NORME INTERNATIONALE
INTERNATIONAL STANDARD

CEI
IEC
300-3-1

Première édition
First edition
1991–11

Gestion de la sûreté de fonctionnement

Partie 3: Guide d'application
Section 1 : Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique

Dependability management

Part 3: Application guide
Section 1: Analysis techniques for dependability: Guide on methodology

Numéro de référence
Reference number
CEI/IEC 300-3-1: 1991

Validité de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique.

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles auprès du Bureau Central de la CEI.

Les renseignements relatifs à ces révisions, à l'établissement des éditions révisées et aux amendements peuvent être obtenus auprès des Comités nationaux de la CEI et dans les documents ci-dessous:

- **Bulletin de la CEI**
- **Annuaire de la CEI**
  Publié annuellement
- **Catalogue des publications de la CEI**
  Publié annuellement et mis à jour régulièrement

Terminologie

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 50: *Vocabulaire Electrotechnique International* (VEI), qui se présente sous forme de chapitres séparés traitant chacun d'un sujet défini. Des détails complets sur le VEI peuvent être obtenus sur demande. Voir également le dictionnaire multilingue de la CEI.

Les termes et définitions figurant dans la présente publication ont été soit tirés du VEI, soit spécifiquement approuvés aux fins de cette publication.

Symboles graphiques et littéraux

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera:

– la CEI 27: *Symboles littéraux à utiliser en électro-technique;*

– la CEI 417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles;*

– la CEI 617: *Symboles graphiques pour schémas;*

et pour les appareils électromédicaux,

– la CEI 878: *Symboles graphiques pour équipements électriques en pratique médicale.*

Les symboles et signes contenus dans la présente publication ont été soit tirés de la CEI 27, de la CEI 417, de la CEI 617 et/ou de la CEI 878, soit spécifiquement approuvés aux fins de cette publication.

Publications de la CEI établies par le même comité d'études

L'attention du lecteur est attirée sur les listes figurant à la fin de cette publication, qui énumèrent les publications de la CEI préparées par le comité d'études qui a établi la présente publication.

Validity of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information relating to the date of the reconfirmation of the publication is available from the IEC Central Office.

Information on the revision work, the issue of revised editions and amendments may be obtained from IEC National Committees and from the following IEC sources:

- **IEC Bulletin**
- **IEC Yearbook**
  Published yearly
- **Catalogue of IEC publications**
  Published yearly with regular updates

Terminology

For general terminology, readers are referred to IEC 50: *International Electrotechnical Vocabulary* (IEV), which is issued in the form of separate chapters each dealing with a specific field. Full details of the IEV will be supplied on request. See also the IEC Multilingual Dictionary.

The terms and definitions contained in the present publication have either been taken from the IEV or have been specifically approved for the purpose of this publication.

Graphical and letter symbols

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications:

– IEC 27: *Letter symbols to be used in electrical technology;*

– IEC 417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets;*

– IEC 617: *Graphical symbols for diagrams;*

and for medical electrical equipment,

– IEC 878: *Graphical symbols for electromedical equipment in medical practice.*

The symbols and signs contained in the present publication have either been taken from IEC 27, IEC 417, IEC 617 and/or IEC 878, or have been specifically approved for the purpose of this publication.

IEC publications prepared by the same technical committee

The attention of readers is drawn to the end pages of this publication which list the IEC publications issued by the technical committee which has prepared the present publication.

NORME INTERNATIONALE
INTERNATIONAL STANDARD

CEI
IEC
300-3-1

Première édition
First edition
1991– 11

Gestion de la sûreté de fonctionnement

Partie 3: Guide d'application
Section 1: Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique

Dependability management

Part 3: Application guide
Section 1: Analysis techniques for dependability: Guide on methodology

Bureau Central de la Commission Electrotechnique Internationale 3, rue de Varembé Genève, Suisse

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE R

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT

Partie 3: Guide d'application

Section 1: Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique

AVANT-PROPOS

1) Les décisions ou accords officiels de la CEI en ce qui concerne les questions techniques, préparés par des Comités d'Etudes où sont représentés tous les Comités nationaux s'intéressant à ces questions, expriment dans la plus grande mesure possible un accord international sur les sujets examinés.

2) Ces décisions constituent des recommandations internationales et sont agréées comme telles par les Comités nationaux.

