whose action can be taken.

C.8.3 Strengths and limitations

The strengths of the Fishbone or Ishikawa diagram are as follows:

- encourages group participation to identify people's perceptions of causal factors;
- seeks causal factors under a set of categories, so will identify a range of causal factors relating to human and organizational factors as well as hardware and procedural factors;
- uses an orderly, easy-to-read format;
- indicates possible causal factors of variation;
- can be used for simple investigations or as part of a more complex investigation.

The limitations of the Fishbone or Ishikawa diagram are as follows:

- there is no underlying model or theory of causation, so the causal factors identified are based on the team's perceptions.

C.9 Safety through organizational learning (SOL)

C.9.1 Overview

SOL [17] is an event analysis technique, which seeks weaknesses in the complex socio-technical system in which the event occurred. The purpose of SOL is to provide a model of the system and identify its weaknesses so it can be improved and recurrence of the focus event prevented. The emphasis is on organizational learning.

C.9.2 Process

SOL has the following steps:

- 1) Describe the situation using a time-actor matrix produced by MES/STEP (see Clause C.3).
- 2) Identify causal factors (which may be direct or indirect see Table C.1) for each event in the time-actor matrix, guided by checklists of questions derived from the experience and research of SOL authors. Direct causal factors are those that immediately resulted in the focus event, indirect causal factors appear further down the causal chain but may involve the same issues.
- 3) Classify causal factors into technology, individuals, working group, organization, and organizational environment.

Table C.1 – Direct and indirect causal factors

Direct causal factors	Indirect causal factors
Information	Information
Communication	Communication
Working conditions	Working conditions
Personal performance	Personal performance
Violations	Violations
Technical components	Scheduling
	Responsibility
	Control and supervision
	Group influence
	Rules, procedures and documents
	Qualifications
	Training
	Organization and management
	Safety principles
	Quality management
	Maintenance
	Regulatory and consulting bodies
	Environmental influences

C.9.3 Strengths and limitations

The strengths of SOL are as follows:

- the check list format allows users who are not specialists in organizational systems or organizational psychology to produce useful analyses;
- the emphasis on causal factors rather than necessary causal factors allows more factors to be brought into consideration than a narrowly causal analysis might do, and thereby offers more chance of identifying possible improvements;
- the format of the event building blocks gives less scope to the judgement of individual analysts and helps to give uniformity to SOL analyses;
- the stopping rule is implicitly defined by the checklist questions: when these have been answered, the information is deemed to be adequate.

The limitations of SOL are as follows:

- there is no specific notion of what is a causal factor other than what is implicit in the checklist questions;
- the level of detail is driven by the predetermined checklist of questions rather than the perceived need;
- the check list of questions was derived from research in the nuclear power industry and may be less suitable for other industries.

C.10 Management oversight and risk tree (MORT)

C.10.1 Overview

MORT [18] was first developed for analysing the root causes and causal factors for incidents in the nuclear power and aviation industries in the USA, but now has been applied in many industries.

MORT is a pre-populated tree based on a model of an organization's management system, which effectively provides a detailed check list for reviewing which parts of management and control systems were less than adequate when the focus event occurred. The basic structure of the tree is shown in Figure C.10.

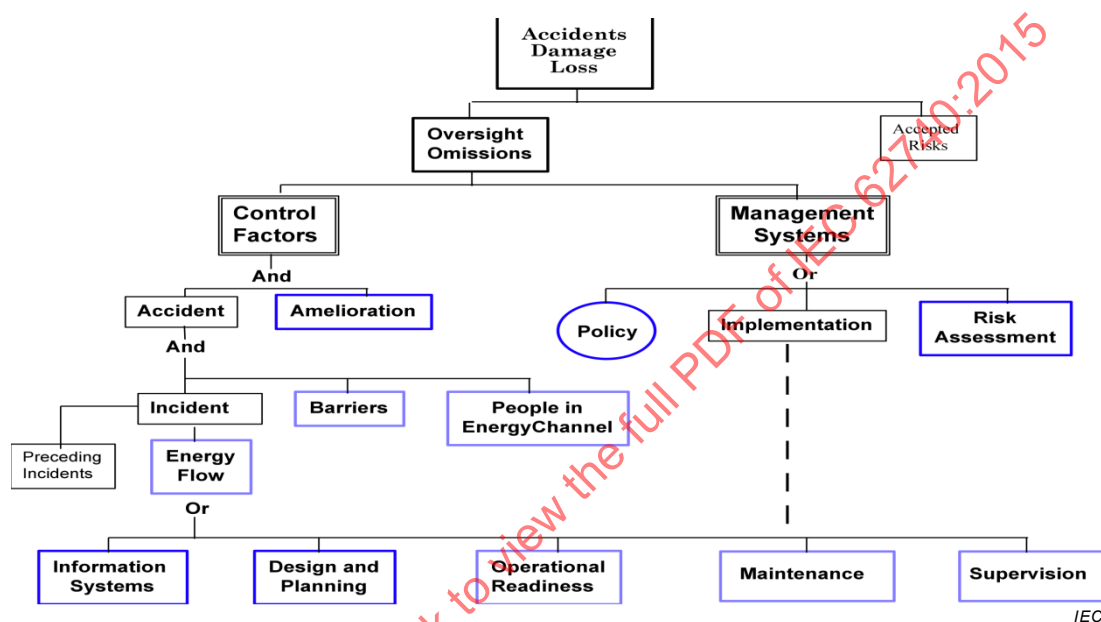


Figure C.10 – Example of a MORT diagram

MORT assumes that a failure occurs as a result of oversights or omissions in either management systems or the specific control factors which should have prevented the focus event from occurring.

Ultimately, failures in either branch in the tree occur because something within the general management systems (information systems, design and planning, operational readiness, maintenance or supervision) was less than adequate. Each box in Figure C.10 is developed into a detailed tree structure showing factors that might have been less than adequate.

C.10.2 Process

Start with the focus event and then work down the MORT tree in a logical manner asking and responding to pre-questions in the MORT manual. Symbols on the MORT chart are colour coded to indicate:

- there is no problem with an element (adequate);
- the element is giving rise to a problem (less than adequate);
- there is need for further enquiries.

C.10.3 Strengths and limitations

The strengths of MORT are as follows:

- provides comprehensive guidance for seeking all possible aspects of the system that were not adequate at the time of the focus event;
- less specialist expertise is needed than in some techniques because detailed guidance is provided on possible causal factors;
- identifies weaknesses in the system which might apply across a wide range of failure scenarios.

The limitations of MORT are as follows:

- explores weaknesses in the system in general that might have played a role in the focus event rather than seeking immediate or necessary causal factors;
- a very large number of questions (around 1 500) are asked, so the method is time consuming and hence most appropriate for serious events;
- unless the organization to which it is applied is a high reliability organization a very large number of weaknesses are found which make it difficult to implement changes;
- tedious when first learning or applying the method.

C.11 AcciMaps

C.11.1 Overview

AcciMaps [19] is based on concepts of causation published by Rasmussen and Svedung [20] and the organizational systems model (see Clause B.4).

AcciMaps is a graphical representation used to structure the analysis of a focus event and to identify the interactions in the socio-technical system in which the focus event occurred. It is a method designed to reveal the system wide failures, decisions and actions involved in a focus event. These are arranged in layers representing the different levels in a socio-technical system from government down to the equipment and surroundings involved. It also looks at the individual actors at each level and their decision-making routines and competence.

An example AcciMap for a gas explosion, showing typical system levels, is given in Figure C.11. The bottom level represents the physical arrangement of the scene of the focus event (buildings, equipment, surroundings, etc.). The next level up is the sequence of events leading to the focus event including the failures, actions and decisions (including normal actions and decisions) that played a part. The higher levels show decisions and actions at each level that influenced, or could have influenced, the sequence of events at the lower levels.

C.11.2 Process

An AcciMaps is developed as follows:

- a) Define a model of the system with different organizational levels.
- b) Populate the levels (using boxes (nodes)) with the decisions and actions relevant to the focus event, the conditions that lead to them and their consequences.
- c) Draw arrows that show all linkages and influences.
- d) A process such as WBA may be added to ascertain which of the identified issues were necessary causal factors of the focus event.

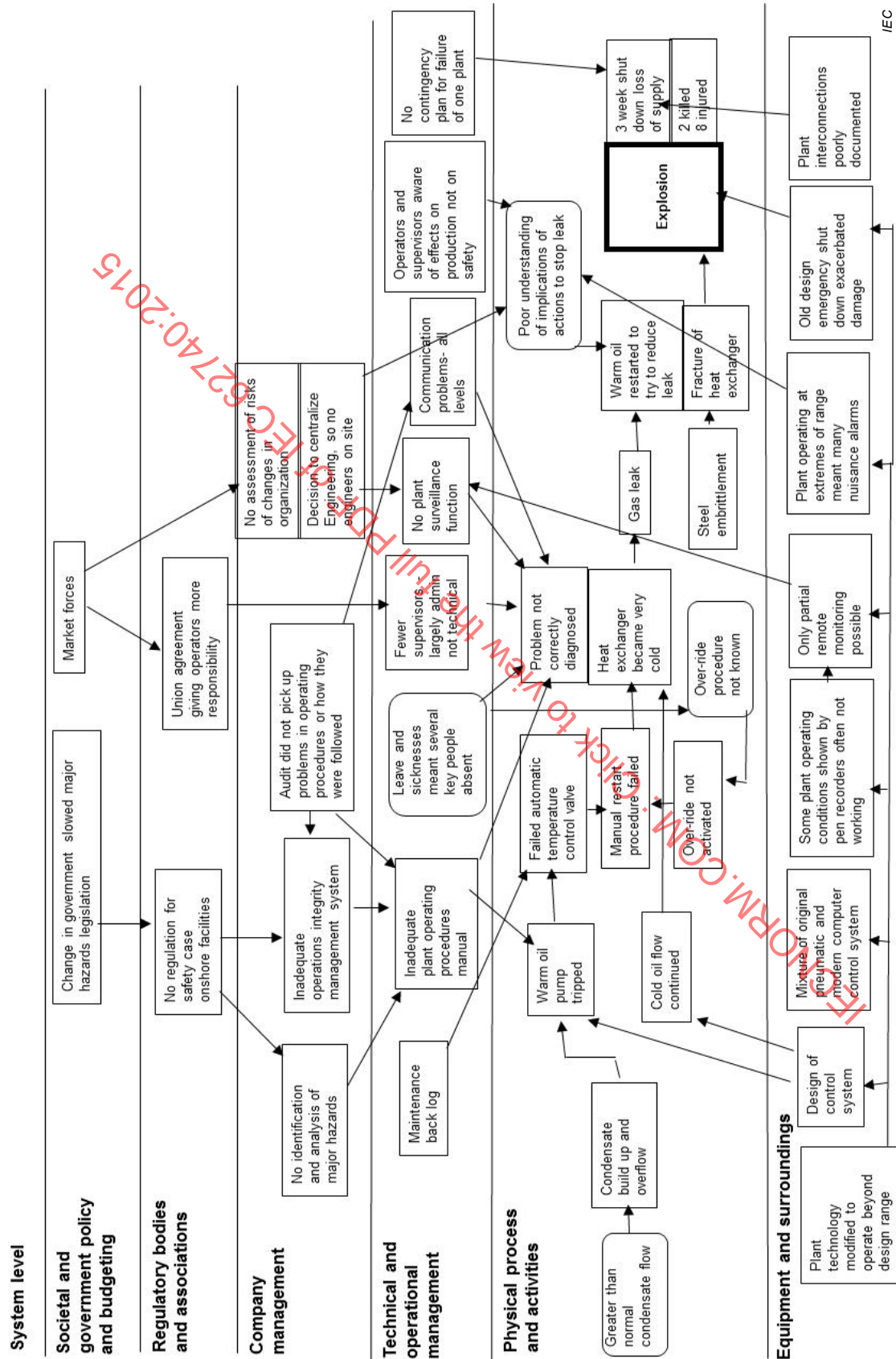


Figure C.11 – Example of an AcciMap

C.11.3 Strengths and limitations

The strengths of AcciMaps are as follows:

- as there is no taxonomy or guidance, AcciMaps has the potential to be highly comprehensive in identifying causal factors across all levels of the system;
- the linkages within and between levels helps ensure that failures are considered in the context of the things that influenced them;
- human error has equal focus with equipment and higher level organizational factors;
- personal factors which influence decisions, particularly at the lower levels, are not included.

The limitations of AcciMaps are as follows:

- the lack of a taxonomy means that the factors identified are based on the team's perception;
- the organizational model comes from outside the analysis and there is no criterion to ensure it is adequate;
- the result of the AcciMaps analysis is lightly constrained, therefore it is possible to derive different AcciMaps for the same focus event;
- with no specific taxonomy it is difficult to aggregate multiple analyses to find common factors;
- the generality of factors in the nodes is often high and can be very abstract. This makes it difficult to derive precise actions;
- it has a weak analytical approach to physical and equipment failures;
- it does not represent the results of a causal analysis by itself.

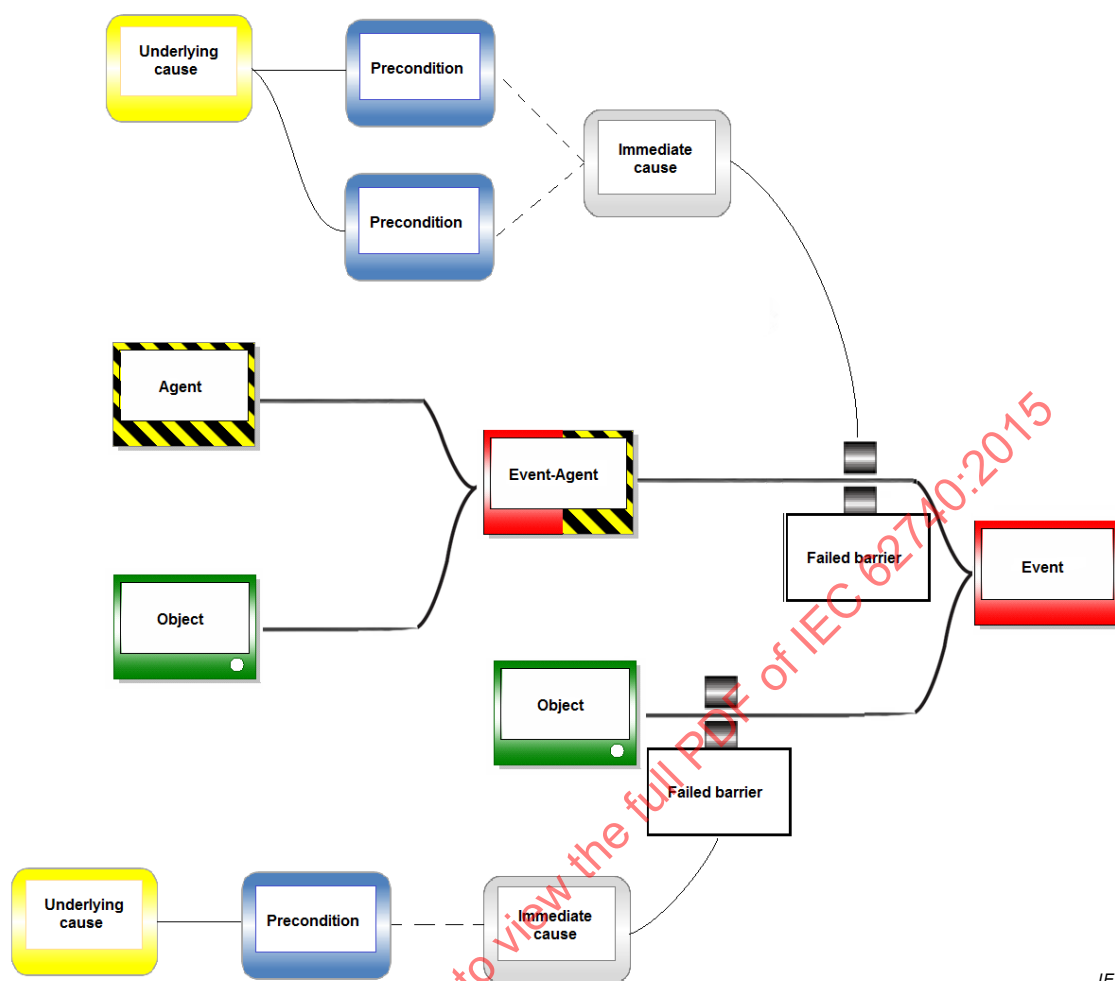
C.12 Tripod Beta

C.12.1 Overview

Tripod Beta [21] is an incident investigation and analysis methodology which combines the ideas from Reason's model (see Clause B.3) and Barrier Analysis (see Clause B.2), along with Rasmussen's generic error modelling system (GEMS) and Wagenaar's Tripod causation path. It describes incidents in terms of 'objects', e.g. people, equipment, etc. being changed by 'agents of change', e.g. anything with the potential to change an object. It also models 'barriers', showing them, for example, as effective, failed or inadequate.

Tripod Beta provides a format and rules for modelling the events (focus event and the events leading up to, and after, the focus event) and linking each element together, working back ultimately to the underlying causes. A number of software packages have been developed based on these rules, but it can be used with or without software. The software-based techniques contain checklists derived from the models and from analysis of past events mostly in the off shore oil industry.

The core of a Tripod analysis is a 'tree' diagram representation of the causal network (see Figure C.12) which describes the focus event as a network of events and their relationships.



IEC

Figure C.12 – Example of a Tripod Beta tree diagram

C.12.2 Process

The process for developing the Tripod Beta tree diagram is to identify the following:

- The agent (hazard or hazards) that lead to the focus event and the target that was harmed.
- Controls or barriers, that were missing or failed, that could have prevented the event or protected the target.
- Immediate causes – the human act, which resulted in the failed barrier. These are failures or errors that have immediate effect and occur at the point of contact between a human and a system (e.g. pushing an incorrect button, ignoring a warning light).
- Preconditions – psychological and situational precursors e.g. the type of human failure (slip, lapse, violation, etc.).
- Underlying causes (latent failures) in the organization, i.e. inadequacies in the management system, culture, etc. These can be categorized into pre-defined 'basic risk factors', derived from brainstorming and research into results of audits and accident investigations in the off shore oil industry.

C.12.3 Strengths and limitations

The strengths of the Tripod methodology are as follows:

- provides a map of the focus event and its causal factors;
- can help direct the investigation and define its scope;

- defines the barriers in the system;
- based on scientific research including a model of human behaviour to uncover what is behind the observed behaviour;
- leads the investigator to consider the reasons behind the immediate causes and human error;
- menu driven software is available.

The limitations of the Tripod methodology are as follows:

- can be resource intensive;
- leads to system level underlying causes which an organization might not be able to accept;
- use of the basic risk factors to categorize underlying causes can be too generic and simplistic;
- conclusions do not lead to simple remedial actions;
- extensive training is generally required.

C.13 Causal analysis using STAMP (CAST)

C.13.1 Overview

CAST [7] is a technique that examines the entire socio-technical process involved in a focus event. CAST is based on STAMP (see Clause B.5), which is used to guide the causal analysis. CAST documents the dynamic process leading to the focus event, including the socio-technical control structure as well as the constraints that were violated at each level of the control structure and why. The analysis results in multiple views of the focus event, depending on the perspective and level from which the focus event is being viewed.

To illustrate CAST, consider a focus event involving the contamination of a public water supply with *E. coli* in a small town in Canada. Figure C.13 shows the safety control structure for the water supply of the town. There are three physical systems being controlled: the well system, the water supply and public health. Each component in the structure controlling these processes has specific safety-related responsibilities. For example, the Ministry of the Environment provides oversight and control of the local water systems. Each component of the control structure gets feedback about the state of the process it is controlling. One common cause is that the controller gets incorrect feedback and thinks the state of the controlled process is different than it is. For example, budgets were cut and the Ministry of the Interior reduced the number of inspections and inspectors.

Figure C.14 shows the analysis of the role of the local health department in the focus event, including the roles and responsibilities, the unsafe control actions, the context in which the unsafe control actions were provided, and the flaws in the process (mental) model that contributed to the behaviour. Figure C.15 shows the same thing for another component of the control structure, the water system operations management.

In a full analysis, each component of the control structure would be considered with respect to their contribution to the focus event. In most focus events, contributions can be found from every component of the control structure.

Other features of the analysis (not shown) include examining the dynamic changes over time in the system that contributed to the focus event and the role of flawed communication and coordination.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

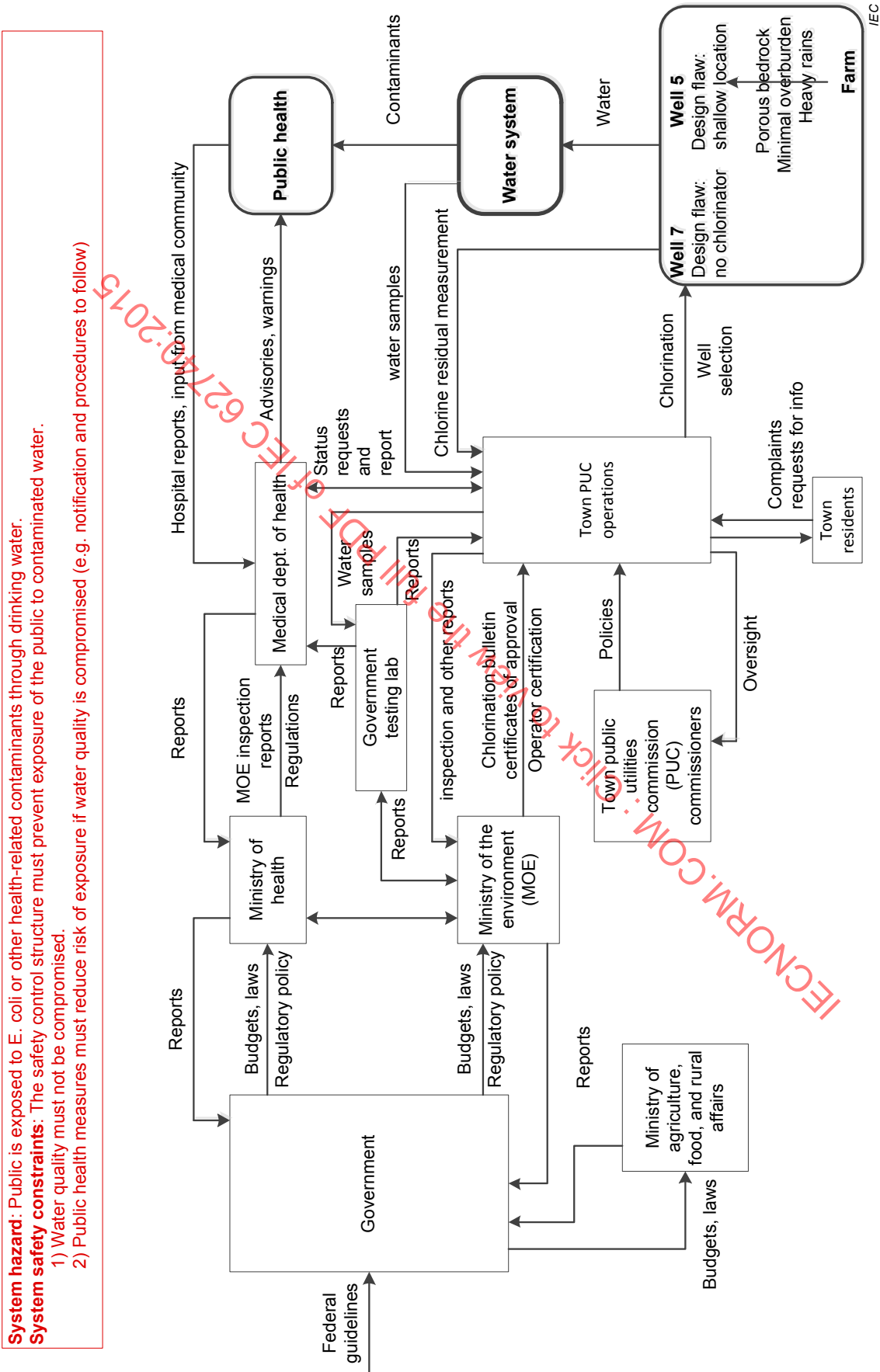


Figure C.13 – Control structure for the water supply in a small town in Canada

Medical department of health	
Safety requirements and constraints: • Provide oversight of drinking water quality • Follow up on adverse drinking water quality reports • Issue boil water and other advisories if public health at risk	Mental model flaws: • Thought adverse water quality reports were being received • Unaware of reports of E. coli linked to treated water • Thought Mr K was relaying the truth • Unaware of poor state of local water operations
Context in which decision made: • Most recent water quality reports over 2 years old • Illness surfacing in communities outside the town • E. coli most commonly spread through meat	Coordination • Assumed the ministry of environment was ensuring inspection report problems were resolved
Inadequate control actions: • Advisory delayed • Advisory should have been more widely disseminated • Public health inspector did not follow up on 1998 inspection report	

Figure C.14 – Example CAST causal analysis for the local Department of health

Town PUC operations management	
Safety requirements and constraints: • Monitor operations to ensure that sample taking and reporting is carried out • Keep accurate records • Update knowledge as required	Mental model flaws: • Believed sources for water system were generally safe • Thought untreated water was safe to drink • Did not understand health risks posed by under chlorinated water • Did not understand risks of bacterial contaminants like E. coli • Did not believe guidelines were a high priority
Context in which decision made: • Complaints by citizens about chlorine taste in drinking water • Improper activities were an established practice for 20 years • Lacked adequate training and expertise	
Inadequate control actions: • Inadequate monitoring and supervision of operations • Adverse test results not reported when asked • Problems discovered during inspections not rectified • Inadequate response after first symptoms in community • Did not maintain proper training or operations records	

Figure C.15 – Example CAST causal analysis for the local public utility operations management

C.13.2 Process

CAST has the following steps:

- Identify the system(s) involved in the focus event.
- Identify the system constraints associated with the focus event.
- Document the control structure in place. This structure includes the roles and responsibilities of each component in the structure as well as the controls provided or created to execute their responsibilities and the relevant feedback (if any) provided to help them do this.