3) Dans le but d'encourager l'unification internationale, la CEI exprime le voeu que tous les Comités nationaux adoptent dans leurs règles nationales le texte de la recommandation de la CEI, dans la mesure où les conditions nationales le permettent. Toute divergence entre la recommandation de la CEI et la règle nationale correspondante doit, dans la mesure du possible, être indiquée en termes clairs dans cette dernière.

La présente Norme internationale a été établie par le Comité d'Etudes n° 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

Règle des Six Mois	Rapport de vote
56(BC)138	56(BC)146

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

L'annexe A est donnée uniquement à titre d'information.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT

Part 3: Application guide

Section 1: Analysis techniques for dependability: Guide on methodology

FOREWORD

1) The formal decisions or agreements of the IEC on technical matters, prepared by Technical Committees on which all the National Committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.

2) They have the form of recommendations for international use and they are accepted by the National Committees in that sense.

3) In order to promote international unification, the IEC expresses the wish that all National Committees should adopt the text of the IEC recommendation for their national rules in so far as national conditions will permit. Any divergence between the IEC recommendation and the corresponding national rules should, as far as possible, be clearly indicated in the latter.

This International Standard has been prepared by IEC Technical Committee No. 56: Dependability.

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

Six Months' Rule	Report on Voting
56(CO)138	56(CO)146

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

Annex A is for information only.

INTRODUCTION

Les techniques d'analyse de la sûreté de fonctionnement servent à examiner et prévoir les caractéristiques de fiabilité, de disponibilité, de maintenabilité et de sécurité d'un système.

Les analyses de sûreté de fonctionnement sont surtout effectuées pendant les phases de concept et de définition, de conception et de développement, d'exploitation et de maintenance, à des niveaux différents et avec plus ou moins de détails afin d'évaluer et de déterminer les caractéristiques de sûreté de fonctionnement d'un système ou d'une installation. Elles permettent aussi de confronter les résultats de l'analyse aux exigences prescrites.

INTRODUCTION

Dependability analysis techniques are used for the review and prediction of the reliability, availability, maintainability and safety measures of a system.

Dependability analyses are conducted mainly during the concept and definition phase, the design and development phase, and the operation and maintenance phase at various system levels and degrees of detail in order to evaluate and determine the dependability measures of a system or an installation. They are also used to compare the results of the analysis with specified requirements.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT

Partie 3: Guide d'application

Section 1: Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique

1 Domaine d'application

La présente Norme internationale présente une vue générale des procédures d'analyse de la sûreté de fonctionnement communément employées. Pour ces différentes techniques, elle décrit la méthodologie habituelle, les avantages et les inconvénients, les données d'entrées ainsi que d'autres spécifications.

Ce guide est une introduction à la méthodologie existante. Il est destiné à fournir à l'analyste les informations qui lui sont nécessaires pour choisir les méthodes d'analyse les plus appropriées au système. Des normes disponibles de la CEI donnant des détails sur des méthodes sont indiquées dans le tableau 2.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Tout document normatif est sujet à révision et les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer l'édition la plus récente des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 50(191): 1990, *Vocabulaire Electrotechnique International (VEI), Chapitre 191: Sûreté de fonctionnement et qualité de service.*

CEI 812: 1985, *Techniques d'analyse de la fiabilité des systèmes – Procédures d'analyse des modes de défaillance et de leurs effets (AMDE).*

CEI 1025: 1990, *Analyse par arbre de panne (AAP).*

CEI 1078: 1991, *Technique d'analyse de la sûreté de fonctionnement - Méthode du diagramme de fiabilité.*

3 Définitions

Les termes et les définitions sont conformes au Chapitre 191 du Vocabulaire Electrotechnique International (VEI).

En outre, les définitions suivantes sont applicables pour cette norme:

3.1 **système**: Entité du plus haut niveau considéré dans l'analyse.

3.2 **composant**: Entité du plus bas niveau considéré dans l'analyse.

3.3 **allocation**: Procédure mise en oeuvre pendant la conception d'une entité en vue de répartir les exigences imposées aux caractéristiques relatives à cette entité entre ses sous-entités, conformément à des critères donnés.

NOTE - «Système» peut être remplacé par «sous-système», etc., le cas échéant.

DEPENDABILITY MANAGEMENT

Part 3: Application guide

Section 1: Analysis techniques for dependability: Guide on methodology

1 Scope

This International Standard gives a general overview of commonly used dependability analysis procedures. It describes the usual methodologies, the advantages and disadvantages, data input and other requirements for the various techniques.

This guide is an introduction to the available methodology and is intended to provide the analyst with the necessary information in order to choose the analysis method most appropriate to the system. Available IEC standards, providing details, are indicated in table 2.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent edition of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 50(191): 1990, *International Electrotechnical Vocabulary, Chapter 191: Dependability and quality of service.*

IEC 812: 1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA).*

IEC 1025: 1990, *Fault tree analysis (FTA).*

IEC 1078: 1991, *Analysis techniques for dependability - Reliability block diagram method.*

3 Definitions

Terms and definitions are in accordance with Chapter 191 of the International Electrotechnical Vocabulary.

In addition, the following definitions are applicable for this standard:

3.1 **system**: Item on the highest level considered in the analysis.

3.2 **component**: Item on the lowest level considered in the analysis.

3.3 **allocation**: A procedure applied during the design of an item intended to apportion the requirements for performance measures for an item to its subitems according to given criteria.

NOTE - "System" may be replaced by "sub-system", etc., as applicable.

4 Généralités

Les méthodes d'analyse permettent l'évaluation de caractéristiques qualitatives et l'estimation de caractéristiques quantitatives (par exemple, taux de défaillance, MTTF, MTBF, fiabilité, disponibilité en régime établi) qui décrivent le fonctionnement prévu à long terme d'un système. Afin de réaliser une analyse de système qui soit systématique et reproductible, il est important d'employer une procédure cohérente.

Toutefois, il n'existe pas de méthode d'analyse de la sûreté de fonctionnement qui, seule, soit suffisamment exhaustive et souple pour couvrir toutes les complexités possibles du modèle, indispensables à l'évaluation des caractéristiques de systèmes réels (matériel et logiciel, structure fonctionnelle complexe, diverses technologies, structures réparables et pouvant être entretenues, etc.). Diverses méthodes d'analyse complémentaires devront peut-être être appliquées pour parvenir à une analyse correcte de systèmes complexes ou à fonctions multiples.

5 Analyse de la sûreté de fonctionnement des systèmes: démarche de base

Les procédures spécifiques d'analyse sont données dans les normes décrivant chaque méthode d'analyse. On trouvera dans ce qui suit une description des procédures, démarches et exigences générales.

5.1 *Procédure générale*

La procédure comprend, selon le cas, les étapes suivantes:

Etape 1

Enumérer tous les impératifs et toutes les caractéristiques et propriétés concernant la fiabilité et la disponibilité des systèmes, les conditions ambiantes, les conditions de fonctionnement ainsi que les exigences relatives à l'entretien et aux réparations. Définir le système à analyser et inclure une description de tous les modes de fonctionnement du système et de toutes les relations fonctionnelles jusqu'à des niveaux plus élevés et jusqu'aux processus et systèmes à interface.

Etape 2

Définir la panne du système, les critères et les conditions de panne d'après les impératifs de fonctionnement du système, le fonctionnement attendu et le milieu dans lequel le système fonctionne. Il convient également de tenir compte des performances du logiciel.

Etape 3

Lorsque des résultats numériques sont nécessaires, il est recommandé de procéder à une allocation de la fiabilité en fonction d'une conception préliminaire (attribution à chaque sous-système d'une partie du taux de défaillance ou de l'indisponibilité totale autorisée du système).

4 General

The analysis methods allow the evaluation of qualitative characteristics and estimation of measures (e.g. failure rate, MTTF, MTBF, reliability, steady state availability) which describe the predicted long-term operating behaviour of a system. In order to perform a systematic and reproducible system analysis, use of a consistent procedure is essential.

However, no single dependability analysis method is sufficiently comprehensive and flexible to deal with all the possible model complexities required to evaluate the features of practical systems (hardware and software, complex functional structures, various technologies, repairable and maintainable structures, etc.). It may be necessary to consider several additional analysis methods to ensure proper treatment of complex or multi-functional systems.

5 Basic approach to system dependability analysis

Specific procedures for analysis are contained in the standards describing each analysis method. General procedures, approaches and requirements are described hereinafter.