- d) Determine the proximate events leading to the focus event.
- e) Analyse the focus event at the physical system level. Identify the contribution of each of the following to the events: physical and operational controls, physical failures, dysfunctional interactions, communication and coordination flaws, and unhandled disturbances. Determine why the physical controls in place were ineffective.
- f) Moving up the levels of the control structure, determine, as follows, how and why each successive higher level allowed or contributed to the inadequate control at the current level.
 - 1) For each system constraint, either the responsibility for enforcing it was never assigned to a component in the control structure or a component(s) did not exercise adequate control to ensure their assigned responsibilities were enforced in the components below them.
 - 2) Identify unsafe decisions or control actions, including actions provided by software, operators, managers, regulators, etc.
 - 3) Any human decisions or flawed control actions need to be understood in terms of the information available to the decision maker as well as any information that was not available, the behaviour shaping mechanisms (the context and influences on the decision making process), the value structures underlying the decision, and any flaws in the process models (mental models) of those making the decisions and why those flaws existed.
- g) Examine the overall coordination and communication (including missing feedback) that contributed to the focus event.

Although the process is described in terms of steps, the process need not be linear nor does one step need to be completed before the next one is started.

C.13.3 Strengths and limitations

The strengths of CAST are as follows:

- looks back through time to determine how the system evolved to a state of high risk;
- identifies the social and managerial factors and not just the human operations or technical system failures;
- does not impose any particular social theory on the analysis, any model of social behaviour could be used to generate the analysis results.

The limitations of CAST are as follows:

- it is not possible to graphically present the analysis, as the inclusion of indirect relationships between causal factors means that circles and arrows (which depict direct relationships) are not adequate to describe all the causal factors;
- may require more resources and time to fully understand the focus event than other methods with a more limited focus.

Annex D (informative)

Useful tools to assist root cause analysis (RCA)

D.1 General

Annex D describes tools and techniques that can support the conduct of RCA.

D.2 Data mining and clustering techniques

D.2.1 Overview

Modern data mining techniques enable a search for specific properties and conditions. Clustering analysis selects data that are closely related, and thereby identify deviating data (outliers). Modern cluster analysis can detect data that are closely related in one, two or more dimensions and thereby analyse products or processes that are closely related and identify deviating data points (outliers).

In RCA, data mining and clustering analysis can give valuable clues and help to confirm or reject potential root causes. In some cases, e.g. aerospace and medical equipment, it is required to store batch numbers for the finished products and the associated component batch numbers and raw material batch numbers. This information can provide a useful structure for identifying correlations which hint at possible causal relations.

D.2.2 Example 1

A company observes 12 % failures of stocked items. Analysis shows that a plastic part is broken. The start of the 12 % failure pattern is identified as a batch number and a manufacturing date. This date is correlated with delivered batches of the plastic parts. There is no correlation. There is no correlation either with the batches of plastic raw materials. However, there is a correlation with the batches of a spring that load the plastic part. The problem started 3 days after a new batch of springs was received. The changes that were made between the two batches of springs is investigated. The difference is a new surface treatment against corrosion. This surface treatment process is investigated and contains a note that this treatment may interfere with certain plastic materials. Further analysis shows that the corrosion protection accelerates crack propagation in this plastic. Analysis of the data sheet for the plastic material shows a warning against local overload that may cause cracks. The conclusion therefore is that a causal hypothesis can be formulated: that a plastic part is continuously overloaded and undergoes fracture through local overload, and the fractures propagate in a manner accelerated by the new anti-corrosion treatment of the springs. These cracks then propagate in an accelerated manner due to the new anti-corrosion treatment of the springs. A failure analysis has previously shown a pattern on the fracture surface consisting of crack propagation lines originating in the points of contact with the spring and a brittle surface from the final fracture. The causal-explanatory hypothesis may be confirmed at a given level of confidence by experiment: setting up a number of plastic parts with and without the new treatment. If it is observed that plastic parts with the new treatment predominantly fail, one may conclude that the causal hypothesis is confirmed to the appropriate degree of confidence using standard methods of statistical inference.

D.2.3 Example 2

A number of soldering failures is observed in the field. The manufacturing weeks for the failed products are plotted in calendar time. It is observed that the manufacturing dates of the products with soldering failures are clustering in certain weeks. A causal hypothesis may be formulated on the basis of the initial observation, which is then confirmed to a given degree of confidence using standard statistical inference on the process-control data from

manufacturing, which indicate that the soldering process in these weeks was likely not performed under appropriate control. The conclusion is, to a high level of confidence, that a root cause of the soldering failures is insufficient process control of the solder process.

D.2.4 Example 3

A component is tested on a test board by twisting the board. The number of twists to failure is plotted on a Weibull plot (see IEC 61649 [22]). The analysis identifies a "weak" and a "strong" population (see IEC 61163-1 [23]). One component from the weak and one component from the strong population is analysed by cross-sectioning of the micro ball grid array (BGA) solder balls. It is noted that the component from the weak population has a large number of large voids in the solder balls, while the solder balls from the strong population have no or few small voids. It is concluded that a root-causal hypothesis is formulated, that voids in the solder balls of the micro BGA are a root cause of the incident events. The root-causal hypothesis is confirmed by collecting data on operational use and observing through analysis of the data that the reduction in voids correlates with successful use of the component.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

Annex E (informative)

Analysis of human performance

E.1 General

People at any level in an organization make decisions or perform or omit actions which may play a part in the events leading to a focus event. Human performance may be above or below expectation and the impact may be positive or negative. Decisions can be correct in the circumstances in which they were made but turn out to have unintended results.

People may make errors, be misguided or misinformed, be inappropriately motivated, may be trying to perform correctly or may knowingly violate rules. Analysis of human aspects of causation is complex and generally requires specialist expertise if it is required to go beyond identifying what occurred to seeking why and hence making recommendations.

E.2 Analysis of human failure

Analysis of human failures starts by identifying the error mode. This is the external manifestation of the error, i.e. what is observed to have been done (or not done). Examples of error modes are as follows:

- omitted;
- too early;
- too late;
- too much;
- too little;
- wrong direction;
- wrong object;
- wrong action;
- wrong sequence.

There are then a number of different taxonomies for categorizing and analysing causes of these errors. They differ in the number and types of classifications they consider and in the models of human behaviour on which the taxonomies are based and on where the most emphasis is placed. The following are generally considered:

- a) The internal error mode and error mechanism. This is the reason behind the error in psychological meaningful terms e.g. for an error mode of “took a wrong turn in car”, the internal error mode and mechanism might be incorrect decision due to habit intrusion.
- b) Inherent problems of the task, e.g. conflicting goals, planning problems, constraints, cognitive demands etc.
- c) Performance shaping factors (PSF). These are the conditions of the technical or organizational environment or internal to a person which affect how well a task will be performed (see IEC 62508 [24]).

Some models also include an analysis of the flow of information and feedback without which correct judgements are unlikely to be made. The importance of these methods is that they first identify the psychological error mechanism before identifying why the error was made. For example if the error mechanism is not due to a lack of knowledge or skill, then further training is unlikely to be useful. If a decision is made to violate a procedure, then the reasons why this occurred should be investigated rather than assuming increased supervision is the solution.

Two examples of methods which can be used to analyse the causes of human failure which illustrate these principles are:

- Technique for retrospective and predictive analysis of cognitive errors (TRACEr);
- Human factors analysis and classification scheme (HFACS).

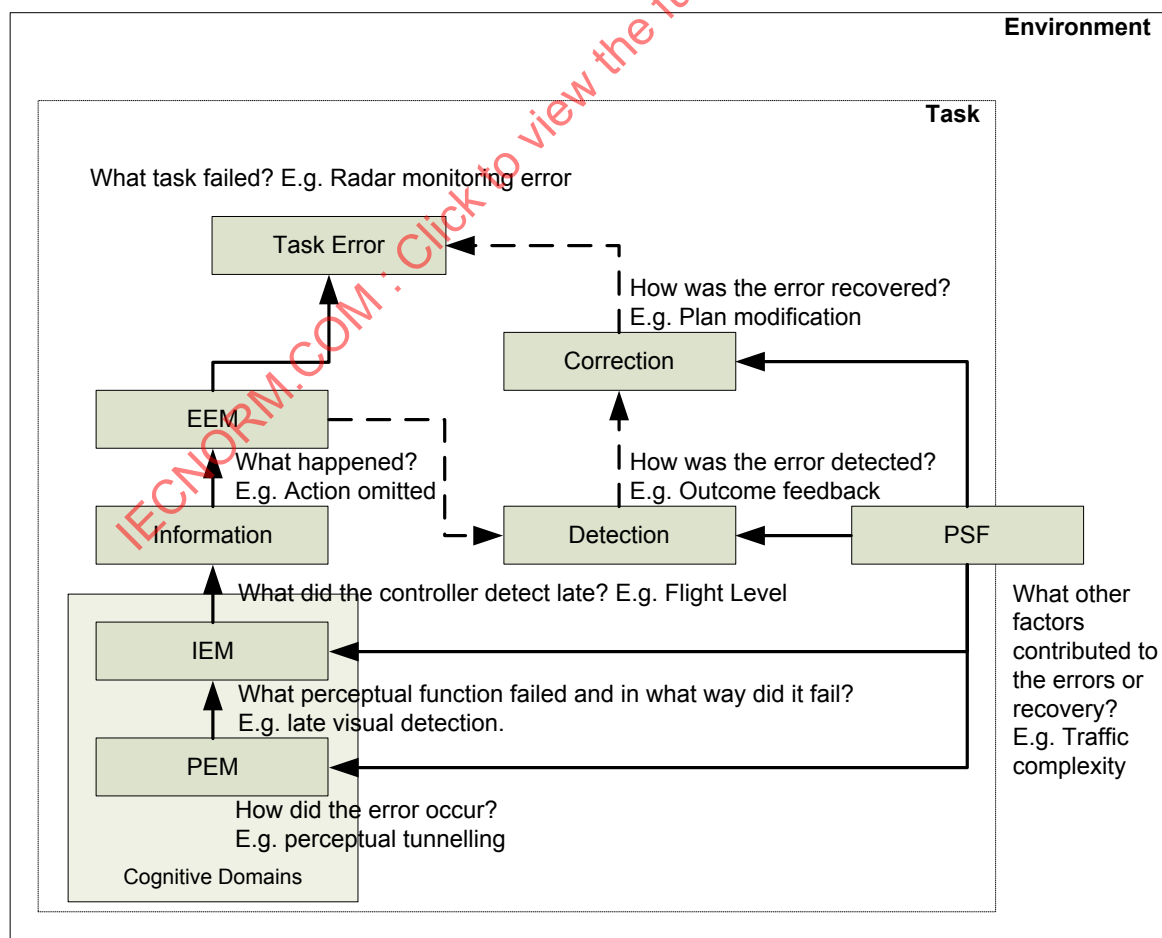
E.3 Technique for retrospective and predictive analysis of cognitive errors (TRACEr)

E.3.1 Overview

TRACEr [25] was developed for use in air traffic control. TRACEr, has eight modules as shown in Figure E.1, which can be divided into the following three categories:

- the context in which the error occurred, i.e. the nature of the task, the environment and the PSFs;
- the production of the error, i.e. the external error modes (EEM), internal error modes (IEM), the psychological error mechanisms (PEM) and the information on which the individuals based their actions;
- the detection and correction of the error.

The error production modules are based on the cognitive processes involved when a person perceives something needs to be done and takes action, e.g. perception, memory, decision-making and action (see Figure E.2).



IEC

Figure E.1 – Example of an TRACEr model [25]

Cognitive domain	Cognitive function	Relevant keywords	Example IEM
Perception	Vision	None, late, incorrect	Late detection
	Identification	None, late, incorrect	Misidentification
	Recognition/comparison	None, late, incorrect	Hearback error
Memory	Recall perceptual information	None, incorrect	Forget temporary information
	Previous action	None, incorrect	Forget previous actions
	Immediate/current action	None, incorrect	Forget to perform action
	Prospective memory	None, incorrect	Prospective memory failure
	Stored information (procedural and declarative knowledge)	None, incorrect	Mis-recall stored information
Judgement, planning and decision-making	Judgement	Incorrect	Misprojection
	Planning	None, too little, incorrect	Underplan
	Decision making	None, late, incorrect	Incorrect decision
Action Execution	Timing	Early, late, long, short	Action too early
	Positioning	Too much, too little, incorrect, wrong direction	Positioning error, overshoot
	Selection	Incorrect	Typing error
	Communication	None, unclear, incorrect	Unclear information transmitted

IEC

Figure E.2 – Generation of internal error modes

E.3.2 Process

A TRACER model is created using the following steps:

- Analyse the task being carried out and identify any environmental or situational factors that might affect human performance (PSF), which includes task complexity, knowledge and experience of the person, the ambient environment, etc.
- Identify EEMs, which are classified in terms of selection and quality, timing and sequence, and communication (see Table E.1).
- Identify the IEMs, which describe what cognitive function failed and in what way, the taxonomy for which is shown in Figure E.2.
- Identify the information issues associated with the IEM, i.e. what information was misperceived, forgotten, misjudged or mis-communicated.
- Identify the PEMs, which are the cognitive biases known to affect performance within each cognitive domain (see Table E.2).
- Review the error detection process, which is how the person became aware of the error, what medium informed them of the error and what external factors improved or degraded detection.
- Consider correction, i.e. what was done to correct the error, did other factors internal or external improve or degrade the error correction.

Table E.1 – External error modes

Selection and quality	Timing and sequence	Communication
Omission	Action too long	Unclear information transmitted
Action too little	Action too short	Unclear information received
Action too much	Action too early	Information not sought/obtained
Action in wrong direction	Action too late	Information not transmitted
Right action on wrong object	Action repeated	Information not recorded
Wrong action on right object	Mis-ordering	Incomplete information transmitted
Wrong action on wrong object		Incomplete information received
Extraneous act		Incomplete information recorded
		Incorrect information recorded

Table E.2 – Psychological error mechanisms

Perception	Memory	Decision making	Action
Expectation bias	Similarity interference	Incorrect knowledge	Manual variability
Spatial confusion	Memory capacity overload	Lack of knowledge	Spatial confusion
Perceptual confusion	Negative transfer	Failure to consider side effects	Habit intrusion
Perceptual discrimination failure	Mis-learning	Integration failure	Perceptual confusion
Perceptual tunnelling	Insufficient learning	Misunderstanding	Mis-articulation
Stimulus overload	Infrequency bias (memory failure due to knowledge not being used sufficiently frequently)	Cognitive fixation	Environmental intrusion
Vigilance failure	Memory block	False assumption	Other slip
Distraction	Distraction/preoccupation	Prioritization failure	Distraction preoccupation
		Risk negation or tolerance	
		Risk recognition failure	
		Decision freeze	

E.4 Human factors analysis and classification scheme (HFACS)

E.4.1 Overview

HFACS [26] was developed by behavioural scientists in the United States Navy and analyses the causes of human error based on Reason's model (see Clause B.3). There are four levels of consideration based on Reason's model of slices of Swiss cheese:

- organizational influences;
- supervision;
- preconditions for unsafe acts;
- unsafe acts.

Some applications add a fifth level above organizational influences relating to legislation and government.

E.4.2 Process

Each level is subdivided into categories; examples are given of possible causal factors within the category. Different applications use the same categories (shown in the boxes below) but

may have different examples depending on the industry, and may provide a few examples or a more detailed check list. Examples of the four levels are shown in Figure E.3 to E.6.

Consideration of cause starts with Level 1 so that precursors for the act in question take account of the type of error involved then continues up through the levels seeking weaknesses that contributed to the focus event.

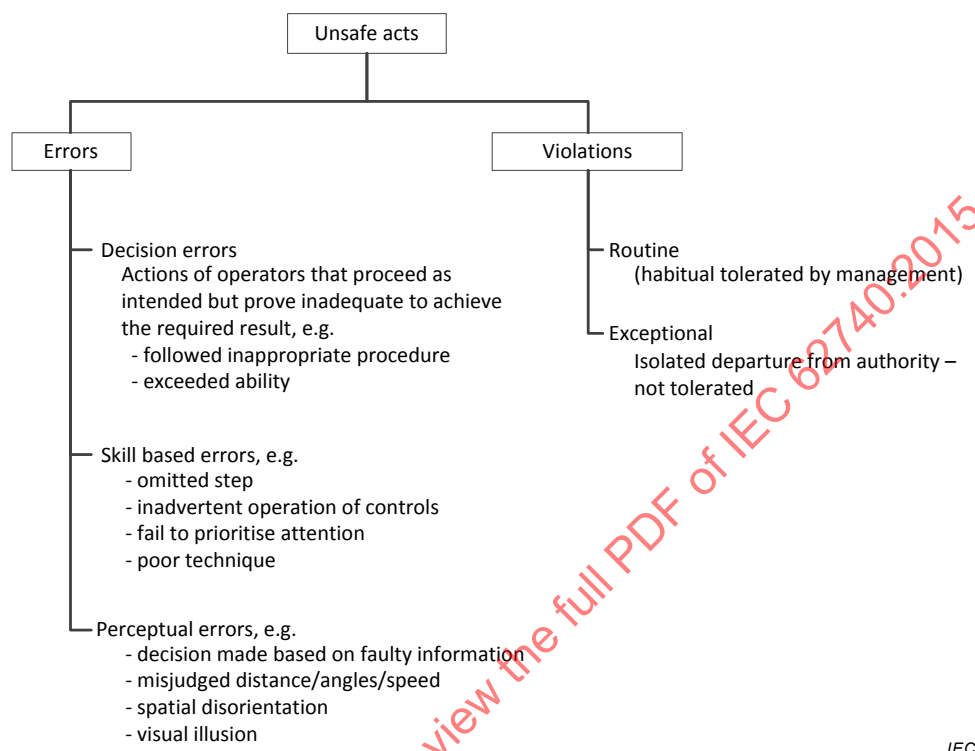


Figure E.3 – Level 1: Unsafe acts

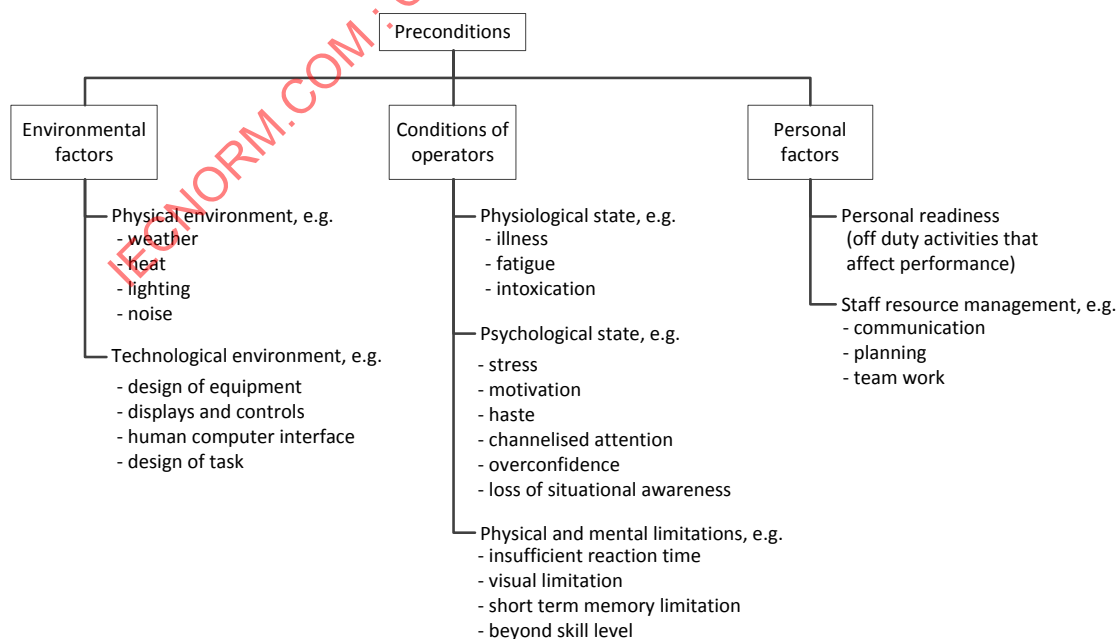
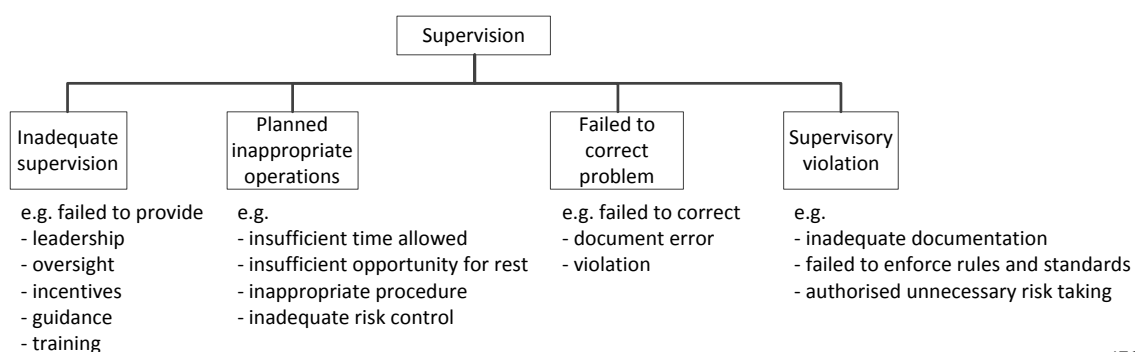
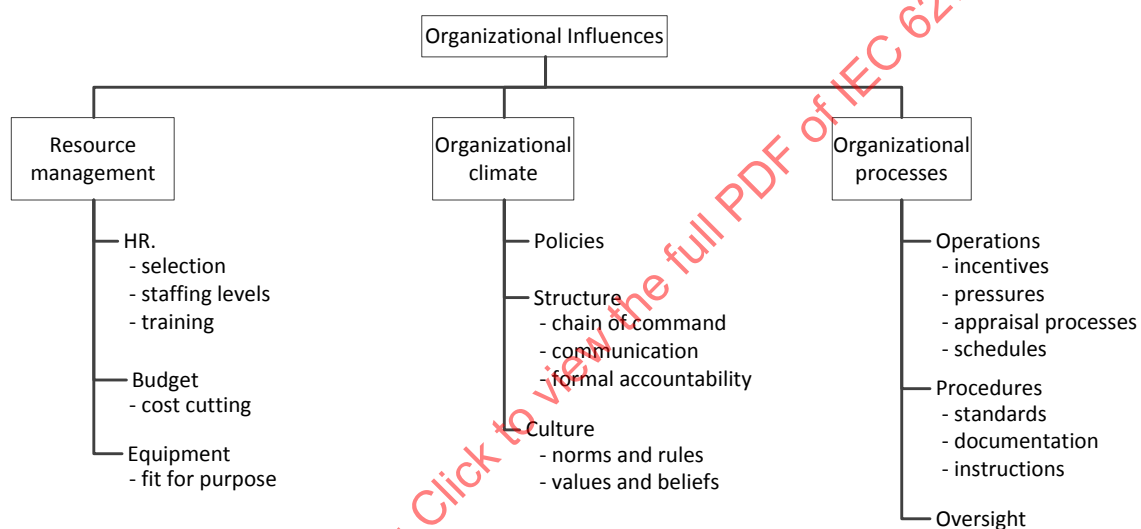


Figure E.4 – Level 2: Preconditions



IEC

Figure E.5 – Level 3: Supervision Issues

IEC

Figure E.6 – Level 4: Organizational Issues

Bibliography

- [1] ISO Guide 73: 2009, *Risk management – Vocabulary*
- [2] IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*
- [3] HADDON, W Jr., *Energy Damage and the Ten Counter-Measure Strategies*, The Journal of the Human Factors and Ergonomics Society, 1973
- [4] HOLLNAGEL, E., *Barriers and Accident Prevention*, Ashgate Publishing Limited, 2004
- [5] REASON, J., *Human Error*, Cambridge University Press, 1990
- [6] CHECKLAND, P., *Systems Thinking, Systems Practice: Includes A 30-Year Retrospective*, Wiley Pages: 416, 1999
- [7] LEVESON, N., *Engineering a Safer World*, MIT Press, 2012
- [8] RASMUSSEN, J., *Risk Management in a Dynamic Society: A Modelling Problem*, Safety Science Volume 27, Issue 2-3, Pages: 183-213, 1997
- [9] Technical Research and Analysis Center: Events and Causal Factors Analysis, SCIE-DOE-01-TRAC-14-95, 1995
- [10] BENNER, L. Jr., *Accident Investigations: Multilinear Event Sequencing Methods*, Journal of Safety Research 7, 67-73, 1975
- [11] HENDRICK, K. and BENNER, L. Jr., *Investigating Accidents with STEP*, Marcel Dekker Inc, 1986
- [12] MONTEAU, M., *Analysis and reporting: accident investigation*, Encyclopaedia of Occupational Health and Safety, 57-22:26, ISBN 1:92-2-1-103290-6, 1982
- [13] SANDERS, J., *Introduction to Why-Because Analysis*, 2012
- [14] US Nuclear Regulatory Commission: NUREG 0492, Fault Tree Handbook, January, 1981
- [15] IEC 61025, *Fault tree analysis (FTA)*
- [16] ISHIKAWA, K., *Guide to Quality Control*, Asia Productivity Organization, 1986
- [17] FAHLBRUCH, B. and SCHÖBEL, M., SOL – *Safety through organizational learning: A method for event analysis*. Safety Science, Volume 49, Pages 27–31, 2011
- [18] JOHNSON, W. and DEKKER, M., *MORT Safety Assurance Systems*, 1980
- [19] SVEDUNG, J. and RASMUSSEN, J., *Graphic representation of Accident Scenarios: Mapping System Structure and the Causation of Accidents*, Safety Science, Volume 40, Pages 397-417, 2002
- [20] SVEDUNG, J. and RASMUSSEN, J., *Risk Management in a Dynamic Society: A Modelling Problem*, Safety Science, Volume 27, Pages 183-213, 1997
- [21] Energy Institute, *Tripod Beta: Guidance on the use of Tripod Beta in the investigation and analysis of incidents, accidents and business losses*, 2013
<http://www.tripodfoundation.com>
- [22] IEC 61649, *Weibull analysis*
- [23] IEC 61163-1, *Reliability stress screening – Part 1: Repairable assemblies manufactured in lots*

- [24] IEC 62508:2010, *Guidance on human aspects of dependability*
- [25] SHORROCK, S. and KIRWAN, B., *Development and application of a human error identification tool for air traffic control*, Applied Ergonomics, Volume 33, Pages 319–336, 2002
- [26] SHAPPELL, S. and WIEGMANN, D., *Applying Reason: The Human Factors Analysis and Classification System (HFACS)*, Human Factors and Aerospace Safety, Volume 1, Pages 59-86 , 2001
- [27] ISO/IEC 31010:2009, *Risk management – Risk assessment techniques*
- [28] ISO 31000: 2009, *Risk management – Principles and guidelines*

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

SOMMAIRE

AVANT-PROPOS	72
INTRODUCTION.....	74
1 Domaine d'application	75
2 Références normatives	75
3 Termes, définitions et abréviations	75
3.1 Termes et définitions	75
3.2 Abréviations	78
4 RCA – Vue d'ensemble	78
5 Le processus de RCA	79
5.1 Vue d'ensemble	79
5.2 Début.....	81
5.3 Etablissement des faits	83
5.4 Analyse.....	84
5.4.1 Description	84
5.4.2 Equipe d'analyse	85
5.5 Validation.....	86
5.6 Présentation des résultats.....	87
6 Choix des techniques pour l'analyse des causes	88
6.1 Généralités	88
6.2 Choix des techniques d'analyse	88
6.3 Outils utiles pour faciliter la RCA	89
Annexe A (informative) Résumé et critères des techniques de RCA les plus communément utilisées	90
A.1 Généralités	90
A.2 Techniques d'analyse de cause initiale	90
A.3 Critères.....	91
Annexe B (informative) Modèles de RCA	94
B.1 Généralités.....	94
B.2 Analyse des barrières	94
B.2.1 Vue d'ensemble	94
B.2.2 Points forts et limites	95
B.3 Modèle de Reason (modèle du fromage suisse).....	95
B.3.1 Vue d'ensemble	95
B.3.2 Points forts et limites	96
B.4 Les modèles des systèmes	96
B.5 Modèle et processus d'accident théorique des systèmes (STAMP)	97
B.5.1 Vue d'ensemble	97
B.5.2 Points forts et limites	97
Annexe C (informative) Description détaillée des techniques RCA	99
C.1 Généralités	99
C.2 Graphique des événements et des facteurs causaux (ECF)	99
C.2.1 Vue d'ensemble	99
C.2.2 Processus.....	100
C.2.3 Points forts et limites	101
C.3 Séquençage d'événements multilinéaires (MES) et restitution d'événements successifs (STEP).....	101

C.3.1	Vue d'ensemble	101
C.3.2	Processus.....	103
C.3.3	Points forts et limites	103
C.4	Méthode du 'pourquoi'	105
C.4.1	Vue d'ensemble	105
C.4.2	Processus.....	107
C.4.3	Points forts et limites	108
C.5	Méthode de l'arbre des causes (CTM).....	108
C.5.1	Vue d'ensemble	108
C.5.2	Processus.....	111
C.5.3	Points forts et limites	112
C.6	Etude des facteurs de causalité (WBA)	112
C.6.1	Vue d'ensemble	112
C.6.2	Processus.....	115
C.6.3	Points forts et limites	116
C.7	Méthode de l'arbre de panne et de l'arbre de réussite	116
C.7.1	Vue d'ensemble	116
C.7.2	Processus.....	117
C.7.3	Points forts et limites	118
C.8	Diagramme d'Ishikawa ou arêtes de poisson.....	118
C.8.1	Vue d'ensemble	118
C.8.2	Processus.....	119
C.8.3	Points forts et limites	120
C.9	Sécurité via l'apprentissage organisationnel (SOL)	120
C.9.1	Vue d'ensemble	120
C.9.2	Processus.....	120
C.9.3	Points forts et limites	121
C.10	Arbre de supervision de la gestion et des risques (MORT)	122
C.10.1	Vue d'ensemble	122
C.10.2	Processus.....	124
C.10.3	Points forts et limites	124
C.11	AcciMaps	124
C.11.1	Vue d'ensemble	124
C.11.2	Processus.....	125
C.11.3	Points forts et limites	128
C.12	Tripod Beta	129
C.12.1	Vue d'ensemble	129
C.12.2	Processus.....	130
C.12.3	Points forts et limites	131
C.13	Analyse casuelle à l'aide de STAMP (CAST).....	131
C.13.1	Vue d'ensemble	131
C.13.2	Processus.....	136
C.13.3	Points forts et limites	137
Annexe D (informative)	Outils utiles pour faciliter l'analyse de cause initiale (RCA)	138
D.1	Généralités	138
D.2	Techniques d'exploration de données et d'analyse typologique	138
D.2.1	Vue d'ensemble	138
D.2.2	Exemple 1	138
D.2.3	Exemple 2	139

D.2.4 Exemple 3	139
Annexe E (informative) Analyse des performances humaines	140
E.1 Généralités	140
E.2 Analyse des échecs humains	140
E.3 Technique d'analyse rétrospective et prédictive d'erreur cognitive (TRACEr)	141
E.3.1 Vue d'ensemble	141
E.3.2 Processus.....	143
E.4 Analyse des facteurs humains et plan de classification (HFACS)	145
E.4.1 Vue d'ensemble	145
E.4.2 Processus.....	145
Bibliographie.....	150
Figure 1 – Processus de RCA.....	81
Figure B.1 – Barrières en échec, inefficaces et manquantes qui entraînent l'événement d'accident	94
Figure C.1 – Exemple de graphique ECF	100
Figure C.2 – Données dans un module d'événement.....	103
Figure C.3 – Exemple de matrice chronologie-acteurs	105
Figure C.4 – Exemple d'arbre de pourquoi	107
Figure C.5 – Symboles et liens utilisés dans la CTM.....	109
Figure C.6 – Exemple d'arbre de cause	111
Figure C.7 – Exemple de WBG	115
Figure C.8 – Exemple d'arbre de panne pendant l'analyse.....	117
Figure C.9 – Exemple de diagramme d'Ishikawa ou arêtes de poisson.....	119
Figure C.10 – Exemple de diagramme MORT	123
Figure C.11 – Exemple d'AcciMap.....	128
Figure C.12 – Exemple de diagramme d'arbre Tripod Beta.....	130
Figure C.13 – Structure de contrôle de l'alimentation en eau d'une petite ville du Canada.....	135
Figure C.14 – Exemple d'analyse causale CAST du service local de santé	135
Figure C.15 – Exemple d'analyse causale CAST de gestion d'exploitation du service public local	136
Figure E.1 – Exemple de modèle TRACEr [25].....	143
Figure E.2 – Génération de modes d'erreurs internes	143
Figure E.3 – Niveau 1: Actes non sûrs	146
Figure E.4 – Niveau 2: Préconditions	147
Figure E.5 – Niveau 3: Problèmes de supervision	148
Figure E.6 – Niveau 4: Problèmes d'organisation	149
Tableau 1 – Etapes de la RCA.....	80
Tableau A.1 – Brève description des techniques de RCA.....	90
Tableau A.2 – Résumé des critères des techniques de RCA	91
Tableau A.3 – Attributs des techniques de RCA génériques.....	93
Tableau B.1 – Exemples de barrières	95
Tableau B.2 – Exemple de document d'analyse des barrières	95

Tableau C.1 – Facteurs causaux directs et indirects	121
Tableau E.1 – Modes d'erreurs externes	144
Tableau E.2 – Mécanismes d'erreurs psychologiques	145

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

ANALYSE DE CAUSE INITIALE (RCA)

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62740 a été établie par le comité d'études 56 de l'IEC: Sécurité de fonctionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1590/FDIS	56/1608/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

INTRODUCTION

L'analyse de cause initiale (RCA) désigne tout processus systématique qui identifie les facteurs qui ont contribué à un événement d'intérêt donné (événement d'accent). La RCA est réalisée en étant entendu que les événements sont résolus via la compréhension de leurs causes initiales, plutôt que de leurs symptômes évidents et immédiats. La RCA a pour objectif de révéler les causes initiales afin que la probabilité de leur survenue ou leur impact si elles surviennent puissent être modifiés.

Une importante distinction est à faire en ce que la RCA est utilisée pour analyser un événement d'accent qui s'est produit; elle analyse ainsi le passé (a posteriori). Cependant, la connaissance des causes initiales d'événements passés peut entraîner des actions qui amènent à des améliorations dans le futur.

La présente Norme internationale est conçue pour refléter les bonnes pratiques actuelles dans la réalisation d'une RCA. La présente norme est de nature générale, de sorte qu'elle peut apporter des lignes directrices pour de multiples secteurs et situations. Il peut exister des normes sectorielles qui établissent des méthodologies préférentielles pour des applications particulières. Si lesdites normes sont cohérentes avec la présente norme, alors les normes sectorielles seront généralement suffisantes.

La présente norme est une norme générique et n'aborde pas explicitement la sécurité ou les enquêtes d'accidents, bien que les méthodes décrites dans la présente norme puissent être utilisées dans ce but.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

ANALYSE DE CAUSE INITIALE (RCA)

1 Domaine d'application

La présente Norme internationale décrit les principes basiques de l'analyse de cause initiale (RCA) et spécifie les étapes qu'il convient qu'un processus de RCA inclue.

La présente norme identifie plusieurs attributs de techniques de RCA, qui aident à sélectionner la technique appropriée. Elle décrit chaque technique de RCA, ainsi que ses points forts et limites.

La RCA est utilisée pour analyser les causes initiales des événements d'accident, que leurs conséquences soient positives ou négatives, mais est plus couramment utilisée pour l'analyse des défaillances et des accidents. Les causes de tels événements peuvent être de nature multiple, notamment en fonction de la conception, des processus et des techniques, des caractéristiques organisationnelles, des aspects humains et des événements externes. La RCA peut être utilisée pour étudier les causes de non-conformité en termes de qualité (ou autres) des systèmes de gestion ainsi que pour l'analyse des défaillances, par exemple lors de la maintenance ou de l'essai des équipements.

La RCA est utilisée pour analyser des événements d'accident qui se sont produits, cette norme ne couvre donc que les analyses a posteriori. Il est reconnu que certaines des techniques de RCA avec adaptations peuvent être utilisées de manière proactive lors de la conception et du développement d'entités et pour l'analyse causale au cours de l'évaluation des risques; cependant, la présente norme met l'accent sur l'analyse des événements qui se sont produits.

L'objectif de la présente norme est de décrire un processus en vue de réaliser une RCA et d'expliquer les techniques permettant d'identifier les causes initiales. Lesdites techniques n'ont pas été conçues pour identifier la responsabilité ou la fiabilité, car ceci ne fait pas partie du domaine d'application de la présente norme.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60050 (toutes les parties), *Vocabulaire Electrotechnique International*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les définitions données dans l'IEC 60050-192, ainsi que les suivantes, s'appliquent.

3.1 Termes et définitions

3.1.1

cause

circonstance ou ensemble de circonstances qui entraînent une défaillance ou une réussite

Note 1 à l'article: Une cause peut apparaître lors de la spécification, de la conception, de la fabrication, de l'installation, de l'exécution ou de la maintenance.

[SOURCE: IEC 60050-192:2014, 192-03-11, modifiée – ajout des mots "circonstance ou" et "ou une réussite" au terme]

3.1.2

facteur causal

condition, action, événement ou état qui était nécessaire ou qui a contribué à la survenue de l'événement d'accident

3.1.3

élément coadjuvant

condition, action, événement ou état considéré comme secondaire, selon l'occurrence de l'événement d'accident

3.1.4

événement

occurrence ou changement d'un ensemble particulier de circonstances

Note 1 à l'article: Un événement peut être unique ou se reproduire et peut avoir plusieurs causes.

Note 2 à l'article: Un événement peut consister en quelque chose qui ne se produit pas.

Note 3 à l'article: Un événement peut parfois être désigné comme un "incident" ou un "accident".

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modifiée – Suppression de la Note 4 [1]]¹

3.1.5

défaillance <d'une entité>

perte de la capacité à s'exécuter comme cela est exigé

Note 1 à l'article: La défaillance d'une entité est un événement qui provoque une panne de cette entité.

Note 2 à l'article: Les qualificatifs, tels que catastrophique, critique, majeur, mineur, marginal et non significatif, peuvent être utilisés pour classer les défaillances en fonction de la gravité des conséquences, selon des critères de gravité dont le choix et les définitions dépendent du domaine d'application.

Note 3 à l'article: Des compléments tels que mauvais emploi, par fausse manœuvre et par fragilité, peuvent être utilisés pour classer les défaillances selon la cause de la défaillance.

Note 4 à l'article: Il s'agit de la défaillance d'une entité et non pas généralement de son comportement.

[SOURCE: IEC 60050-192:2014, 192-03-01, modifiée – Introduction d'une nouvelle Note 4]

3.1.6

mécanisme de défaillance

processus entraînant une défaillance

Note 1 à l'article: Il peut s'agir d'un processus physique, chimique ou logique, psychologique ou d'une de leurs combinaisons.

[SOURCE: IEC 60050:192:2014, 191-03-12, modifiée – ajout du mot "psychologique"]

3.1.7

événement d'accident

événement qui est destiné à être expliqué d'un point de vue causal

¹ Les chiffres entre crochets se réfèrent à la Bibliographie.

3.1.8**facteur causal immédiat**

condition, action, événement ou état pour lesquels il n'existe aucun autre facteur causal entre ce facteur causal et l'événement d'accent

Note 1 à l'article: Il peut s'agir de plusieurs facteurs causaux immédiats.

3.1.9**facteur causal nécessaire <d'un événement ou d'un état>**

condition, action, événement ou état qui résulte d'un événement ou d'un état donné et sans lequel l'événement ou l'état donné ne se serait pas produit

3.1.10**erreur humaine**

discordance entre l'action humaine effectuée ou omise et l'action voulue ou exigée

Note 1 à l'article: La première édition de l'IEC 60050-191:1990 a identifié le terme "faute" comme un synonyme du terme "erreur humaine", mais une faute est un type d'erreur humaine.

Note 2 à l'article: Le terme d'erreur humaine s'applique à toute situation dans laquelle le résultat n'est pas celui attendu, et ce que le but recherché par la personne soit correct ou non.

[SOURCE: IEC 60050-192:2014, 192-03-14, modifiée – Omission de l'exemple; ajout des Notes 1 et 2]

3.1.11**entité**

sujet à l'étude

Note 1 à l'article: L'entité peut être une pièce isolée, un composant, un dispositif, une unité fonctionnelle, un équipement, un sous-système ou un système.

Note 2 à l'article: L'entité peut être composée de matériel, de logiciel, de personnel ou d'une quelconque de leurs combinaisons.

Note 3 à l'article: L'entité est souvent composée d'éléments dont chacun peut être considéré individuellement.

[SOURCE: IEC 60050-192:2014, 192-01-01, modifiée – omission des références internes et des Notes 4 et 5]

3.1.12**cause initiale**

facteur causal sans aucun précédent et qui est pertinent dans le cadre de l'analyse

Note 1 à l'article: Un événement d'accent comprend normalement plusieurs causes initiales.

Note 2 à l'article: Dans certaines langues, le terme "cause initiale" désigne la combinaison des facteurs causaux qui n'ont aucun précédent causal (coupe de facteurs causaux).

3.1.13**analyse de cause initiale**

RCA

processus systématique visant à identifier les causes d'un événement d'accent

Note 1 à l'article: La définition 192-12-05 de l'IEC 60050-192:2014 fournit la définition plus restrictive suivante "processus systématique visant à identifier la cause d'une panne, d'une défaillance ou d'un événement indésirable, de telle sorte qu'il puisse être éliminé par des modifications de conception, de processus ou de procédure". La présente norme utilise une définition étendue pour permettre une plus vaste applicabilité du processus.

Note 2 à l'article: L'abréviation «RCA» est dérivée du terme anglais développé correspondant «root cause analysis».

3.1.14

partie prenante

personne ou organisation qui peut affecter, être affecté(e) ou se sentir affecté(e) par une décision ou une activité

[SOURCE: IEC 60300-1: 2014, 3.1.15] [2]

3.1.15

règle d'arrêt

moyen raisonnable et explicite visant à déterminer dans quels cas un facteur causal est défini comme étant une cause initiale

3.2 Abréviations

Abréviation	Français	Anglais
BGA	Boîtier micro matriciel à billes	Ball grid array
CAST	Analyse casuelle à l'aide de STAMP	Causal analysis using STAMP
CCT	L'essai de complétude des causes	Causal completeness test
CT	L'essai contrefactuel	Counterfactual test
CTM	Méthode de l'arbre des cause	Causes tree method
ECF	Événements et des facteurs causaux	Events and causal factors
EEM	Mode d'erreur externe	External error mode
FTA	L'analyse par arbre de panne	Fault tree analysis
GEMS	Système de modélisation d'erreurs génériques	Generic error modelling system
HFACS	Analyse des facteurs humains et plan de classification	Human factor analysis and classification scheme
IEM	Mode d'erreur interne	Internal error mode
MES	Séquençage d'événements multilinéaires	Multilinear events sequencing
MORT	Arbre de supervision de la gestion et des risques	Management oversight and risk tree
PEM	Mécanisme d'erreur psychologique	Psychological error mechanism
PSF	Facteurs de modélisation des performances	Performance shaping factors
RCA	Analyse de cause initiale	Root cause analysis
SOL	Sécurité via l'apprentissage organisationnel	Safety through organizational learning
STAMP	Analyse causale via un modèle et le processus d'accident théorique des systèmes	Systems theoretic accident model and process
STEP	Restitution d'événements successifs	Sequentially timed events plotting
TRACER	Technique d'analyse rétrospective et prédictive d'erreur cognitive	Technique for retrospective and predictive analysis of cognitive errors
WBA	Etude des facteurs de causalité	Why-because analysis

4 RCA – Vue d'ensemble

La RCA désigne tout processus systématique visant à identifier la ou les causes contribuant à un événement d'accident. La cause immédiate ou évidente d'un événement d'accident est souvent le symptôme de causes sous-jacentes et peut ne pas permettre d'identifier la ou les véritables causes initiales qu'il convient d'identifier et de résoudre. La RCA fournit une meilleure compréhension de la raison de la survenue des événements. La RCA peut identifier les éléments suivants:

- a) cause initiale unique;

- b) causes initiales multiples pour lesquelles l'élimination de n'importe laquelle des causes empêchera l'événement d'accent de se produire;
- c) causes initiales qui sont des facteurs coadjuvants et où l'élimination changera la probabilité de la survenue de l'événement d'accent, mais qui peuvent ne pas l'empêcher directement;
- d) causes initiales de réussites.

En résolvant la ou les causes initiales, il est possible de prendre des décisions concernant les actions appropriées qui généreront de meilleures conséquences dans le futur; la mise en œuvre des actions appropriées basées sur la RCA est un moyen plus efficace d'empêcher le même événement ou des événements similaires avec conséquences négatives de se produire ou d'augmenter la probabilité de répétition d'événements à conséquences positives, que de simplement résoudre les symptômes immédiatement évidents.

La RCA peut être appliquée à n'importe quel événement d'accent résultant d'une réussite ou d'une défaillance, par exemple:

- 1) enquête relative à des événements d'accent technologiques, médicaux et professionnels;
- 2) analyse des défaillances des systèmes technologiques, afin de déterminer pourquoi une entité n'a pas pu s'exécuter de façon exigée ou au moment exigé;
- 3) analyse des processus de contrôle qualité et d'affaires;
- 4) analyse des conséquences de réussite.

La RCA peut être réalisée à plusieurs niveaux de décomposition, par exemple au niveau du système ou au niveau des composants ou en sélectionnant différents événements ou conséquences comme point de départ. Le niveau approprié pour réaliser l'analyse dépendra de l'événement d'accent.

La RCA est utilisée pour analyser des événements d'accent qui se sont réellement produits; elle est donc applicable au cours des phases d'essai et d'exécution d'un projet ou pendant le cycle de vie du produit. La RCA peut identifier les problèmes de processus, y compris la conception, le contrôle qualité, la gestion de la sûreté de fonctionnement et la gestion de projet.

Les avantages de la réalisation d'une RCA incluent:

- obtention d'une meilleure compréhension de ce qu'il s'est passé;
- identification de la source des problèmes afin qu'une action corrective puisse empêcher des événements futurs;
- identification des causes des événements à conséquences positives pour qu'ils puissent être reproduits;
- identification d'actions plus efficaces pour résoudre les causes des événements d'accent;
- atteinte plus efficace des objectifs de l'enquête sur l'événement d'accent;
- prise en charge de la traçabilité entre les preuves de l'enquête sur l'événement d'accent et ses conclusions;
- augmentation de la cohérence entre les enquêtes sur les événements d'accent similaires;
- augmentation de l'objectivité de l'analyse de l'événement d'accent.

5 Le processus de RCA

5.1 Vue d'ensemble

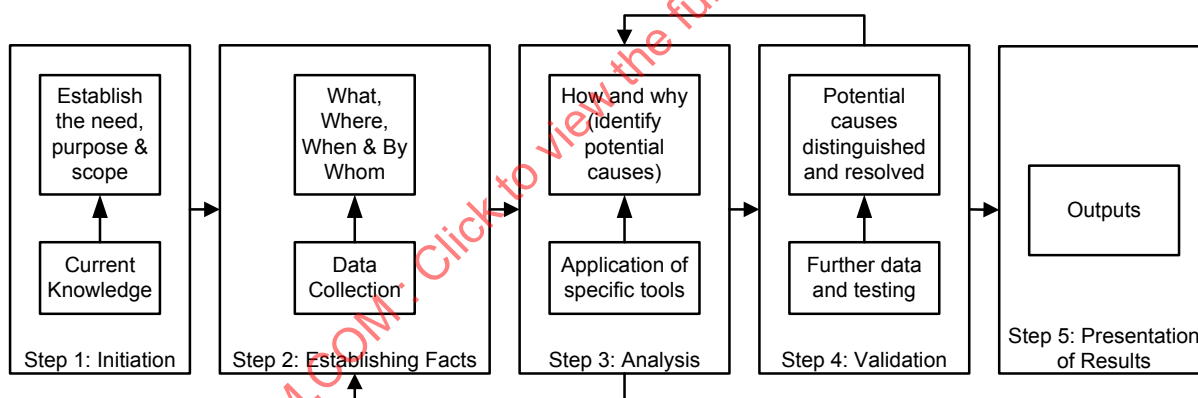
Pour être efficace, il convient que la RCA soit effectuée de façon systématique sous forme d'enquête, en intégrant les causes initiales et les conclusions dans des preuves

documentées. Pour ce faire, il convient que la RCA inclue les cinq étapes présentées dans le Tableau 1 et illustrées dans la Figure 1.

Tableau 1 – Etapes de la RCA

Etape	Concepts et tâches à réaliser
Début	Fondé sur les connaissances disponibles sur l'évènement d'accident, déterminer le besoin de réaliser une RCA et définir son objectif et son domaine d'application
Etablissement des faits	Collecter les données et établir les faits de ce qu'il s'est passé, où, comment et par qui
Analyse	Utiliser les outils et les techniques de RCA pour établir comment et pourquoi l'évènement d'accident s'est produit
Validation	Distinguer et résoudre les différentes possibilités liées à la manière et aux raisons de la survenue de l'évènement d'accident
Présentation des résultats	Présenter les résultats de l'analyse de l'évènement d'accident

La RCA est par nature itérative, notamment en ce qui concerne la collecte et l'analyse des données, dans le sens où des données sont collectées sur 'ce' qu'il s'est passé, puis elles sont analysées afin de déterminer quelles autres données ont besoin d'être collectées. Une fois ces données rassemblées, une analyse approfondie est réalisée et les écarts sont identifiés, pour lesquels d'autres données sont collectées. Ce processus est répété jusqu'à ce que l'objectif de l'analyse soit atteint et que les causes initiales soient identifiées. Les résultats de la RCA dépendront de son objectif et de son domaine d'application.



IEC

Légende

Anglais	Français
Establish the need, purpose and scope	Etablir le besoin, l'objectif et le domaine d'application
Immediate facts	Faits immédiats
Step 1: Initiation	Etape 1: Début
What, where, when and who	Quoi, où, quand et qui
Data collection	Collecte de données
Step 2: Establishing facts	Etape 2: Etablissement des faits
How and why (identify potential causes)	Comment et pourquoi (identifier les causes potentielles)
Application of specific tools	Application d'outils spécifiques
Step 3: Analysis	Etape 3: Analyse

Anglais	Français
Potential causes distinguished and resolved	Causes potentielles identifiées et résolues
Further data and testing	Autres données et essai
Step 4: Validation	Étape 4: Validation
Outputs	Résultats
Step 5: Presentation of results	Étape 5: Présentation des résultats

Figure 1 – Processus de RCA

5.2 Début

La première étape démarre le processus de RCA en évaluant le besoin de réaliser une RCA. Elle définit l'objectif et le domaine d'application de l'analyse en réponse à l'événement d'accent et fixe une équipe et des ressources pour réaliser la RCA.

Il existe généralement des critères qui sont utilisés pour déterminer les cas où une RCA est exigée; ces critères peuvent inclure:

- tout événement unique qui a des effets de grande ampleur;
- des événements indésirables multiples et similaires;
- un paramètre qui dépasse un niveau de tolérance défini;
- des défaillances ou des réussites (quel que soit leur niveau d'effet) qui impliquent des entités critiques d'équipement ou d'activités.

Lors de la définition des types d'événements qui exigent la réalisation d'une RCA, il est important de prendre en compte qu'un événement avec un effet de grande ampleur peut avoir des causes initiales communes avec d'autres événements à effets mineurs. L'analyse et la résolution des causes initiales des événements à effets mineurs peuvent empêcher la survenue d'un événement de grande ampleur. Voici des exemples d'événements où une RCA peut être exigée: achèvement d'un projet (réussites et défaillances), défaillances qui entraînent des coûts inacceptables, une blessure ou une mort, des performances ou des délais inacceptables, des conséquences contractuelles de grande ampleur et une panne de l'équipement.

Dans le cas où la RCA est exigée, les événements d'accent à analyser sont décrits et une équipe adéquate est composée pour l'analyse. Il convient que la description inclue les données de fond et le contexte dans lequel le ou les événements d'accent s'est/se sont produit(s). Une description adéquate d'un événement d'accent est courte, simple et facile à comprendre; il convient qu'elle ne soit pas orientée vers l'utilisation d'une solution spécifique. Cette description est utilisée pour identifier les membres appropriés de l'équipe d'analyse et pour établir à quel niveau commencer la collecte des données.

Il convient que l'objectif et le domaine d'application de la RCA soient déterminés en prenant compte le niveau de connaissances sur le système, les fonctions, les interfaces, etc. Dans certains cas, l'objectif de l'analyse est d'identifier les causes de l'événement d'accent; cet objectif peut être plus vaste dans d'autres cas. Par exemple, afin d'identifier également les sujets de préoccupation qui ne sont pas ceux qui ont entraîné la survenue de l'événement d'accent.

Il y a en général deux différents types de RCA qui ont des objectifs divers et qu'il convient de ne pas mélanger. Ces deux types peuvent être décrits comme suit:

- 1) analyse d'un événement d'accent observé utilisant uniquement des informations factuelles vérifiables;
- 2) analyse d'un événement d'accent pour obtenir des hypothèses de séquences d'événements et de causes.

Le premier type se concentre uniquement sur des faits observés. Il peut s'agir d'une analyse "per se" en fonction de l'objectif de l'étude et aucune hypothèse concernant la survenue de l'événement n'est acceptable pour cette analyse. Le second type peut être mis en œuvre lorsque des informations factuelles en nombre suffisant ne sont pas disponibles et des hypothèses de causes potentielles sont acceptables pour les besoins de l'analyse. .

Il convient également d'identifier les résultats exigés de la RCA. Se reporter aux exemples ci-dessous:

- fournir une description de chaque cause initiale ainsi que suffisamment de données de fond pour permettre l'identification des actions adéquates;
- recommander des actions qui, réalisées ensemble, empêchent la réapparition d'événements similaires avec des conséquences négatives et augmentent la probabilité de réapparition de réussites;
- identifier, mettre en œuvre et revoir les actions pour résoudre les causes initiales.

La RCA peut inclure l'analyse de systèmes dans lesquels les limites évoluent et interagissent continuellement avec leur environnement); cette interaction peut prendre la forme d'un transfert d'informations, d'énergie ou de matériaux. De ce fait, il convient que le domaine d'application spécifie la limite de l'analyse (ce qui est inclus et ce qui est exclu).

Quand cela est possible, il convient que le domaine d'application de l'analyse inclue une définition de la 'règle d'arrêt', qui constitue le point au niveau duquel une action peut être définie ou qui indique que des preuves supplémentaires de cause ne sont plus nécessaires dans le cadre de l'analyse. Par exemple, le dernier point au niveau duquel une action corrective peut être identifiée, avant les facteurs qui ne peuvent pas être influencés, comme la météo. Il peut cependant être plus approprié d'établir la règle d'arrêt au niveau des points de revue qui déterminent si une analyse plus poussée est exigée.

La RCA peut être réalisée efficacement par un seul individu, à condition que ledit individu soit expérimenté dans la technique d'analyse causale, soit un expert du domaine (ou ait un accès immédiat aux experts du domaine) et ait accès à toutes les données exigées. Cependant, il est plus commun de confier la réalisation de la RCA à une équipe. Il convient que les membres de l'équipe d'analyse soient choisis en fonction de l'expertise spécifique exigée pour analyser l'événement d'accident. Il convient que l'équipe comporte:

- un ou des individus qui peuvent fournir une présentation complète des systèmes ainsi que des connaissances sur le programme, le projet et l'événement d'accident;
- un facilitateur qualifié dans la technique d'analyse causale, préférablement entraîné ou expérimenté dans la facilitation de la technique d'analyse causale;

Les membres de l'équipe peuvent être modifiés en fonction de l'activité réalisée; par exemple, les membres de l'équipe responsables de la collecte des données ne seront pas forcément les mêmes que ceux responsables de la réalisation de l'analyse. Les membres de l'équipe peuvent être des ingénieurs, des techniciens, des opérateurs, des commerciaux et des responsables. Il convient de considérer l'emploi de tiers afin de fournir un point de vue indépendant et d'éviter les "angles morts" qui peuvent exister au sein de l'organisation. Il convient d'inclure des membres supplémentaires à l'équipe, dédiés à des activités spécifiques au cours de l'enquête, afin soit d'apporter une expertise dans l'équipe, soit d'augmenter l'influence de l'équipe. Le rôle de ces membres supplémentaires consiste à soutenir l'enquête pour ne pas qu'elle soit interrompue pour des raisons techniques ou de frontières organisationnelles. Il n'est pas approprié que les individus qui peuvent avoir eu un rôle dans la causalité de l'événement d'accident fassent partie de l'équipe. Il convient de collecter leurs observations au cours des deux premières étapes.

5.3 Etablissement des faits

Cette étape inclut toutes les activités nécessaires pour préparer l'analyse. L'établissement des faits est habituellement la plus grande partie de la RCA. Il convient de déterminer les faits sur 'ce' qu'il s'est passé, 'où', 'quand' et 'par qui'.

Il convient de collecter les données avant qu'elles ne soient perdues (par exemple avant que les preuves ne soient éparpillées ou éliminées où que la mémoire des témoins soit moins claire. En général, les données collectées comprendraient:

- a) le contexte dans lequel l'événement d'accent s'est produit;
- b) les conditions, avant, pendant et après l'événement d'accent;
- c) l'implication du personnel, y compris les actions effectuées (ou non effectuées) et les décisions prises;
- d) les données contextuelles à propos des alentours, y compris les données environnementales;
- e) la façon dont l'organisation opère, y compris les organigrammes, les processus et procédures, ainsi que la formation et les compétences;
- f) les données historiques relatives à des événements similaires ou à des précurseurs;
- g) les écarts par rapport au résultat attendu;
- h) les interactions avec d'autres entités et avec le personnel;
- i) l'équipement impliqué, son état de fonctionnement et la conformité avec les exigences.

La liste suivante répertorie des exemples de données qui peuvent être pertinentes:

- 1) Inspection de preuves physiques telles que des composants défailants et des rapports de défaillance. Généralement, l'expérience déterminera quelles preuves physiques sont exigées. S'il subsiste des doutes, il convient de retenir les preuves. Il est également important de préserver les preuves.
- 2) Photographies et vidéos prises par des caméras de surveillance. Le fait de photographier la zone où s'est produit l'événement de différents points de vue sera également utile lors de la phase d'analyse.
- 3) Données opérationnelles, enregistrées par des systèmes de surveillance, des systèmes de contrôle, des enregistreurs d'alarmes et d'événements, etc. Les enregistrements d'opérateurs peuvent se montrer critiques pour comprendre les conditions d'exploitation au moment de la défaillance; de plus, comme ils sont généralement datés (ou à rythme commandé par l'horloge), ils sont idéaux pour générer la chronologie des événements.
- 4) Témoignages individuels, collectés en menant des entretiens. Il convient d'orienter les entretiens sur la collecte des données, par exemple la création d'une chronologie cohérente, etc.; toute discussion prématurée sur les causes de la défaillance peut impacter de façon négative le processus d'entretien. Il convient de préparer des questions avant l'entretien afin de s'assurer que toutes les informations exigées sont obtenues. Il convient de faire des entretiens avec les individus les plus familiers de l'événement d'accent; cependant, il faut prendre en considération la réalisation d'entretiens avec d'autres membres du personnel, par exemple des individus qui ont effectué la même tâche dans le passé. Il convient que tous les entretiens soient documentés.
- 5) Preuves documentées des procédures pertinentes, de l'environnement d'exploitation et de l'environnement réglementaire.

Cette étape peut inclure l'analyse de la défaillance, qui examine les composants défailants à l'aide d'une vaste gamme de méthodes incluant la microscopie, la spectroscopie et les essais non destructifs ou des modèles sur le développement de la défaillance tel que la modélisation feu ou la modélisation crash.

Une fois que toutes les données associées à l'événement d'accent ont été collectées, il convient de revoir les données pour déterminer leur exactitude et leur pertinence, de collecter

les données manquantes et de résoudre toutes les incohérences pour s'assurer qu'une image claire et cohérente de l'événement d'accent est générée.

Les résultats de cette étape sont des informations et une meilleure compréhension, soutenues par des preuves physiques et des énoncés sur

- ce qu'il s'est passé, y compris les circonstances qui ont mené à l'événement d'accent,
- la séquence temporelle des événements qui ont mené à l'événement d'accent,
- la localisation de l'événement d'accent,
- les actions des personnes associées à l'événement d'accent,
- toutes les conditions nécessaires à l'événement d'accent,
- les conséquences de l'événement d'accent.

5.4 Analyse

5.4.1 Description

Après avoir déterminé 'ce' qu'il s'est passé, 'où', 'quand' et 'par qui', cette étape établit 'comment' et 'pourquoi' l'événement d'accent s'est produit. L'objectif de cette étape est de comprendre l'événement d'accent et ses causes en structurant les données collectées dans un formulaire qui permet d'identifier systématiquement les causes initiales.

La RCA analyse normalement les faits pour identifier les causes qui étaient nécessaires pour que l'événement d'accent se produise, désignées par le terme "facteurs causaux nécessaires". Cependant, dans certains cas, par exemple lorsqu'une quantité insuffisante de faits est disponible, l'analyse peut suggérer une ou plusieurs hypothèses de cause et peut également identifier les facteurs coadjuvants et les conditions prédominantes qui étaient probablement associées avec l'événement d'accent, mais qu'on ne peut pas prouver être des facteurs causaux nécessaires.

L'analyse implique les éléments suivants:

- organisation des preuves physiques et des énoncés sur: les actions, les événements, les conditions et les conséquences.
- recherche de la façon et de la raison de la survenue de l'événement d'accent à l'aide des données collectées afin de justifier les conclusions. Des modèles de causalité, des essais en laboratoire, des listes de contrôle et des taxonomies ou analyses statistiques des données peuvent être utilisés pour faciliter ce processus.
- projection au-delà des facteurs causaux immédiats pour définir pourquoi ils se sont produits. Le but est de rechercher tous les facteurs causaux qui ont contribué, non pas de se limiter aux causes évidentes.
- poursuite de ce processus jusqu'à ce que la règle d'arrêt soit invoquée et que les causes initiales soient identifiées. Il peut exister de multiples causes initiales qui peuvent être indépendantes ou en corrélation.

De façon générale, les facteurs causaux peuvent impliquer des problèmes techniques, des aspects humains et des facteurs relatifs à l'environnement physique ou psychosocial dans lequel s'est produit l'événement d'accent. Il convient de prendre en considération tous ces éléments lors de la recherche des causes initiales. Il convient donc que les individus dotés d'une expertise dans ces domaines soient impliqués dans l'analyse.

Il convient de décrire les facteurs causaux clairement et sans ambiguïté. Lorsqu'une action, une omission ou une décision d'origine humaine est identifiée comme un facteur causal, il convient de spécifier la nature de ladite action ou décision, par exemple "l'opérateur a éteint le mauvais interrupteur de puissance", plutôt que "erreur humaine".

L'analyse des facteurs causaux peut prendre en considération (en fonction de l'objectif et du domaine d'application de l'analyse):

- la façon dont l'événement d'accent s'est produit, par exemple le processus physique, chimique, psychologique ou logique impliqué;
- les conditions ou les événements précédents qui ont été nécessaires à la survenue de l'événement d'accent;
- les relations entre les facteurs causaux, y compris la façon dont ils se sont combinés pour causer l'événement d'accent ainsi que la façon dont une cause initiale entraîne l'événement d'accent;
- les influences organisationnelles ou hiérarchiques ainsi que les facteurs humains qui étaient impliqués dans l'événement d'accent ou dans les événements et les conditions qui y ont mené;
- les conditions prédominantes qui peuvent avoir contribué à la survenue de l'événement, mais qui n'en ont pas été des facteurs causaux nécessaires;
- les sujets de préoccupation qui aurait pu mener à d'autres événements d'accent (ce ne sont pas des facteurs causaux à proprement parler, mais peuvent être un résultat de l'analyse).

Il convient d'utiliser une technique d'analyse structurée pour effectuer l'analyse. Plusieurs techniques formelles existent, de techniques basées sur des listes de contrôle des causes aux techniques qui guident l'analyste lors de la considération des causes ou qui présentent de façon graphique les résultats. Un éventail de techniques simples à complexes est utilisé, qui exige des intervenants ou des facilitateurs adéquatement formés afin de faire l'analyse. Certaines techniques sont basées sur des modèles particuliers sur la façon dont un événement d'accent se produit et donnent donc une accentuation particulière aux résultats. Les différents modèles sont basés sur différentes hypothèses relatives à la causalité, ils tendent donc à mener l'enquêteur à identifier les différents facteurs coadjuvants.

Dans certains cas, il est approprié d'utiliser plus d'une technique ou de prendre en considération plus d'un modèle afin d'identifier toutes les causes initiales.

Les modèles de causalité sont décrits dans l'Annexe B et les techniques d'analyse sont décrites dans l'Annexe C. La technique la plus appropriée dépendra de l'événement d'accent, de l'objectif et du domaine d'application de l'analyse (voir Article 6).

L'analyse peut indiquer que des données supplémentaires sont exigées. Il convient que les demandes pour de telles données se produisent tout au long de l'analyse afin de résoudre les incohérences ou les écarts dans l'analyse. Il convient de poursuivre l'analyse jusqu'à ce qu'une 'règle d'arrêt' soit invoquée.

5.4.2 Équipe d'analyse

Il convient de nommer un responsable pour l'étape d'analyse, qui se charge du suivi du travail préparatoire comme suit:

- a) obtention des copies des rôles et des responsabilités convenus au sein de l'équipe, mais aussi de l'objectif et du domaine d'application de l'analyse;
- b) obtention des copies de la description de l'événement d'accent et des faits établis;
- c) choix des techniques d'analyse à utiliser;
- d) conversion de la description de l'événement d'accent et des faits établis dans un format adéquat pour utilisation dans la technique d'analyse sélectionnée;
- e) développement d'un plan d'analyse;
- f) formation de l'équipe d'analyse;
- g) facilitation ou organisation de la formation des membres de l'équipe pour la technique d'analyse sélectionnée;

- h) choix des outils logiciels ou des autres modèles à utiliser au cours de l'analyse;
- i) organisation d'une recherche à faire dans les bases de données, les supports, les procédures judiciaires, etc. afin d'identifier les événements d'accident de nature similaire ou qui peuvent s'être produits avec les mêmes technologies ou des technologies similaires.

Il convient que le responsable revoie les informations disponibles afin de déterminer quelles techniques d'analyse il convient d'appliquer et quelles compétences sont exigées. Il peut être nécessaire d'obtenir des conseils d'experts dans le domaine de la RCA concernant le choix de la technique d'analyse. Le responsable peut également exiger un facilitateur RCA expert pour tout ou partie de l'analyse, en fonction de la complexité de l'événement d'accident, de la complexité ou du volume des preuves et des données ou de la technique d'analyse sélectionnée.

L'analyse est généralement réalisée par une équipe, dont chaque membre est choisi pour son expérience et ses compétences. Il convient que l'équipe d'analyse soit aussi réduite que possible et soit cohérente avec l'expérience et les compétences techniques et opérationnelles exigées à disposition. Lorsque les observations de plusieurs tiers, parties prenantes ou entités sont exigées, il convient que l'équipe d'analyse englobe des représentants de chaque groupe. Il est à la charge du responsable de s'assurer que les parties prenantes pertinentes soient informées, afin que leurs représentants soient disponibles au cours de l'analyse.

Il convient de déterminer le rôle et les responsabilités des membres de l'équipe d'analyse et d'établir les jalons dès les prémices de l'analyse. Il convient d'établir un programme des réunions, qui reflète les objectifs et les jalons fournis par l'équipe d'analyse. Cela aura pour but de permettre de transférer toutes les recommandations en temps opportun.

Il convient que le responsable développe un plan d'analyse, dont il convient qu'il englobe les éléments suivants:

- 1) description de l'événement d'accident;
- 2) rôles et responsabilités convenus au sein de l'équipe, mais aussi objectif et domaine d'application de l'analyse;
- 3) liste des membres de l'équipe et parties prenantes à représenter;
- 4) heure, date et lieu des réunions pour l'analyse;
- 5) résumé des données disponibles;
- 6) technique(s) d'analyse à utiliser;
- 7) organisation pour la formation de l'équipe d'analyse sur la technique d'analyse sélectionnée (si cela est exigé);
- 8) formulaire d'enregistrement de l'analyse et des résultats de l'analyse, y compris les références à tout modèle ou outil logiciel à utiliser.

Il convient que le responsable mette en place une salle appropriée avec équipements visuels et d'enregistrement pour la tenue de réunions d'analyse efficaces. Il convient qu'un pack de briefing comprenant le plan d'analyse et toute documentation ou référence essentielle à lire avant la réunion soit envoyé aux membres de l'équipe d'analyse avant la première réunion, afin qu'ils puissent se familiariser avec les informations disponibles et la technique d'analyse sélectionnée.

Il convient que le responsable s'assure qu'un système de communication approprié est en place pour informer et transférer les résultats de l'analyse aux personnes en charge de la prochaine étape du processus de RCA (voir 5.5).

5.5 Validation

Diverses activités de revue sont réalisées tout au long du processus de RCA afin de déterminer si les données collectées sont pertinentes et si l'analyse est représentative des données collectées. Cette étape soumet les causes identifiées dans l'analyse à l'essai afin de

déterminer si elles peuvent être corroborées et si elles peuvent être insérées dans l'analyse ou faire l'objet d'une activité distincte.

Une revue indépendante peut être réalisée pour évaluer si l'analyse est complète et correcte, mais aussi pour déterminer si l'objectif de l'analyse a été atteint. La méthode de revue sera basée sur la technique d'analyse utilisée et sur l'événement d'accent. Dans certains cas, des expériences peuvent être effectuées afin de réitérer la survenue de l'événement d'accent; il convient donc que les méthodes statistiques appropriées soient utilisées pour évaluer le degré de confirmation de l'hypothèse sur la cause. Si les causes sont validées par le biais d'une simulation, il convient de prendre soin de s'assurer que la simulation est représentative.

Au cours de l'analyse, il peut y avoir plusieurs hypothèses alternatives sur la façon dont l'événement aurait pu se produire. Si l'objectif est de reproduire un rapport factuel des causes alors, il convient qu'à la fin de l'analyse, les causes soient validées et que ne soit retenue qu'une seule conclusion.

Cette étape peut exiger la collecte de données supplémentaires afin de trouver des preuves directes corroborant ou alléguant les causes identifiées. Des preuves peuvent ne pas toujours être disponibles pour valider entièrement toutes les causes potentielles.

5.6 Présentation des résultats

Les résultats de l'analyse seront fonction de l'objectif de l'analyse. Par exemple, si l'objectif de l'analyse est d'identifier les actions qui, effectuées ensemble, empêchent la survenue d'autres événements similaires, il convient que les résultats de l'analyse identifient les actions correctives qui rompent le lien de causalité et empêchent l'événement d'accent de se produire à nouveau. Si l'objectif de l'analyse est de réitérer des réussites, alors il convient que les actions qui augmentent la probabilité de la survenue ou les conséquences de l'événement d'accent soient énoncées. L'efficacité des résultats de l'analyse dépendra de la qualité de l'analyse.

Il convient de développer un format de présentation des résultats de la RCA accepté de tous, qui résume l'analyse et regroupe les résultats exigés de l'analyse, par exemple les actions recommandées. Si le résultat attendu de la RCA est de produire les actions recommandées, il convient que le résumé intègre au moins les éléments suivants:

- a) une description générale de chaque cause nécessitant une action, ainsi que suffisamment d'informations de fond et de détails pour s'assurer que la nécessité de résoudre chaque cause soit comprise et que les actions à entreprendre puissent être identifiées;
- b) un ensemble d'options pour les actions de résolution et, si réalisable et dans le domaine d'application, un résumé des avantages et des coûts de chacune d'entre elles;
- c) des actions recommandées pour résoudre chacune des causes identifiées.

Il convient que les actions correctives soient évaluées en termes d'efficacité et de réalisme. De manière générale, les actions correctives visent à atteindre les objectifs suivants:

- modifier la probabilité de survenue de l'événement d'accent et/ou de ses conséquences (par exemple, réduire la probabilité de survenue ou les conséquences d'événements indésirables ou augmenter la probabilité de survenue ou les conséquences d'événements de réussite);
- ne pas introduire de nouveaux risques inacceptables; par exemple, il ne faut pas que la sécurité d'autres systèmes soit dégradée par l'action corrective suggérée.

Lorsque des actions sont identifiées, il convient qu'elles soient revues avant d'être mises en œuvre afin de déterminer si, en plus de résoudre les causes initiales, elles n'ont pas introduit de nouvelles conséquences inattendues et si elles fonctionnent donc comme prévu. Il convient que la réapparition du même événement ou d'un événement similaire soit surveillée, afin d'évaluer l'efficacité des actions entreprises.

6 Choix des techniques pour l'analyse des causes

6.1 Généralités

Des techniques formelles ont été conçues pour aider les analystes à identifier les facteurs causaux et éventuellement les causes initiales. Les techniques d'analyse peuvent assumer une ou plusieurs des fonctions suivantes:

- organiser les données, fournir une structure pour l'analyse et identifier si des preuves supplémentaires sont nécessaires;
- fournir une visualisation des preuves relatives à l'événement d'accent, comme une séquence temporelle des événements ou des chaînes causales;
- effectuer une analyse statistique des données, notamment provenant de plusieurs événements similaires, afin d'identifier les facteurs causaux communs;
- fournir des lignes directrices pour identifier les facteurs causaux possibles et entamer une enquête approfondie ou une comparaison des données (de telles méthodes incluent des listes de contrôle et des méthodes basées sur des modèles de causalité);
- aider les analystes à travers les chaînes causales pour établir un ensemble de causes initiales.

6.2 Choix des techniques d'analyse

La RCA est effectuée selon divers degrés de détails et peut exploiter un éventail de techniques d'analyse simples à complexes. Il convient que le niveau de détail de l'analyse et que les techniques utilisées incluent les caractéristiques suivantes:

- être justifiables et appropriés par rapport à l'événement d'accent soumis à l'analyse, au domaine d'application et à l'objectif de l'analyse;
- fournir des résultats qui améliorent la compréhension des causes initiales de l'événement d'accent;
- pouvoir être utilisés d'une manière traçable, répétable et vérifiable.

Les techniques d'analyse à utiliser sont sélectionnées en fonction des facteurs applicables, tels que

- les caractéristiques de la technique d'analyse,
- les caractéristiques de l'événement d'accent, par exemple sa gravité ou sa gravité et sa complexité potentielles,
- les caractéristiques de l'organisation, par exemple les techniques approuvées dans son secteur d'activité ou l'évaluation coûts-bénéfices,
- l'objectif de l'analyse, comme les résultats exigés ou les attentes des parties prenantes,
- le ou les modèles de causalité les plus appropriés selon les objectifs de l'analyse.

Les attributs des techniques d'analyse les plus souvent utilisées sont décrits à l'Annexe A. Les critères utilisés pour caractériser les techniques décrites à l'Annexe A sont les suivants:

- expertise exigée;
- soutien des outils;
- extensibilité;
- représentation graphique;
- modularité;
- reproductibilité;
- contrôles de plausibilité;
- rigueur intellectuelle;

- séquence temporelle;
- spécificité.

Les descriptions détaillées des techniques de RCA sont décrites à l'Annexe C, qui inclut les méthodes les processus utilisés pour chaque technique ainsi que leurs points forts et limites.

6.3 Outils utiles pour faciliter la RCA

Les techniques modernes d'exploration de données permettent de rechercher des propriétés et des conditions spécifiques. L'analyse typologique sélectionne les données qui sont étroitement liées et identifie donc les données qui dévient (valeurs aberrantes). Les techniques modernes d'analyse typologique peuvent détecter des données qui sont étroitement liées sur une ou plusieurs dimensions et donc analyser des produits ou des processus qui sont étroitement liés afin d'identifier des points de données qui dévient (valeurs aberrantes). Une présentation de ces techniques est fournie à l'Annexe D.

De multiples événements d'accent et techniques d'analyse impliquent des facteurs humains et diverses taxonomies ont été développées pour faciliter la recherche des causes initiales quand un comportement humain est impliqué. Deux exemples sont donnés à l'Annexe E.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

Annexe A (informative)

Résumé et critères des techniques de RCA les plus communément utilisées

A.1 Généralités

L'Annexe A répertorie et décrit brièvement les techniques de RCA les plus communément utilisées et fournit une liste de référence des critères qui peuvent être utilisés pour comparer différentes techniques de RCA. La liste n'est pas exhaustive, mais inclut des exemples des différents types de techniques utilisées.

A.2 Techniques d'analyse de cause initiale

Le Tableau A.1 fournit une liste et une brève description des techniques de RCA les plus communément utilisées.

Tableau A.1 – Brève description des techniques de RCA

Technique	Description
Graphique des événements et des facteurs causaux (ECF)	L'analyse ECF identifie la séquence temporelle d'une série de tâches et/ou d'actions ainsi que les conditions sous-jacentes qui mènent à un événement d'accent. Celles-ci sont affichées dans un diagramme de causes et effets
Séquençage d'événements multilinéaires (MES) et restitution d'événements successifs (STEP)	Le MES et la STEP sont des méthodes de regroupement de données et de suivi pour l'analyse d'événements d'accent complexes. Les résultats sont affichés sous la forme d'une matrice chronologie-acteurs
Méthode du pourquoi	La méthode du 'Pourquoi' guide l'analyse par le biais de la chaîne causale en posant la question pourquoi un certain nombre de fois
Méthode de l'arbre des causes (CTM)	La CTM est une technique systématique pour l'analyse et la représentation graphique des événements et conditions qui ont contribué à un événement d'accent. La méthode CTM est similaire à la méthode du pourquoi dans la théorie; elle élabore cependant un arbre plus complexe et prend en compte explicitement les causes techniques, organisationnelles, humaines et environnementales
Etude des facteurs de causalité (WBA)	La WBA établit le réseau des facteurs causaux responsables d'un événement d'accent à l'aide d'une comparaison à deux facteurs, l'essai contrefactuel. Le réseau des facteurs est affiché dans un graphique des facteurs de causalité
Méthode de l'arbre de panne et de l'arbre de réussite	L'arbre de panne ou l'arbre de réussite est une représentation graphique des informations, qui permet à l'utilisateur de mener une analyse déductive pour déterminer les combinaisons critiques qui entraînent une réussite ou une défaillance, qui sont affichées graphiquement dans un diagramme en forme d'arbre logique
Diagramme d'Ishikawa ou arêtes de poisson	Le diagramme d'Ishikawa ou arêtes de poisson est une technique qui permet d'identifier, d'analyser et de représenter les causes possibles d'un événement d'accent. Cette technique illustre la relation entre l'événement d'accent et tous les acteurs qui peuvent l'avoir influencé
Sécurité via l'apprentissage organisationnel (SOL)	La SOL est un outil d'analyse basé sur une liste de contrôle et dédié aux événements d'accent dans des centrales nucléaires. Les résultats sont présentés visuellement dans un diagramme chronologie-acteurs, issue de la méthode MES/STEP
Arbre de supervision de la gestion et des risques (MORT)	Le graphique MORT est un arbre de panne prérempli avec des événements, habituellement des pannes ou des oublis, exprimés en termes génériques. L'arbre MORT comporte deux branches principales et plusieurs sous-branches pour fournir un niveau de détails élevé. La première des branches principales identifie environ 130 facteurs de contrôle spécifiques tandis que la seconde identifie plus de 100 facteurs du système de gestion. Ce graphique contient également 30 facteurs du système d'informations supplémentaires qui sont communs aux deux branches principales de l'arbre

Technique	Description
AcciMaps	AcciMaps est principalement une technique d'affichage des résultats pour une analyse causale. Elle exige un modèle organisationnel pour ranger les facteurs en diverses couches et pour extraire les facteurs dans les couches; elle exploite une version de l'essai contrefactuel (voir WBA) pour déterminer les relations de causalité entre les facteurs
Tripod Beta	Tripod Beta est un diagramme en forme d'arbre qui représente le lien de causalité, en s'intéressant sur les facteurs humains et en cherchant les défaillances dans l'organisation qui peuvent causer des erreurs humaines
Analyse causale via le modèle et le processus d'accident théorique des systèmes (STAMP) (CAST)	La CAST est une technique qui examine l'intégralité du processus sociotechnique impliqué dans un événement d'accident. La CAST documente le processus dynamique entraînant l'événement d'accident, y compris la structure de contrôle sociotechnique ainsi que les contraintes qui ont été enfreintes à chaque niveau de la structure de contrôle

A.3 Critères

Le Tableau A.2 répertorie et décrit les critères utilisés pour caractériser les techniques de RCA énumérées dans le Tableau A.1. Chaque critère possède trois niveaux indiqués par un (+), un (o) ou un (–), ces niveaux indiquant la portée.

Les attributs de chaque technique de RCA utilisant les critères du Tableau A.2 sont spécifiés dans le Tableau A.3.

Tableau A.2 – Résumé des critères des techniques de RCA

Critères	Description	Niveaux
Expertise exigée	La méthode nécessite-t-elle un "utilisateur sophistiqué" (exige-t-elle l'utilisation de techniques qui exigent une expertise technique, telles que la démonstration de théorème)? Est-elle adaptée à une utilisation par des experts du domaine uniquement?	• Intuitive, peu de formation exigée (+) • Formation limitée exigée, par exemple une journée (o) • Grand effort de formation exigé, par exemple une semaine (–)
Soutien des outils	Le soutien des outils est-il nécessaire?	• Peut être appliquée correctement sans soutien dédié des outils (+) • Le soutien des outils n'est pas exigé, mais il est habituellement nécessaire pour une utilisation efficace (o) • Le soutien des outils est nécessaire, la méthode ne peut être appliquée qu'avec un soutien dédié des outils (–)
Extensibilité	La méthode est-elle extensible? La méthode peut-elle être utilisée de façon économique pour des événements d'accident aussi bien simples que complexes? Un sous-ensemble de la méthode peut-il être appliqué à des événements d'accident plus petits ou moins significatifs et l'intégralité de la méthode réservée aux événements d'accident plus importants ou plus significatifs? La question d'extensibilité demande si la complexité de la méthode d'analyse s'adapte à la complexité de l'événement d'intérêt	• S'adapte parfaitement à la complexité (+) • Extensibilité limitée, frais considérables pour chaque application (o) • Aucune extensibilité, l'intégralité de la méthode doit être appliquée (–)

Critères	Description	Niveaux
Représentation graphique	Quelle est la nature de la représentation graphique de la méthode? Le principe motivateur est qu'un dessin vaut mieux qu'un long discours. Il est souvent plus éloquent d'afficher les résultats d'une méthode d'analyse sous forme d'image, de graphique ou de toute autre illustration, que sous une forme purement textuelle. Les propriétés souhaitables d'une représentation graphique sont les suivantes: • afficher clairement la sémantique de la causalité (y compris le sens des facteurs causaux et la taxonomie des facteurs); • être cognitivement (relativement) facile à évaluer par un seul individu, • idéalement, une représentation graphique pourrait également afficher l'historique de l'analyse	• Représentation graphique avec sémantique clairement définie et cognitivement facile à comprendre (+) • Représentation graphique, mais sans sémantique (o) • Aucune représentation graphique définie (–)
Reproductibilité	Les résultats de la méthode sont-ils reproductibles? Différents analystes obtiendraient-ils des résultats similaires pour le même événement d'accent?	• Les résultats peuvent être reproduits, on observe des différences uniquement dans la représentation des résultats, leur formulation, etc. (+) • On peut reproduire une quantité significative des résultats, mais certaines différences seront observées (o) • Les résultats dépendront de l'expertise de l'analyste (–)
Contrôles de plausibilité	Existe-t-il des contrôles de plausibilité raisonnables et rapides pour les résultats obtenus et qui ne dépendent pas de l'outil utilisé? Quels moyens existe-t-il de contrôler l'"exactitude" des résultats? Un exemple serait des listes de contrôle	• Il existe des contrôles de plausibilité pour presque tous les aspects (+) • Il existe des contrôles de plausibilité, mais ils ne couvrent pas nécessairement tous les aspects (o) • Il n'existe que des moyens limités de contrôler la plausibilité (–)
Rigueur intellectuelle	Dans quelle mesure la méthode est-elle rigoureuse? La rigueur revêt deux aspects pertinents: • La méthode a-t-elle un sens rigoureux et une sémantique formelle pour les notions clés de facteur causal et de cause initiale? La sémantique est-elle simple à appliquer? • Les résultats de la méthode sont-ils adaptés à une vérification formelle (mathématique)? Dans quelle mesure l'application de la méthode est-elle maniable?	• Définie formellement et peut être formellement vérifiée (+) • Définition semi-formelle (o) • Définition informelle (–)
Séquence temporelle	La méthode inclut-elle une représentation de la séquence temporelle des événements?	• Oui (+) • Seulement indirectement (o) • Non (–)
Spécificité	La mesure dans laquelle la méthode limite l'analyse aux facteurs causaux nécessaires plutôt que d'explorer un éventail de problèmes généraux avec le système, qui ont existé au moment de l'événement d'accent et qui peuvent y avoir contribué	• La méthode analyse uniquement les facteurs causaux nécessaires de l'événement d'accent (+) • La méthode peut être utilisée pour analyser les facteurs coadjuvants ainsi que les facteurs causaux nécessaires de l'événement d'accent (o) • La méthode cherche les problèmes généraux, qu'ils soient ou non des facteurs causaux nécessaires de l'événement d'accent (–)

Annexe B (informative)

Modèles de RCA

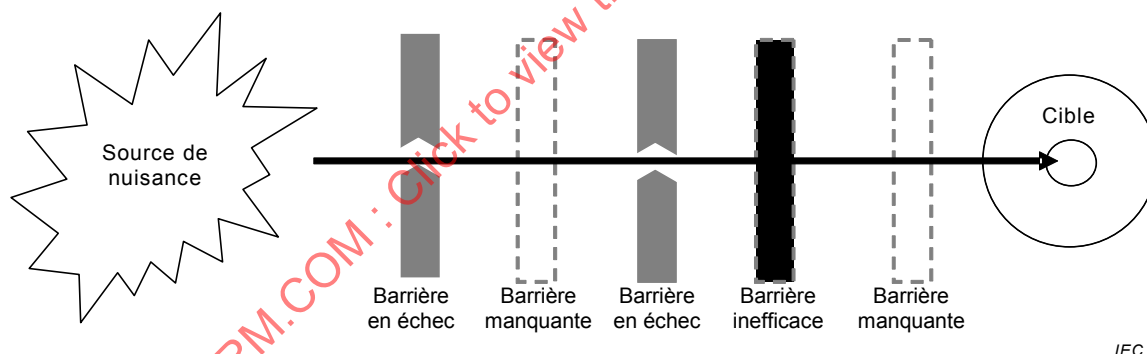
B.1 Généralités

La présente annexe décrit les modèles de RCA les plus communément utilisés, qui fournissent diverses façons d'aborder des événements d'accident. Les différents modèles sont basés sur certaines hypothèses concernant l'événement d'accident, par exemple, l'analyse des barrières suppose que l'événement d'accident s'est produit suite à une barrière manquante, en échec ou inefficace. Ainsi, les différents modèles tendent à mener l'enquêteur à identifier divers facteurs causaux. Les modèles sont utilisés pour orienter le processus de pensée en cohésion avec les techniques de l'Annexe C ou simplement pour identifier un ensemble de facteurs causaux.

B.2 Analyse des barrières

B.2.1 Vue d'ensemble

L'analyse des obstacles se base sur l'hypothèse qu'un événement d'accident se produit suite à l'interaction d'une source de nuisance sur une cible et que ceci peut être empêché grâce à l'utilisation de barrières [3]. Un événement indésirable se produit lorsque les barrières sont manquantes, en échec ou inefficaces (voir la Figure B.1).



IEC

**Figure B.1 – Barrières en échec, inefficaces et manquantes
qui entraînent l'événement d'accident**

Haddon [3] considérait les événements d'accident selon le fait que la source de nuisance est une énergie physique et que les barrières peuvent être un moyen de modifier l'énergie ou de la retenir d'affecter la cible. Le modèle a été étendu de diverses manières [4], par exemple les barrières sont souvent catégorisées en barrières physiques ou administratives (voir des exemples dans le Tableau B.1). Les barrières peuvent également être interprétées en termes de prévention, de protection et de détection (par exemple dans le contexte où l'événement d'accident est un feu, il s'agirait de l'utilisation de matériaux non inflammables, de la fourniture d'extincteurs et de l'installation de détecteurs de fumée).

Les résultats de l'analyse incluent généralement un document d'analyse des barrières (voir le Tableau B.2), qui identifie les barrières qui étaient soit disponibles, mais inefficaces, soit manquantes lors de la survenue de l'événement d'accident.

Tableau B.1 – Exemples de barrières

Barrières physiques ou d'énergie	Barrières administratives
Fonctions de sûreté techniques	Procédures d'exploitation et de maintenance de l'installation
Appareils de sécurité et de relève	Réglementations, politiques et pratiques
Autorisations de conception prudente	Formation et éducation
Équipement redondant	Protection du travail
Portes et vannes verrouillées	Permis de travail
Appareils de protection de défaut de mise à la masse	Personnel expérimenté
Blindage et protections	Méthodes de communication (communication tridirectionnelle)
Alarmes	Pratiques de supervision
Systèmes automatiques de confinement d'incendie	

Tableau B.2 – Exemple de document d'analyse des barrières

Conséquence indésirable (que s'est-il passé?)	Source de nuisance	Barrière(s) ayant dû rejeter l'évènement indésirable	Mécanisme de défaillance de la barrière (façon dont la barrière a subi une défaillance)	Évaluation de la barrière (pourquoi les barrières ont subi une défaillance)
Répertorier un élément après l'autre; cela peut ne pas être dans l'ordre séquentiel		Répertorier toutes les barrières physiques et administratives pour chaque conséquence indésirable		Identifier si la barrière était manquante, défaillante ou inefficace; et pourquoi
Le technicien de maintenance a desserré l'écrou sur la bride d'un tuyau pressurisé	Liquide pressurisé	Procédure pour éteindre la pompe et relâcher la pression avant le démarrage des travaux	Pression relâchée sur le mauvais système	Étiquetage trop flou

B.2.2 Points forts et limites

Les points forts de l'analyse des barrières sont les suivants:

- identifie les actions de correction exigées pour s'assurer que les barrières adéquates (en nombre et en efficacité) sont en place.

Les limites de l'analyse des barrières sont les suivantes:

- peut ne pas reconnaître toutes les barrières défaillantes ou manquantes ou l'effet du rythme ou de la fréquence à laquelle les barrières ont été sollicitées;
- résout les facteurs causaux immédiats plutôt que les causes initiales; cherche par exemple quelle barrière a subi une défaillance et comment, mais n'explore pas les raisons de quelque manière que ce soit.

B.3 Modèle de Reason (modèle du fromage suisse)

B.3.1 Vue d'ensemble

Le modèle de Reason [5] est basé sur le postulat que les éléments basiques exigés de tout système de production sont

- des décisions appropriées de la direction de l'installation et du siège social,
- des activités de gestion de ligne, des formations sur les opérations de maintenance, etc.,
- fiables et adéquats pour l'utilisation d'équipements,
- du personnel motivé,
- l'intégration d'éléments humains et mécaniques,
- des protections contre les risques prévisibles.

Il y a inévitablement des faiblesses dans ces éléments, qui peuvent être considérés comme des défaillances latentes. Si ces derniers deviennent un événement déclencheur, qui peut ne pas avoir d'importance dans d'autres circonstances, ceci résulte en une défaillance.

Les faiblesses des éléments du système de production sont représentées par des trous dans des tranches de fromage suisse. Un événement se produira lorsque toutes les faiblesses individuelles s'aligneront. Le modèle de Reason n'est pas à proprement parler un modèle de barrières, puisque les couches sont des systèmes d'exploitation normaux dotés de faiblesses plutôt que des barrières ou des contrôles défaillants.

Les taxonomies d'erreurs humaines basées sur le modèle de Reason ont été développées pour divers secteurs d'activité.

B.3.2 Points forts et limites

Les points forts du modèle de Reason sont les suivants:

- encourage l'analyste à explorer les facteurs causaux de l'erreur de l'opérateur et donc les moyens potentiels pour la réduire.

Les limites du modèle de Reason sont les suivantes:

- analyse superficielle des facteurs causaux techniques ou environnementaux, puisque les aspects techniques ne sont représentés que sous forme de barrières défaillantes;
- suppose que le problème principal est une erreur de l'opérateur (les erreurs à d'autres niveaux et les défaillances organisationnelles sont explorées principalement dans la façon dont elles ont influencé l'erreur de l'opérateur);
- ne fournit pas de taxonomie pour faciliter l'identification des motivations et précurseurs psychologiques de l'erreur humaine ou bien l'identification des défaillances latentes; exige donc une expertise en psychologie individuelle ou organisationnelle pour être utilisée correctement.

B.4 Les modèles des systèmes

La théorie des systèmes [6] a été développée dans les années 1940 et 1950 afin de gérer la complexité croissante des systèmes après la seconde Guerre mondiale et de tenir compte des aspects sociaux et techniques des systèmes comme un tout.

Dans les modèles du système, on suppose que l'interaction humaine avec la technologie dans des structures sociales complexes est influencée par les objectifs, les politiques et la culture des organisations et par des éléments économiques, juridiques, politiques et environnementaux tant internes qu'externes. Ce système est influencé par le rythme rapide de l'évolution technologique, par un environnement de plus en plus concurrentiel et agressif, ainsi que par des facteurs tels que les pratiques réglementaires changeantes et la pression publique. Dans ce contexte, les événements d'accent sont causés par de multiples facteurs et attendent généralement d'être "libérés", c'est-à-dire qu'ils ne sont pas dus à une action ou à un événement.

Les défaillances surviennent à cause des interactions complexes entre les composants du système, qui peuvent entraîner une dégradation des performances du système. Deux ou plus d'événements discrets au sein des éléments du système peuvent interagir de façon inattendue, que les concepteurs n'auraient pas pu prévoir et que les opérateurs ne peuvent pas comprendre ni contrôler sans essais ni modélisations exhaustifs. Les facteurs contribuant à l'événement d'accident peuvent inclure les effets des décisions qui sont normales dans les circonstances dans lesquelles elles ont été prises, mais qui produisent des conséquences indésirables.

Les méthodes basées sur un modèle de systèmes ne cherchent pas de chaîne de causalité ni d'erreur individuelle ou de défaillance technique, mais considèrent le système comme un tout, avec ses interactions et ses faiblesses. Les défaillances matérielles ou humaines individuelles peuvent être reconnues, mais l'accent est mis sur les interactions et les problèmes du système.

B.5 Modèle et processus d'accident théorique des systèmes (STAMP)

B.5.1 Vue d'ensemble

Le STAMP [7] est un modèle de causalité basé sur la théorie des systèmes [6] et qui étend le modèle traditionnel (chaînes d'événements de défaillance directement liés) pour inclure les contributeurs techniques et sociaux aux événements d'accident et à leurs relations. Il capture également les événements d'accident qui impliquent des interactions dans les composants pas en panne du système et dans les processus, des mécanismes causaux indirects et systémiques, une prise de décision du management et des opérateurs complexe, une technologie avancée telle que les logiciels et les systèmes numériques, ainsi que les défauts de conception du système.

STAMP suppose que les incidents surviennent lors des interactions entre les humains, les machines et l'environnement; il traite les systèmes comme des problèmes de contrôle dynamiques dans lesquels les contrôles tendent à gérer les interactions entre les composants du système et son environnement. L'objectif du contrôle est de mettre en place des contraintes sur le comportement des composants du système; par exemple, les avions, dans un système de contrôle du trafic aérien, doivent toujours maintenir une distance de séparation minimale. Les événements d'accident résultent d'un contrôle ou d'une mise en œuvre inadaptée des contraintes sur le développement, la conception et l'exploitation du système. Dans l'accident de la navette spatiale "Challenger", par exemple, les joints toriques n'ont pas contrôlé la libération des gaz propulseurs dans la liaison intersegment de la navette spatiale. Dans STAMP, la cause d'un événement d'accident est une structure de contrôle défaillante.

STAMP comprend également le concept selon lequel les incidents sont souvent issus d'une lente migration de l'ensemble du système vers un état de risque élevé [8] de sorte que les pressions financières et autres qui conduisent à un changement de comportement dans le temps peuvent être prises en compte pour le processus d'analyse causale.

B.5.2 Points forts et limites

Les points forts de STAMP sont les suivants:

- il prend en compte l'ensemble du système sociotechnique dans la causalité;
- il inclut les facteurs indirects et systémiques dans l'explication causale;
- il fournit un modèle pour expliquer les accidents dans les systèmes très complexes;
- il identifie les causes au sein même du processus dans lequel un système a été développé.

Les limites de STAMP sont les suivantes:

- exige que les événements d'accent soient analysés d'une façon dont les ingénieurs n'ont souvent pas l'habitude; cela peut donc prendre plus de temps d'apprendre à analyser les événements d'accent à l'aide de processus d'analyse basés sur STAMP.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015

Annexe C **(informative)**

Description détaillée des techniques RCA

C.1 Généralités

L'Annexe C décrit une gamme de techniques utilisées dans un RCA. La liste n'est pas exhaustive, mais inclut des exemples des différents types de techniques utilisées. Un certain nombre de ces techniques est pris en charge par des outils logiciels. Une partie de la méthodologie et des outils logiciels a des éléments propriétaires, ce qui peut avoir un impact sur le coût de mise en œuvre de la technique.

Certaines techniques visent à identifier les facteurs causaux dont il peut être montré qu'ils sont nécessaires si l'événement d'accent doit se produire. D'autres méthodes recherchent les faiblesses générales du système dans son ensemble qui ont probablement contribué à l'événement d'accent, mais en l'absence desquelles l'événement d'accent aurait pu se produire. Dans certaines terminologies, un "facteur causal " ne peut pas être ainsi décrit sauf si cela est nécessaire pour l'événement d'accent. Dans cette annexe, ces facteurs causaux sont appelés "facteurs causaux nécessaires". Les faiblesses identifiées qui peuvent avoir joué un rôle dans l'événement d'accent, mais qui peuvent ne pas être nécessaires sont appelées "facteurs coadjuvants".

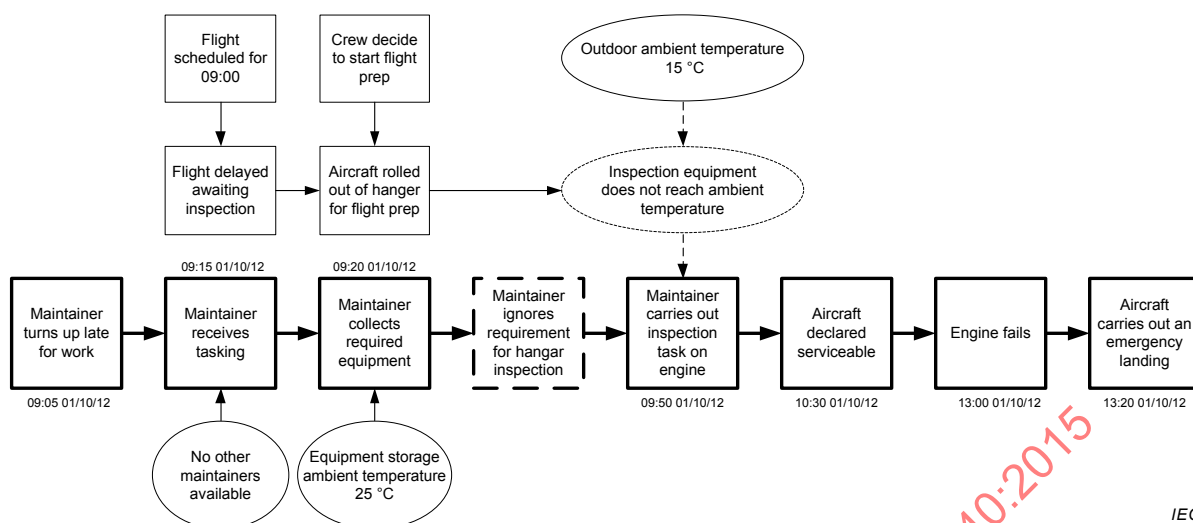
En règle générale, l'identification des facteurs causaux nécessaires sera répétable et basée sur des preuves. Il peut y avoir un niveau plus élevé de subjectivité dans l'identification des facteurs contributifs et des techniques d'analyse différentes avec un accent différent pourront identifier des facteurs différents.

C.2 Graphique des événements et des facteurs causaux (ECF)

C.2.1 Vue d'ensemble

Le graphique ECF [9] enregistre les événements dans l'ordre chronologique de gauche à droite dans des rectangles, avec des événements caractérisés par des sujets uniques et des verbes actifs. Chaque événement est dérivé strictement du précédent. Les conditions nécessaires pour les événements sont affichées dans des formes ovales au-dessus et au-dessous de la séquence d'événements (les conditions sont des états ou des circonstances plutôt que des événements.) Les événements sont connectés par des lignes pleines et les conditions par des lignes en pointillés. Les événements et les conditions basés sur des preuves ont un contour plein alors que les événements et les conditions basés sur des présomptions ont un contour en pointillés. Il peut y avoir plusieurs séquences ou branches d'événements, chacune avec ses propres conditions.

La Figure C.1 illustre un exemple de graphique ECF, dans lequel une activité de maintenance a été effectuée de façon incorrecte parce que l'agent d'entretien est arrivé en retard, ce qui a provoqué un atterrissage en urgence d'un avion.



IEC

Légende

Anglais	Français
Flight scheduled for 09:00	Vol planifié pour 09:00
Flight delayed awaiting inspection	Vol retardé en attente de l'inspection
Crew decide to start flight prep	L'équipage décide de démarrer les préparatifs du vol
Aircraft rolled out of hanger for flight prep	Avion sorti du hangar pour les préparatifs du vol
Outdoor ambient temperature 15 °C	Température ambiante extérieure 15 °C
Inspection equipment does not reach ambient temperature	L'équipement d'inspection n'a pas atteint la température ambiante
Maintainer turns up late for work 09:05 01/10/12	L'agent d'entretien arrive en retard au travail 09:05 01/10/12
No other maintainers available	Aucun autre agent d'entretien disponible
09:15 01/10/12 Maintainer receives tasking	09:15 01/10/12 L'agent d'entretien reçoit la tâche
Equipment storage ambient temperature 25 °C	Température ambiante du stockage de l'équipement 25 °C
09:20 01/10/12 Maintainer collects required equipment	09:20 01/10/12 L'agent d'entretien récupère l'équipement requis
Maintainer ignores requirement for hangar inspection	L'agent d'entretien ignore l'exigence d'inspection du hangar
Maintainer carries out inspection task on engine 09:50 01/10/12	L'agent d'entretien effectue la tâche d'inspection sur le moteur 09:50 01/10/12
Aircraft declared serviceable 10:30 01/10/12	L'avion est déclaré fonctionnel 10:30 01/10/12
Engine fails 13:00 01/10/12	Défaillance du moteur 13:00 01/10/12
Aircraft carries out an emergency landing 13:20 01/10/12	L'avion effectue un atterrissage d'urgence 13:20 01/10/12

Figure C.1 – Exemple de graphique ECF

C.2.2 Processus

Voici une description du processus de développement d'un graphique ECF:

- a) Identifier l'événement d'accent et l'enregistrer dans une zone sur la droite.
- b) Enregistrer la chaîne de base des événements qui ont conduit à l'événement d'accent; chaque événement de la chaîne et immédiat et nécessaire pour l'événement sur la droite. La conséquence est donc enregistrée sur la droite de chaque événement (facteur causal). De même, la conséquence d'un événement précédent peut en outre être le facteur causal d'un événement suivant. Les événements sont affichés dans des rectangles reliés par des flèches sur la droite de l'événement d'accent.
- c) Déterminer les conditions qui ont conduit à ces événements. Indiquer chacune d'entre elles dans une forme ovale au-dessus de l'événement concerné.
- d) Ajouter toute chaîne secondaire d'événement qui peut être utile pour l'événement d'accent et ses conditions.
- e) Vérifier la validité des facteurs causaux via des preuves qui déterminent si les conditions et les événements sont vrais.
- f) Développer le graphique ECF jusqu'à ce que l'événement au début de la séquence soit identifié et que toutes les conditions qui peuvent être vérifiées par des preuves soient ajoutées.

La chronologie exacte des événements n'est généralement pas connue au début des recherches mais devient plus claire au fur et à mesure que les recherches avancent. Il convient donc d'utiliser une méthode qui permette aux enquêteurs de facilement modifier la séquence d'événements et de conditions quand des informations supplémentaires sont obtenues.

C.2.3 Points forts et limites

Les points forts d'un graphique ECF sont les suivants:

- il aide à la vérification des chaînes causales et des séquences d'événements;
- il fournit une structure pour la collecte, l'organisation et l'intégration des preuves;
- il identifie les informations manquantes;
- il aide à la communication grâce à une aide visuelle efficace qui résume les informations clés sur l'événement d'accent et sur ses causes.

Les limites d'un graphique ECF sont les suivantes:

- il identifie certains facteurs causaux, mais peut ne pas toujours déterminer les causes initiales;
- il peut être trop compliqué pour les problèmes simples.

C.3 Séquençage d'événements multilinéaires (MES) et restitution d'événements successifs (STEP)

C.3.1 Vue d'ensemble

Le MES [10] et la STEP [11] sont des méthodes développées pour analyser les événements d'accents dans des systèmes complexes, où la STEP est un successeur du MES.

Comme pour le graphique ECF, la méthode MES/STEP conçoit un événement d'accent comme provenant d'une succession d'événements associés avec des événements caractérisés par un sujet unique et un verbe actif. Dans le MES et la STEP, le sujet est appelé un acteur (peut être un humain ou une machine, voire une propriété).

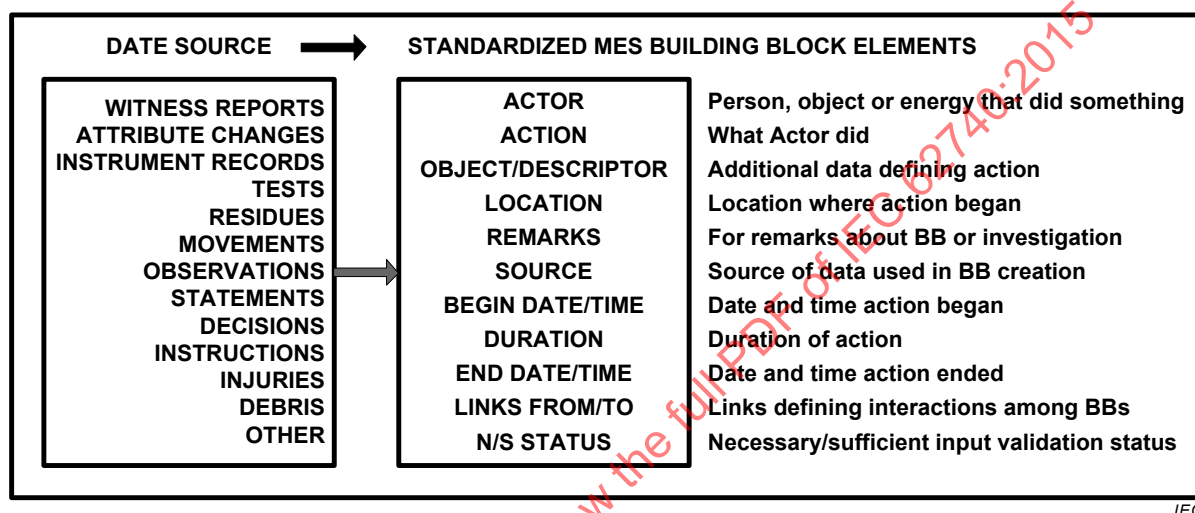
Les événements sont représentés sous forme de modules (BB, building block) d'événements, composés d'enregistrements (partiels ou complets) de données, comme décrit à la Figure C.2. Ils sont arrangés pendant l'analyse dans une matrice chronologie-acteurs dans

laquelle l'axe vertical de la matrice représente les différents acteurs et l'axe horizontal représente la chronologie.

La matrice chronologie-acteurs contient également:

- les conditions nécessaires pour activer un événement, ainsi que les événements précurseurs;
- les annotations de tâches supplémentaires dans une recherche, par exemple une note pour indiquer un déficit d'information ou une explication d'événement incomplète.

Un exemple avec une partie de la représentation d'un événement de maintenance de réservoir est donné à la Figure C.3.



IEC

Légende

Anglais	Français
DATE SOURCE	SOURCE DES DONNEES
STANDARDIZED MES BUILDING BLOCK ELEMENTS	ELEMENTS STANDARDISES DES MODULES MES
WITNESS REPORTS	TEMOIGNAGES
ATTRIBUTE CHANGES	CHANGEMENTS D'ATTRIBUTS
INSTRUMENT RECORDS	ENREGISTREMENTS DES INSTRUMENTS
TESTS	ESSAIS
RESIDUES	RESIDU
MOVEMENTS	MOUVEMENTS
OBSERVATIONS	OBSERVATIONS
STATEMENTS	ENONCES
DECISIONS	DECISIONS
INSTRUCTIONS	INSTRUCTIONS
INJURIES	BLESSURES
DEBRIS	DEBRIS
OTHER	AUTRE

Anglais	Français
ACTOR ACTION OBJECT/DESCRIPTOR LOCATION REMARKS SOURCE BEGIN DATE/TIME DURATION END DATE/TIME LINKS FROM/TO N/S STATUS	ACTEUR ACTION OBJET/DESCRIPTEUR LIEU REMARQUES SOURCE DATE/HEURE DE DEBUT DUREE DATE/HEURE DE FIN LIENS DE/A ETAT N/S
Person, object or energy that did something What Actor did Additional data defining action Location where action began For remarks about BB or investigation Source of data used in BB creation Date and time action began Duration of action Date and time action ended Links defining interactions among BBs Necessary/sufficient input validation status	Individu, objet ou énergie qui a réalisé une action Ce que l'Acteur a fait Données supplémentaires définissant l'action Lieu où a commencé l'action Pour les remarques sur le module ou l'enquête Source des données utilisées dans la création du module Date et heure auxquelles l'action a débuté Durée de l'action Date et heures auxquelles l'action a pris fin Liens définissant les interactions entre les modules Etat de validation de l'entrée Nécessaire/Suffisant

Figure C.2 – Données dans un module d'événement

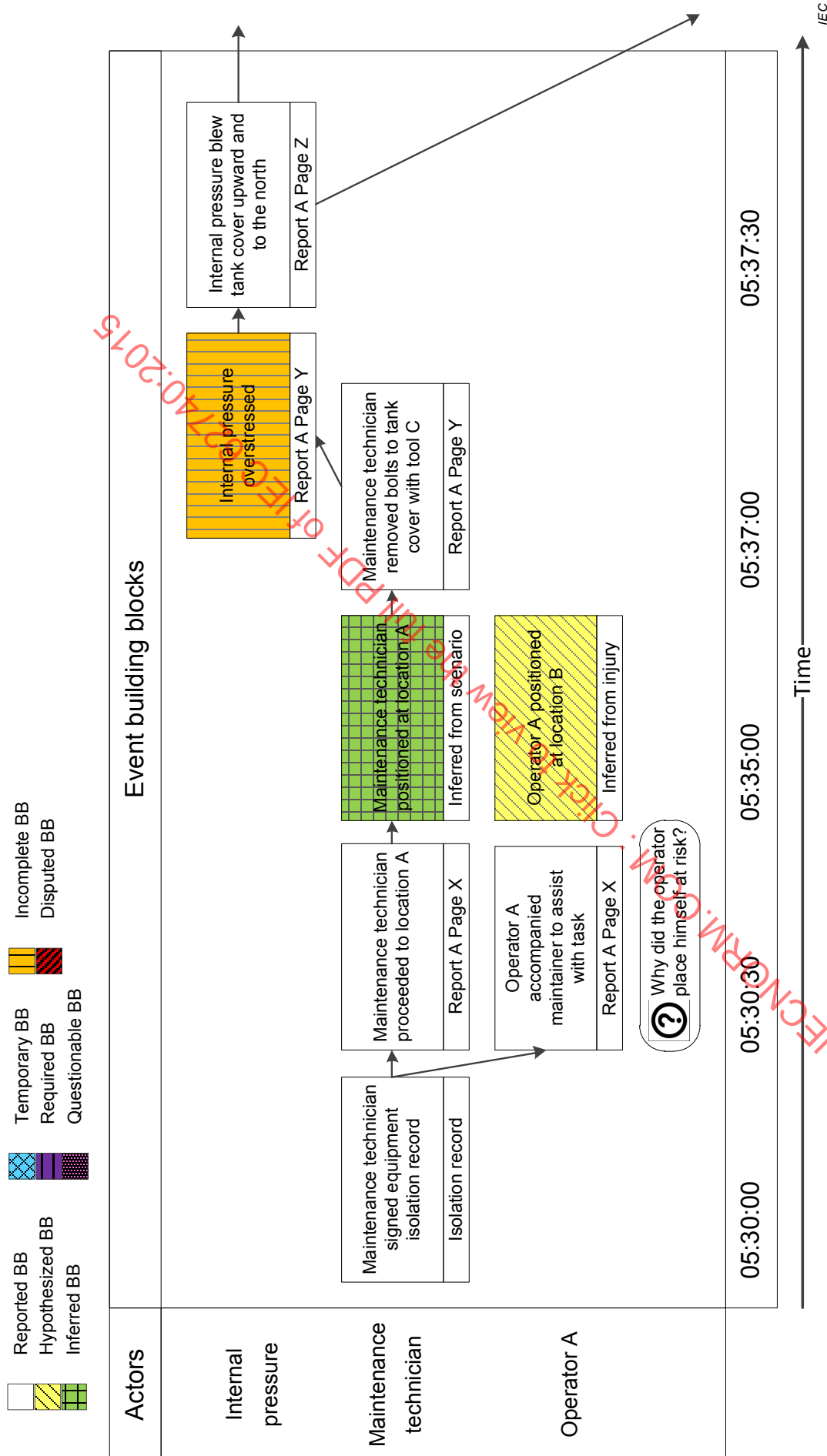
C.3.2 Processus

La méthode MES/STEP comporte les étapes suivantes:

- Regrouper les informations de la série initiale de modules, puis identifier et rechercher les informations manquantes.
- Organiser les modules initiaux dans une matrice chronologie-acteurs.
- Identifier et générer des hypothèses pour "remplir" les écarts avec des événements (sous la forme de nouveaux modules).
- Mettre fin au processus lorsqu'un analyste considère que suffisamment d'informations sont disponibles dans la matrice chronologie-acteurs.

C.3.3 Points forts et limites

La méthode MES/STEP a les mêmes points forts et limites qu'un graphique ECF. Le formatage des données est relativement plus élaboré et il y a des mécanismes explicites pour déterminer et suivre les données manquantes ainsi que les tentatives de détermination de ces données. Certains de ces mécanismes de "comptabilité" sont nécessaires pour gérer des enquêtes complexes avec plusieurs enquêteurs. La matrice chronologie-acteurs est également dotée d'une notation explicite pour enregistrer l'état d'une interrogation en cours ainsi que l'acquisition de données et les tâches explicatives à réaliser. Cela signifie qu'une représentation visuelle compréhensible de l'état d'une enquête est disponible à tout moment au cours d'une enquête.



Légende

Anglais	Français
Reported BB	Module reporté
Hypothesized BB	Module hypothétique
Inferred BB	Module déduit
Temporary BB	Module temporaire
Required BB	Module requis
Questionable BB	Module contestable
Incomplete BB	Module incomplet
Disputed BB	Module contesté
Actors	Acteurs
Event building blocks	Modules de l'événement
Internal pressure	Pression interne
Maintenance technician	Technicien de maintenance
Operator A	Opérateur A
Internal pressure overstressed	Pression interne très élevée
Report A Page Y	Rapport A Page Y
Internal pressure blew tank cover upward and to the north	La pression interne a fait sauter le couvercle du réservoir en l'air, puis vers le nord
Report A Page Z	Rapport A Page Z
Maintenance technician signed equipment isolation record	Le technicien de maintenance a signé le rapport d'isolation de l'équipement
Isolation record	Rapport d'isolation
Maintenance Technician proceeded to location A	Le technicien de maintenance se dirige vers le point A
Report A Page X	Rapport A Page X
Maintenance technician positioned at location A	Le technicien de maintenance se tient sur le point A
Inferred from scenario	Déduit du scénario
Maintenance technician removed bolts to tank cover with tool C	Le technicien de maintenance retire les boulons du couvercle du réservoir avec l'outil C
Report A Page Y	Rapport A Page Y
Operator A accompanied maintainer to assist with task	L'opérateur A accompagne le technicien de maintenance pour l'aider dans sa tâche
Report A Page X	Rapport A Page X
Operator A positioned at location B	L'opérateur A se tient sur le point B
Inferred from injury	Déduit de la blessure
Why did the operator place himself at risk?	Pourquoi l'opérateur s'est-il mis dans une situation risquée?
Time	Heure

Figure C.3 – Exemple de matrice chronologie-acteurs**C.4 Méthode du 'pourquoi'****C.4.1 Vue d'ensemble**

La méthode du pourquoi utilise un processus de questionnement pour mener aux causes initiales.

Le questionnement démarre par un énoncé sur la situation et demande pourquoi elle s'est produite. La réponse à cette question est utilisée pour une deuxième question pourquoi, dont la réponse est utilisée pour une troisième question pourquoi. Le questionnement cesse lorsque la règle d'arrêt est atteinte. Cela exige généralement 5 niveaux de questions; la méthode est donc appelée 5 pourquoi.

Lorsqu'une question pourquoi fournit plusieurs facteurs causaux, chacun d'eux est exploré et la méthode produit un arbre de pourquoi.

La méthode du pourquoi est utilisée seule pour des situations simples, mais est également inhérente dans des méthodes d'arbres plus complexes telles que la méthode de l'arbre des causes (CTM) (voir l'Article C.5). Elle peut être utile pour soutirer des informations aux témoins sur la façon et la raison de la survenue d'un événement puisqu'une simple question 'pourquoi' n'induit aucune hypothèse sur la cause ou n'oriente pas le témoin.

La Figure C.4 illustre l'exemple d'un compresseur qui a subi un arrêt non planifié. Dans l'exemple, les quatre pourquoi suggéraient de nombreux facteurs causaux potentiels pour le manque de lubrification et des preuves ont été recherchées pour définir laquelle s'est produite. Bien qu'une erreur humaine était impliquée dans le sens où un individu n'a pas respecté les procédures de démarrages spécifiées, la recommandation est d'améliorer la conception afin que les moteurs du compresseur et de la pompe soient liés. Dans ce cas, une analyse approfondie des raisons de l'erreur n'est pas utile.



IEC

Légende

Anglais	Français
Focus event	Événement d'accent
Compressor experiences unscheduled shut down	Arrêt non planifié du compresseur

Anglais	Français
Why 1 Shut down by automatic control system	Pourquoi 1 Arrêté par le système de contrôle automatique
Why 2 Bearing overheated	Pourquoi 2 Roulement surchauffé
Why 3 Lack of lubrication	Pourquoi 3 Manque de lubrification
Why 4	Pourquoi 4
Restricted lubrication flow Not a cause Log sheets showed normal pressure differentials	Flux de lubrification restreint N'est pas une cause Le journal montre des différentiels de pression normaux
Lubrication leak Not a cause Inspection showed no leaks	Fuite du lubrifiant N'est pas une cause L'inspection n'a trouvé aucune fuite
Lubrication pump not running	La pompe de lubrification ne fonctionnait pas
Lubrication oil level low	Niveau bas de l'huile de lubrification
Why 5	Pourquoi 5
Not switched on by maintenance person	Pas activée par le technicien de maintenance
Not switched on automatically	Pas activée automatiquement
Why 6 Maintenance person knew but forgot that particular compressor needed separate activation of lube oil	Pourquoi 6 Le technicien de maintenance savait que ce compresseur nécessitait une activation séparée de l'huile de lubrification, mais l'avait oublié
Why 6 Designed to have separate manual operation	Pourquoi 6 Conçu pour la réalisation de certaines opérations manuellement

Figure C.4 – Exemple d'arbre de pourquoi

C.4.2 Processus

La méthode du pourquoi comprend les étapes suivantes:

- Identifier et enregistrer l'événement d'accent comme le point de départ d'un diagramme de pourquoi.
- Demander pourquoi l'événement d'accent s'est produit, en ne recherchant que les facteurs causaux immédiats.
- Demander "pourquoi" successivement en fonction de la réponse précédente. Il convient dans tous les cas que la réponse à la question "pourquoi" soit un facteur causal immédiat de la réponse précédente.

La question "pourquoi" est posée à de nombreuses reprises; en effet, elle est nécessaire pour conduire à une cause initiale. On compte normalement cinq questions, mais cela n'est qu'une ligne directrice. A chaque fois que la question est posée, il peut y avoir plusieurs réponses. Une analyse supplémentaire sera nécessaire pour éliminer ces réponses possibles si elles ne sont pas applicables. Il peut être plus efficace de demander "pourquoi le processus a-t-il échoué?" et pas juste "pourquoi"?

Il peut être utile de prendre en compte un ensemble de catégories de causes telles que celles de la méthode Ishikawa et d'impliquer une équipe de plusieurs individus. Cela permettra d'assurer que tous les domaines pertinents sont pris en compte par les enquêteurs.

C.4.3 Points forts et limites

Les points forts de la méthode du pourquoi sont les suivants:

- elle est simple à appliquer pour ceux concernés par le problème;
- elle est facile à comprendre pour les autres;
- le processus est rapide pour obtenir des résultats pour les problèmes simples;
- elle n'exige pas de connaissances étendues de la part de la personne qui pose les questions;
- elle n'exige pas beaucoup de formation de la part de la personne qui pose les questions.

Les limites de la méthode du pourquoi sont les suivantes:

- elle n'est adaptée qu'à des situations simples;
- elle dépend fortement des connaissances et de l'expertise des personnes qui répondent aux questions, avec une expertise dans les modes de défaillance technique et d'erreur humaine souvent exigée pour atteindre les causes initiales;
- les causes initiales risquent fortement d'être manquées si elles ne font pas partie des connaissances de base des personnes concernées;
- un certain niveau d'incertitude est possible sur le moment auquel les causes initiales appropriées ont été identifiées;
- elle peut être développée à un niveau où les raisons des actions des intervenants sont prises en compte, où les preuves ne sont pas toujours disponibles et où les résultats ne sont donc pas toujours répétables.

C.5 Méthode de l'arbre des causes (CTM)

C.5.1 Vue d'ensemble

La CTM [12] est une technique systématique pour l'analyse et la représentation graphique des événements et conditions qui ont contribué à un événement d'accent.

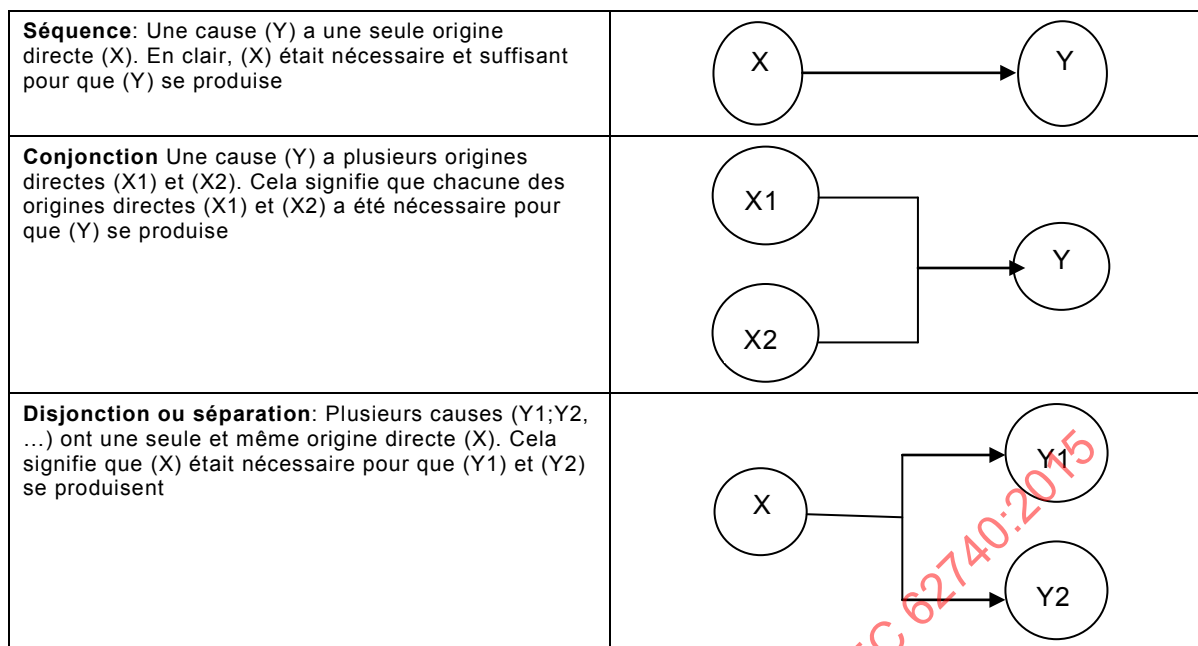
La méthode examine tous les composants du système associés à l'événement d'accent. L'enquête débute par l'établissement de faits tangibles, en prenant soin, au cours de cette étape, de ne pas les interpréter ou de ne pas exprimer d'opinion à leur égard.

La méthode CTM est similaire à la méthode du pourquoi dans la théorie; elle élabore cependant un arbre plus complexe et prend en compte explicitement les facteurs causaux techniques, organisationnels, humains et environnementaux. Chaque antécédent (facteur causal identifié) est soumis à l'essai pour vérifier qu'il s'agit d'un facteur causal immédiat et nécessaire de la précédente, alors que la méthode du pourquoi est moins rigoureuse. Ainsi, la CTM est adaptée à des situations plus complexes.

La CTM est également similaire à un arbre de panne, mais, bien qu'un arbre de panne soit utilisé avant un événement pour explorer toutes les facteurs causaux causes possibles et les relations logiques strictes entre les pannes spécifiées, l'arbre des causes inclut uniquement les facteurs causaux qui s'appliquent à un événement spécifique déjà survenu et ne développe pas les relations logiques en détail.

Un arbre de cause peut être utilisé pour explorer les réussites et les défaillances.

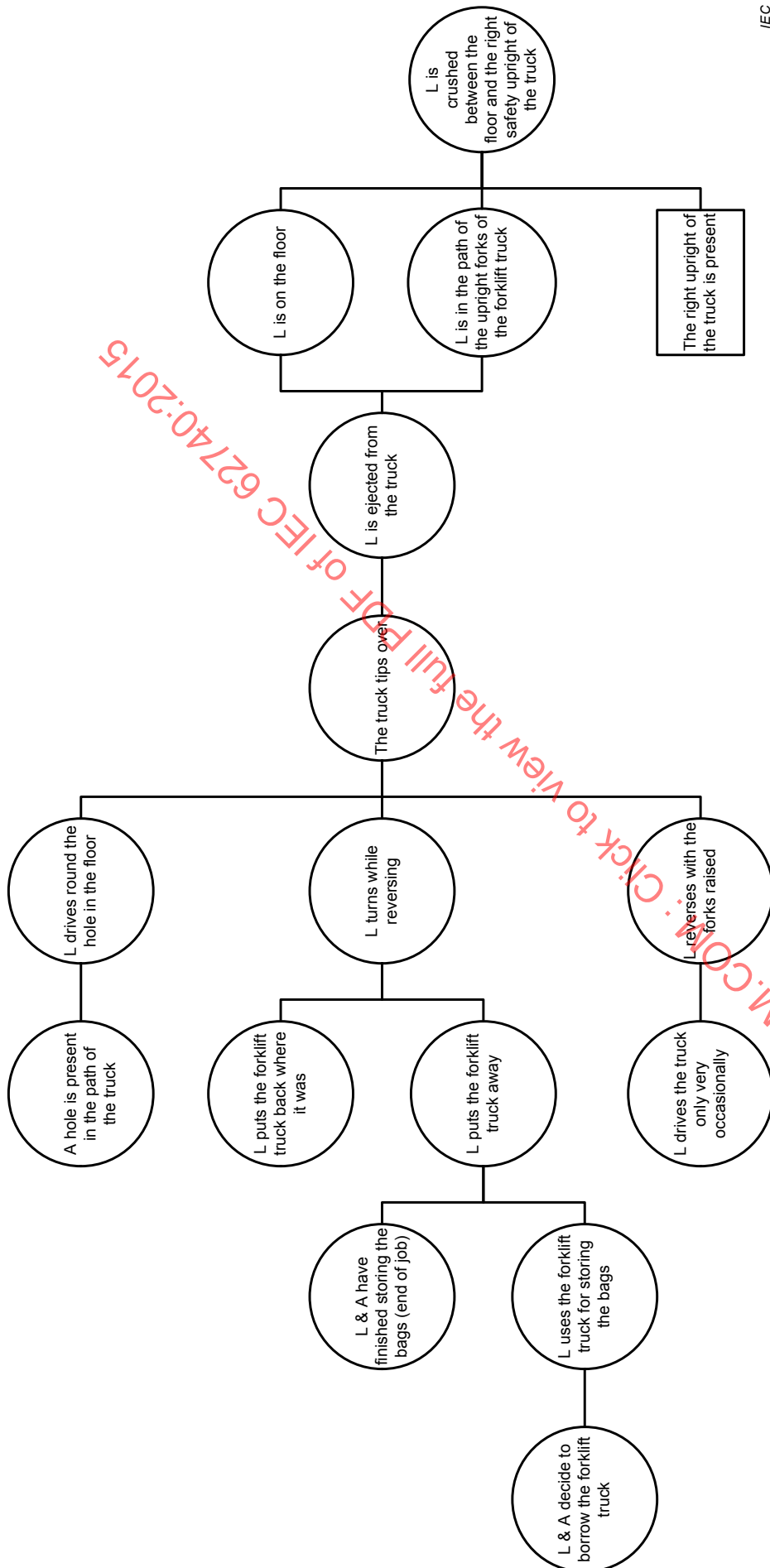
L'arbre de cause élabore un réseau des causes qui ont induit directement ou indirectement l'événement d'accent, à l'aide des relations logiques de l'arbre illustrées à la Figure C.5.



IEC

Figure C.5 – Symboles et liens utilisés dans la CTM

La Figure C.6 montre un arbre d'exemple, dans lequel M. L (la victime) et M. A travaillent de nuit, de façon exceptionnelle, pour stocker un surplus de stock. Conformément au manuel, il était exigé que M. L et M. A chargent le concasseur avec de la "farine" qui devait ensuite être mise en sac et stockée. Normalement, cette activité est sous la responsabilité d'un chef d'équipe dont la présence n'a pas été considérée comme essentielle par la direction pour cette nuit. Sur sa propre initiative et afin de gagner du temps, M. L a pris un chariot élévateur (la clé de démarrage était restée sur le tableau de bord comme d'habitude) pour stocker les sacs. A la fin de la tâche, M. L a décidé de remettre le chariot élévateur à sa place. M. L a effectué un virage serré en marche arrière, les fourches se sont levées, et alors qu'il cherchait à éviter un trou dans le sol, le chariot s'est renversé, écrasant M. L entre le sol et le montant de sécurité droit du chariot.



IEC

Légende

Anglais	Français
L and A decide to borrow the forklift truck	L et A décident d'emprunter le chariot élévateur
L uses the forklift truck for storing the bags	L utilise le chariot élévateur pour stocker les sacs
L and A have finished storing the bags (end of job)	L et A ont terminé le stockage des sacs (fin de la tâche)
L drives the truck only very occasionally	L ne conduit le chariot que très rarement
L puts the forklift truck away	L déplace le chariot élévateur
L puts the forklift truck back where it was	L remet le chariot élévateur à sa place
A hole is present in the path of the truck	Un trou est présent sur le chemin du chariot
L drives round the hole in the floor	L contourne le trou dans le sol
L turns while reversing	L tourne alors qu'il est en marche arrière
L reverses with the forks raised	L se met en marche arrière avec les fourches levées
The truck tips over	Le chariot se renverse
L is ejected from the truck	L est éjecté du chariot
L is on the floor	L est sur le sol
L is in the path of the upright forks of forklift truck	L est sur le chemin des fourches verticales du chariot élévateur
The right upright of the truck is present	Le montant droit du chariot est présent
L is crushed between the floor and the right safety upright of the truck	L est pris en tenailles entre le sol et le montant de sécurité droit du chariot

Figure C.6 – Exemple d'arbre de cause**C.5.2 Processus**

La CTM a les étapes suivantes.

- Identifier l'événement d'accident à analyser et l'enregistrer comme point de départ pour l'arbre.
- Collecter et enregistrer toutes les données pertinentes y compris les individus, leurs activités et leurs actions, les matériaux, l'équipement et les facteurs relatifs à l'environnement physique et psychosocial.
- Etablir une liste des facteurs causaux de l'événement d'accident. Il convient qu'ils soient supportés par des preuves et qu'ils soient exprimés aussi précisément que possible. Les opinions et jugements subjectifs ne sont pas inclus. Les facteurs causaux incluent les facteurs qui ne sont pas habituels ou changent le cours normal des événements et les facteurs qui sont normaux, mais qui ont joué un rôle actif dans la survenue de l'événement.
- Pour remonter la suite des événements jusqu'aux causes initiales, poser systématiquement les questions suivantes pour chaque antécédent qui a été collecté:
 - quel antécédent X a causé directement l'antécédent Y?;
 - X était-il lui-même exigé pour donner lieu à Y? ;
 - si ce n'est pas le cas, quels autres antécédents (X1, X2, etc.) étaient également nécessaires afin de donner lieu directement à Y?
- Afficher ces facteurs causaux nécessaires immédiats dans une case liée par une flèche à l'événement d'accident. (L'arbre peut être dessiné horizontalement ou verticalement, mais est habituellement dessiné horizontalement à partir de la droite, de façon que la lecture de gauche à droite corresponde à la chronologie des événements).
- Continuer de poser les mêmes questions pour chaque facteur causal nécessaire trouvé jusqu'à ce que l'équipe s'accorde sur le fait qu'il soit inutile de poursuivre.

g) Vérifier la validité de l'arbre via des preuves supplémentaires qui déterminent s'il est vrai.

C.5.3 Points forts et limites

Les points forts de la CTM sont les suivants:

- elle fournit une méthode pour structurer les recherches dans les événements complexes;
- elle facilite la lecture du format;
- elle peut être utilisée pour encourager la participation du groupe;
- elle identifie des zones pour la collecte des données au fur et à mesure que les recherches avancent;
- elle peut être utilisée pour analyser les événements de réussite ou de panne;
- elle peut être utilisée pour les événements techniques et non techniques.

Les limites de la CTM sont les suivantes:

- beaucoup de facteurs humains et organisationnels peuvent contribuer à la survenue de l'événement d'accent et il est souvent difficile d'établir lesquels étaient les facteurs causaux nécessaires dans une instance particulière;
- il n'y a pas de lignes directrices sur la façon de rechercher les facteurs causaux; une expertise en erreur humaine et en système organisationnel est donc nécessaire quand l'arbre concerne les défaillances humaines et organisationnelles, où des preuves sont souvent difficiles à obtenir;
- elle est difficile à appliquer quand un événement se produit suite au changement de qualité dans plusieurs domaines, où aucun facteur causal unique n'est un facteur causal nécessaire.

C.6 Etude des facteurs de causalité (WBA)

C.6.1 Vue d'ensemble

La WBA [13] est une technique d'analyse de causalité qui établit lesquels d'un ensemble donné d'événements et de situations sont des facteurs causaux nécessaires. Pour deux événements ou situations donnés, par exemple A et B, une condition appelée l'essai contrefactuel (CT) est utilisée pour établir si A est un facteur causal nécessaire de B. Supposons que deux événements ou situations A et B ont été observés. Le CT demande si, dans le cas où A ne se serait pas produit, B aurait eu lieu ou non. (Puisque A s'est réellement produit, la supposition dans laquelle A ne se serait pas produit est contraire au fait, d'où le mot "contrefactuel".) En posant cette question, il est considéré que toutes les autres conditions sont restées les mêmes. Si la réponse est oui: B n'aurait pas eu lieu, alors A est un facteur causal nécessaire de B. Si la réponse est non: B aurait pu avoir lieu quoi qu'il en soit, même si A ne s'était pas produit (défaillance du CT), alors A n'est pas un facteur causal nécessaire de B.

Le réseau des facteurs causaux est affiché sous la forme d'un graphique des facteurs de causalité (WBG), un ensemble de "nœuds", de cases, de diamants et d'autres formes contenant une brève description du fait, liés par des "traits" ou des flèches, où le nœud à la pointe d'une flèche est un facteur causal nécessaire du nœud au départ de la flèche, tel que déterminé par le CT.

Une WBA est acyclique (ne contient pas de boucles), elle est donc habituellement dessinée avec des flèches pointant généralement vers le haut, comme le montre la Figure C.7, ou horizontalement avec des flèches pointant généralement de gauche à droite ou de droite à gauche

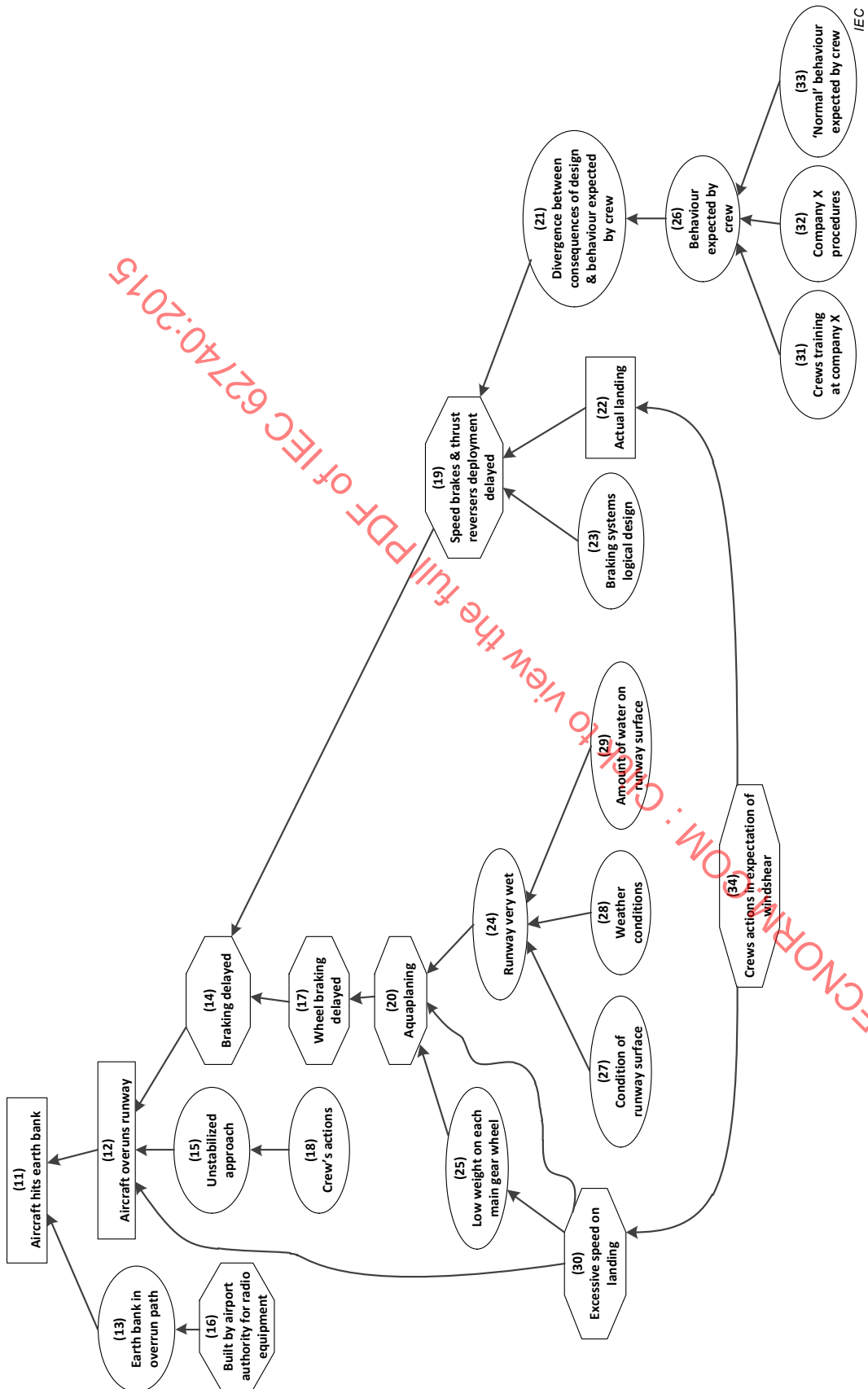
Afin de déterminer si suffisamment de facteurs causaux sont présents dans l'ensemble des événements et de situations présenté, l'essai de complétude des causes (CCT) est réalisé. Le CCT est appliqué à un événement ou à une situation donnée et à l'ensemble de facteurs causaux nécessaires tel que déterminé par le CT. Si le CCT n'est pas réussi, alors l'ensemble

des événements et situations doit être étendu par davantage de facteurs jusqu'à ce que le CCT soit réussi. Supposons qu'il a été déterminé que $A_1, A_2, \dots, A_n$ sont des facteurs causaux nécessaires de B par le CT. Le CCT est donc supposé être réussi, si B ne s'était pas produit, si un des $A_1, A_2, \dots, A_n$ ne s'était pas non plus produit (officiellement, NOT-B est un facteur causal nécessaire de NOT (A_1 AND A_2 AND ... AND A_n)) comme déterminé par le CT).

Lorsqu'un WBG a été élaboré et que le CCT est réussi pour tous les événements et toutes les situations qui le composent, alors le WBG est complet et est supposé représenter une explication causale suffisante de l'événement d'accent.

La Figure C.7 illustre un exemple de WBG pour un accident de dépassement de piste d'un avion commercial.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015



Légende

Anglais	Français
(11) Aircraft hits earth bank	L'avion heurte le talus
Aircraft overruns runway	L'avion dépasse la piste
Earth bank in overrun path	Talus sur la piste
Braking delayed	Freinage retardé
Unstabilized approach	Approche non stabilisée
Built by airport authority for radio equipment	Elaboré par les autorités de l'aéroport pour l'équipement radio
Wheel braking delayed	Freinage des roues retardé
Crew's actions	Actions de l'équipage
Speed brakes and thrust reversers deployment delayed	Utilisation des freins et déploiement des inverseurs de poussée retardés
Aquaplaning	Aquaplanage
Divergence between consequences of design and behaviour expected by crew	Divergence entre les conséquences de la conception et du comportement attendues par l'équipage
Actual landing	Atterrissage
Braking systems logical design	Conception logique des systèmes de freinage
Runway very wet	Piste très mouillée
Low weight on each main gear wheel	Faible poids sur chaque roue du train principal
Behaviour expected by crew	Comportement attendu par l'équipage
Condition of runway surface	Condition de la surface de la piste
Weather conditions	Conditions atmosphériques
Amount of water on runway surface	Quantité d'eau sur la surface de la piste
Excessive speed on landing	Vitesse excessive à l'atterrissage
Crews training at company X	Formation des équipages dans la société X
Company X procedures	Procédures de la société X
'Normal' behaviour expected by crew	Comportement 'normal' attendu par l'équipage
Crews actions in expectation of windshear	L'action des équipages et la préparation à un cisaillement de vent

Figure C.7 – Exemple de WBG**C.6.2 Processus**

La WBA a les étapes suivantes:

- Déterminer un ensemble de faits supposés être pertinents, selon les lignes directrices d'une règle d'arrêt. Ceci établit un ensemble initial de faits C, composé d'événements, d'états et de situations.
- Sélectionner l'événement d'accent (appelé l'événement d'accident dans la WBA).
- Déterminer intuitivement les facteurs causaux nécessaires immédiats de l'événement d'accent à partir de l'ensemble C; contrôler à l'aide du CT. Afficher visuellement les résultats dans un WBG partiel.
- Déterminer intuitivement les facteurs causaux nécessaires des facteurs immédiats; contrôler à l'aide du CT. Etendre le WBG avec ces facteurs.
- Poursuivre pour remplir l'analyse (pour étendre le WBG) en soumettant à l'essai chaque fait dans C par rapport aux facteurs déjà présents dans le WBG.
- Appliquer le CCT pour déterminer si le WBG est complet ou si des facteurs sont manquants dans l'ensemble C.

- g) Etendre C si nécessaire; incorporer les nouveaux faits dans le WBG à l'aide du CT. Si suffisamment d'informations sont disponibles, des hypothèses peuvent être incluses, à condition qu'elles soient clairement identifiées en tant que telles.
- h) Conclure lorsque le CCT affiche suffisamment de facteurs causaux pour chaque fait, conformément à la règle d'arrêt. Si un nombre insuffisant de faits est disponible, des hypothèses doivent être incluses afin de permettre au CCT de réussir, à condition que les hypothèses soient clairement identifiées en tant que telles.

C.6.3 Points forts et limites

Les points forts de la WBA sont les suivants:

- peut être réalisée avec une formation minimale (avec l'utilisation d'outils adaptés qui fournissent une aide à l'extraction des faits à partir de descriptions narratives; un analyste inexpérimenté peut généralement obtenir une WBA réussie en deux heures).
- les résultats de l'analyse sont facilement compréhensibles par des tiers.
- l'expérience conceptuelle exigée pour effectuer une WBA est limitée (il faut que l'analyste puisse appliquer le CT, puis le CCT);
- tout réseau de phénomènes de causalité peut être analysé via une WBA;
- le raisonnement soutenant une WBA peut être vérifié formellement à l'aide d'une logique formelle.
- peut être utilisée de concert avec d'autres méthodes; par exemple celles fournissant plus de structure à l'ensemble des faits.

Les limites de la WBA sont les suivantes:

- la méthode ne fournit pas de lignes directrices pour la collecte des faits auxquels les essais sont appliqués, par exemple il n'y a aucune organisation des faits en catégories telles que technique, procédure, facteurs humains, organisation, juridique;
- parce que les faits ne sont pas structurés, la WBA fournit des lignes directrices limitées sur l'action corrective, dans le cas où la récurrence doit être évitée.

C.7 Méthode de l'arbre de panne et de l'arbre de réussite

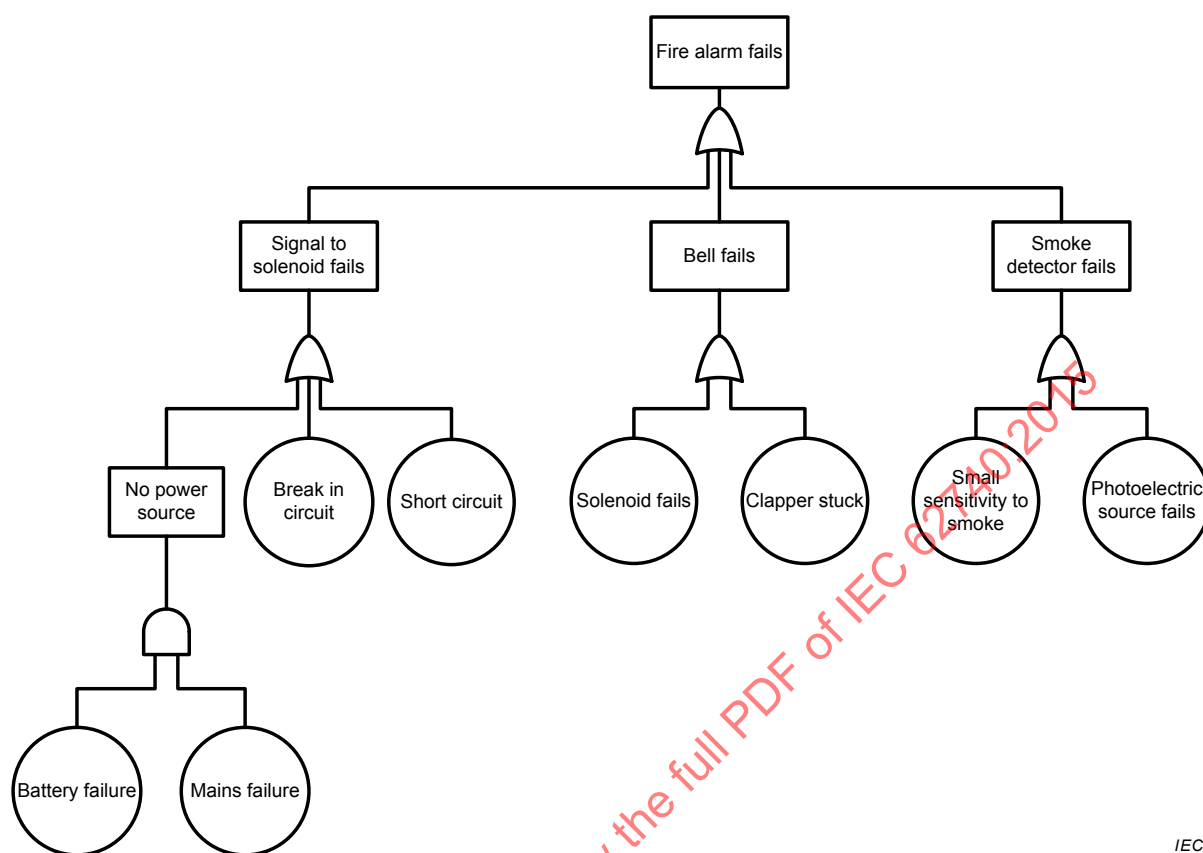
C.7.1 Vue d'ensemble

Un arbre de panne [14] affiche les facteurs de cause nécessaire immédiats d'un événement d'accent, leurs prédécesseurs causaux et les relations logiques entre eux. L'analyse par arbre de panne (FTA) [15] est normalement utilisée comme méthode prioritaire d'identification et d'analyse des modes de panne potentiels, en particulier pour l'équipement. Le diagramme d'arbre de panne peut être utilisé dans RCA via l'élaboration d'un arbre avec la même logique, mais avec, au sein de l'arbre, uniquement les événements qui se sont réellement produits. Les portes OR peuvent être utilisées pendant l'analyse pour décrire d'autres facteurs causaux à évaluer, mais, quand tous les faits sont clairement établis, il convient que seules les portes AND soient conservées, à moins que l'objectif de l'enquête soit d'éviter d'autres événements relatifs. Au fur et à mesure que les recherches avancent, les facteurs causaux potentiels qui ne correspondent pas aux preuves sont donc éliminés et supprimés de l'arbre. A la fermeture de chaque branche de l'arbre, les facteurs causaux de l'événement d'accent deviennent apparents.

Au sens strict, un arbre de panne représente des événements binaires pour lesquels un énoncé est vrai ou faux, par exemple un composant a subi une défaillance ou non. Dans la RCA, la structure de l'arbre de panne est souvent appliquée à un arbre de facteurs causaux où les règles logiques ne sont pas strictement respectées et où des modifications de qualité sont prises en compte ainsi que des événements binaires.

Une logique similaire peut être appliquée lorsque l'événement d'accent est une réussite. Dans ce cas, l'arbre est appelé arbre de réussite.

La Figure C.8 est un exemple d'un arbre de panne.



IEC

Légende

Anglais	Français
Fire alarm fails	Défaillance de l'alarme incendie
Signal to solenoid fails	Défaillance du signal vers le solénoïde
Bell fails	Défaillance de la cloche
Smoke detector fails	Défaillance du détecteur de fumée
No power source	Aucune source d'alimentation
Break in circuit	Interruption dans le circuit
Short-circuit	Court-circuit
Solenoid fails	Défaillance du solénoïde
Clapper stuck	Marteau coincé
Small sensitivity to smoke	Sensibilité légère à la fumée
Photoelectric source fails	Défaillance de la source photoélectrique
Battery failure	Défaillance de la batterie
Mains failure	Défaillance des conducteurs principaux

Figure C.8 – Exemple d'arbre de panne pendant l'analyse

C.7.2 Processus

Le processus de développement de la méthode d'arbre de panne/réussite est le suivant:

- Définir l'événement d'accent à analyser et l'enregistrer comme point de départ pour l'arbre.

- b) Etablir les facteurs causaux nécessaires immédiats de l'événement d'accent et les afficher dans une case liée par une flèche à l'événement d'accent. L'arbre peut être dessiné horizontalement ou verticalement. Il s'agit des facteurs causaux de premier niveau de l'événement d'accent.
- c) Etablir les relations logiques entre les facteurs causaux immédiats à l'aide des portes AND et OR. Les événements au niveau des entrées d'une porte AND doivent être nécessaires et suffisants pour causer l'événement ci-dessus. Les portes OR peuvent être utilisées au cours de l'analyse pour décrire les facteurs causaux potentiels qui exigent une enquête.
- d) Examiner chaque facteur causal pour décider s'il s'agit d'une cause initiale ou le résultat de facteurs causaux sous-jacents.
- e) Valider les facteurs causaux potentiels et mettre à jour l'arbre en conséquence.
- f) Poursuivre l'arbre vers le bas jusqu'à ce que la règle d'arrêt soit atteinte.

Lorsque l'arbre est développé, les facteurs causaux possibles liés aux individus, à l'équipement et à l'environnement sont considérés pour chaque facteur causal à chaque niveau. Il convient de ne pas les séparer en haut de l'arbre.

C.7.3 Points forts et limites

Les points forts de la méthode d'arbre de panne/réussite sont les suivants:

- elle fournit une méthode pour diviser l'analyse des grands événements d'accent complexes;
- elle est supportée par de nombreux packages logiciels commerciaux qui aident dans le développement de la structure de l'arbre de panne;
- elle encourage la participation du groupe;
- elle exploite un format ordonné et facile à lire;
- elle identifie les zones de collecte des données.

Les limites de la méthode d'arbre de panne/réussite sont les suivantes:

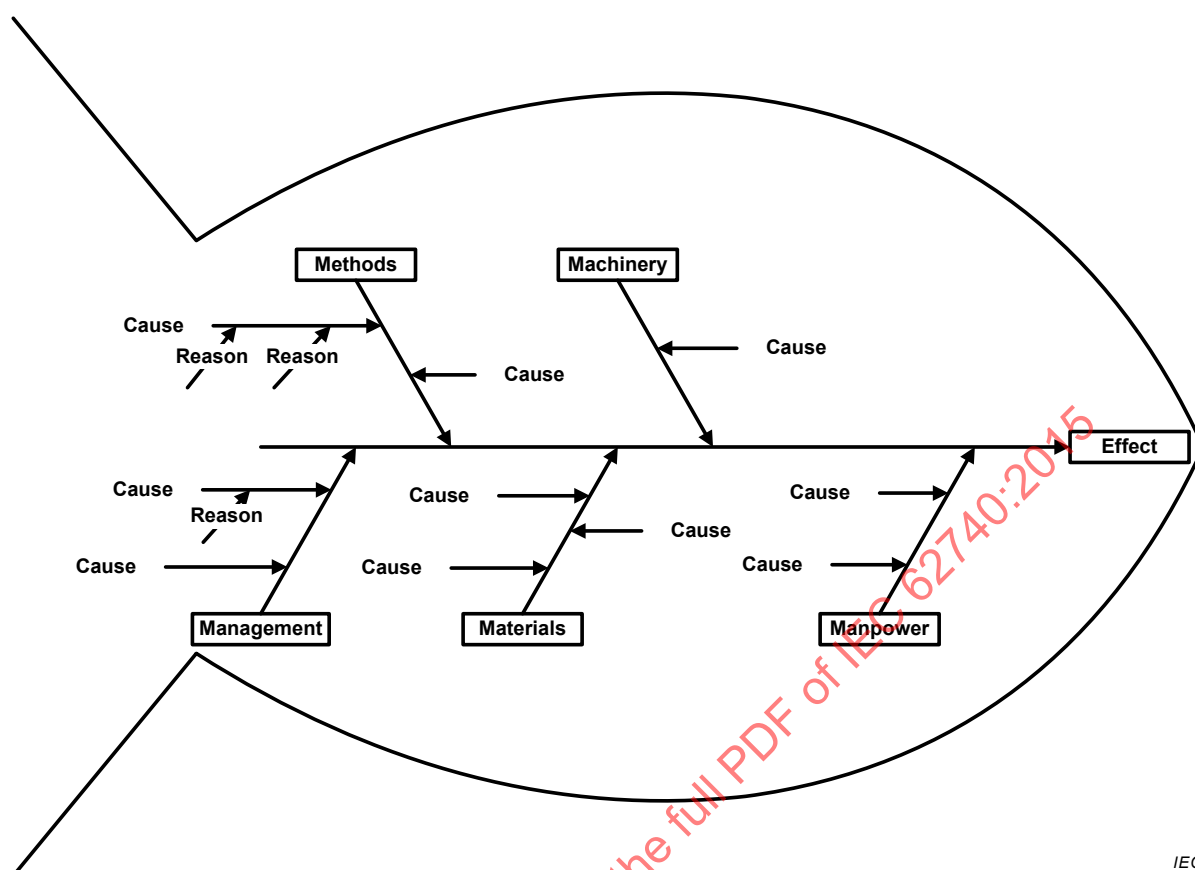
- exige un intervenant expérimenté;
- ne possède aucun modèle de causalité sous-jacent et ne fournit pas de lignes directrices pour la recherche des facteurs causaux;
- ne représente pas facilement les situations où un événement se produit à la suite d'une modification générale de la qualité qui affecte par exemple le respect des procédures ou les tolérances des composants physiques.

C.8 Diagramme d'Ishikawa ou arêtes de poisson

C.8.1 Vue d'ensemble

Le diagramme d'Ishikawa ou arêtes de poisson [16] est une technique qui permet d'identifier, d'analyser et de représenter les causes possibles d'un événement d'accent. Il peut être utilisé pour structurer une session de remue-méninge et pour suggérer des idées si des preuves supplémentaires peuvent être recherchées. La technique a été inventée par Kaoru Ishikawa et illustre de manière graphique la relation entre un événement et tous les facteurs qui l'influencent. Cette technique est aussi appelée "diagramme arêtes de poisson" du fait de son aspect.

La Figure C.9 montre un exemple de diagramme d'Ishikawa ou arêtes de poisson.



IEC

Légende

Anglais	Français
Methods	Méthodes
Machinery	Machines
Cause	Cause
Reason	Raison
Management	Gestion
Materials	Matériaux
Manpower	Main-d'œuvre
Effect	Effet

Figure C.9 – Exemple de diagramme d'Ishikawa ou arêtes de poisson

C.8.2 Processus

Le processus de développement d'un diagramme d'Ishikawa ou arêtes de poisson est le suivant:

- Identifier l'événement d'accent et l'enregistrer sur le côté adéquat et tirer une ligne horizontale à partir de celui-ci. On obtient la tête et la colonne vertébrale d'un poisson.
- Etablir les catégories principales des causes à prendre en compte et tirer des lignes à partir de la colonne pour représenter chaque catégorie. Les catégories communément utilisées incluent:
 - 5M: méthodes, machines, gestion, matériaux, main-d'œuvre;
 - 4P: emplacement, procédures, gens, stratégies;
 - 4S: environs, fournisseurs, systèmes, compétences.

- c) Pour chaque catégorie, identifier les facteurs causaux possibles de l'événement d'accent. Elles sont représentées par des lignes plus petites, qui proviennent des "arêtes" du poisson. Des niveaux de détails encore plus poussés de facteurs causaux peuvent être illustrés grâce à des sous-branches provenant de chaque ligne de cause. Il peut être nécessaire d'éclater le diagramme en plusieurs petits diagrammes si l'une des branches possède trop de sous-branches.
- d) Analyser le diagramme: Le diagramme affiche désormais tous les facteurs causaux possibles de l'événement d'accent. L'étape finale consiste à étudier les facteurs causaux les plus probables qui soumettent à l'essai l'analyse pour vérifier si elle est correcte. L'analyse inclut:
 - 1) la revue de "l'équilibre" du diagramme, en vérifiant avec des niveaux de détails comparables pour identifier le besoin de pousser plus loin l'identification des facteurs causaux;
 - 2) l'identification des facteurs causaux qui apparaissent de façon répétée puisqu'elles peuvent représenter les causes initiales;
 - 3) l'évaluation de ce qui peut être mesuré dans chaque cause afin de quantifier les effets de tout changement apporté;
 - 4) la mise en relief des facteurs causaux pour lesquels des actions peuvent être prises.

C.8.3 Points forts et limites

Les points forts du diagramme d'Ishikawa ou arêtes de poisson sont les suivants:

- elle encourage la participation en groupe pour identifier la perception des facteurs causaux de chaque individu;
- elle recherche les facteurs causaux sous un ensemble de catégories, de façon à identifier un éventail de facteurs causaux liés aux facteurs humains et organisationnels ainsi qu'aux facteurs matériels et procéduraux;
- elle exploite un format ordonné et facile à lire;
- elle indique des facteurs causaux possibles de variation;
- elle peut être utilisée pour des enquêtes simples ou pour un sous-ensemble d'une enquête plus complexe.

Les limites du diagramme d'Ishikawa ou arêtes de poisson sont les suivantes:

- il n'y a aucun modèle sous-jacent ni aucune théorie de causalité, de ce fait les facteurs causaux identifiés sont basés sur la perception des équipes.

C.9 Sécurité via l'apprentissage organisationnel (SOL)

C.9.1 Vue d'ensemble

La SOL [17] est une technique d'analyse d'événement qui recherche les faiblesses du système sociotechnique complexe dans lequel s'est produit l'événement. L'objectif de la SOL est de fournir un modèle du système et d'identifier ses faiblesses pour qu'il puisse être amélioré et que la réapparition de l'événement d'accent soit endiguée. L'accent est mis sur l'apprentissage organisationnel.

C.9.2 Processus

La SOL comporte les étapes suivantes:

- 1) Décrire la situation via une matrice chronologie-acteurs produite par la méthode MES/STEP (voir l'Article C.3).
- 2) Identifier les facteurs causaux (qui peuvent être directs ou indirects, voir Tableau C.1) pour chaque événement dans la matrice chronologie-acteurs, établie à l'aide de listes de contrôle composées de questions tirées de l'expérience et des recherches des auteurs de

la SOL. Les facteurs causaux directs sont ceux qui ont entraîné immédiatement l'événement d'accent; les facteurs causaux indirects apparaissent plus bas dans la chaîne causale, mais peuvent impliquer les mêmes problèmes.

- 3) Classer les facteurs causaux: technologie, individus, groupe de travail, organisation et environnement organisationnel.

Tableau C.1 – Facteurs causaux directs et indirects

Facteurs causaux directs	Facteurs causaux indirects
Informations	Informations
Communication	Communication
Conditions de travail	Conditions de travail
Performances personnelles	Performances personnelles
Infractions	Infractions
Composants techniques	Planification
	Responsabilité
	Contrôle et supervision
	Influence du groupe
	Règles, procédures et documents
	Qualifications
	Formation
	Organisation et gestion
	Principes de sécurité
	Gestion de la qualité
	Maintenance
	Organismes réglementaires et de conseil
	Influences environnementales

C.9.3 Points forts et limites

Les points forts de la SOL sont les suivants:

- le format de la liste de contrôle permet aux utilisateurs qui ne sont pas des spécialistes des systèmes organisationnels ou de la psychologie organisationnelle de produire des analyses utiles;
- l'accent mis sur les facteurs causaux plutôt que sur les facteurs causaux nécessaires permet de prendre en considération plus de facteurs qu'une analyse causale ciblée et offre ainsi plus de chances d'identifier des améliorations possibles;
- le format des modules de l'événement donne un domaine d'application plus strict pour le jugement des analystes individuels et les aide à apporter de l'uniformité aux analyses SOL;
- la règle d'arrêt est définie implicitement par les questions de la liste de contrôle: lorsqu'elles ont obtenu une réponse, l'information est considérée comme étant adéquate.

Les limites de la SOL sont les suivantes:

- il n'y a aucune notion spécifique de ce qu'est un facteur causal à part ce qui est implicite dans les questions de la liste de contrôle;
- le niveau de détail dépend de la liste de contrôle prédéterminée de questions plutôt que du besoin perçu;
- la liste de contrôle de questions est dérivée de recherches dans le secteur du nucléaire et peut être moins adaptée pour d'autres secteurs.

C.10 Arbre de supervision de la gestion et des risques (MORT)

C.10.1 Vue d'ensemble

Le diagramme MORT [18] a été développé initialement pour analyser des causes initiales et les facteurs causaux des incidents des secteurs du nucléaire et de l'aviation aux Etats-Unis, mais s'applique désormais à de nombreux secteurs.

Le diagramme MORT est un arbre prérempli basé sur le modèle d'un système de gestion d'une organisation, qui fournit une liste de contrôle détaillée et efficace pour revoir quelles parties des systèmes de gestion et de contrôle ont eu un état moins qu'approprié lors de la survenue de l'événement d'accent. La structure de l'arbre est illustrée à la Figure C.10.

IECNORM.COM : Click to view the full PDF of IEC 62740:2015