5.1 *General procedure*

The procedure consists of the following steps (as applicable):

Step 1

List all system reliability and availability requirements, characteristics and features, together with environmental and operating conditions, and maintenance requirements. Define the system to be analyzed, its modes of operation, the functional relationships to higher levels and to interfacing systems or processes.

Step 2

Define system fault, fault criteria and conditions based on system functional requirements, expected operation and operating environment. Software performance should also be considered.

Step 3

When numerical results are required, it is recommended to carry out an allocation based on a preliminary design (assignment of a portion of the total permitted system failure rate or unavailability to each sub-system).

Etape 4

Analyse du système de la manière suivante:

4.1) Analyse qualitative (méthode déductive/inductive):

Analyser la structure fonctionnelle du système, rechercher les modes de panne du système/composants, les mécanismes de défaillance, les effets et les conséquences des défaillances, considérer la maintenabilité des entités, établir un modèle de fiabilité et/ou de disponibilité, mettre au point des stratégies de maintenance et de réparation, etc.

4.2) Analyse quantitative (analytique/simulation d'événements):

Rassembler ou identifier les données de fiabilité des composants (par exemple, taux de défaillance), construire un modèle mathématique de fiabilité et/ou de disponibilité, réaliser une estimation numérique des modèles mathématiques, effectuer une analyse de la criticité des composants et des analyses de sensibilité, estimer l'amélioration des performances du système réalisable grâce à la mise en place de sous-structures redondantes et de stratégies de maintenance, etc.

Etape 5

Evaluation des résultats. Comparer ceux-ci aux exigences ou à ceux qui résultent d'autres conceptions. Parmi les autres actions, on peut citer:

5.1) Examiner la conception du système, identifier les faiblesses, les déséquilibres, les modes de défaillance et les composants critiques/à haut risque, étudier les problèmes d'interface du système, les dispositifs et les mécanismes à sûreté intégrée, etc.;

5.2) Trouver des solutions de rechange pour améliorer la sûreté de fonctionnement (par exemple, attribution de redondance, surveillance des performances, détection des pannes procédure de reconfiguration du système, maintenabilité, possibilité de remplacement et de réparation des composants).

5.3) Réaliser des études de coût/bénéfice et évaluer les coûts de conceptions différentes.

La relation entre la procédure générale d'analyse et les méthodes et procédures spécifiques est donnée dans le tableau 1 qui, toutefois, ne se veut pas exhaustif. Les méthodes sont explicitées ci-après de 5.2 à 5.5.

Step 4

Analysis of the system as follows:

4.1) Qualitative analysis (deductive/inductive methodology):

Analyze the functional system structure, determine system/component fault modes, failure mechanisms, effects and consequences of failures, consider item maintainability, construct reliability and/or availability models, determine possible maintenance and repair strategies, etc.

4.2) Quantitative analysis (analytical or event simulation methods):

Obtain or identify item reliability data (e.g. failure rates), construct mathematical reliability and/or availability models, perform numerical evaluations of mathematical models, perform component criticality and sensitivity analyses, evaluate improvement of system performance due to redundant substructures and maintenance strategies, etc.

Step 5

Evaluation of results, comparison with requirements and/or alternative designs. Additional activities may include:

5.1) Reviewing system design, determining weaknesses, unbalances, critical/high risk fault modes and items, considering system interface problems, fail-safe features and mechanisms, etc.

5.2) Developing alternative ways for improving dependability (e.g. redundancy allocation, performance monitoring, fault detection, system reconfiguration procedures, maintainability, component replaceability, and repair procedures).

5.3) Performing trade-off studies and evaluating the cost of alternative designs.

The relationships between the general analysis procedure and the specific methods and procedures are given in table 1 (note that table 1 is not exhaustive). The methods are explained further in 5.2 to 5.5 inclusive.

Tableau 1 – Correspondance entre les méthodes et la procédure générale d'analyse

Etapes de la procédure générale		Méthodes d'analyse				
N°	Activité	AMPE/AMPEC Analyse des modes de panne et de leurs effets/criticité	AAP Analyse par arbre de panne	DF Diagramme de fiabilité	AGM Analyse par graphe de Markov	PFDP Prévision de fiabilité par décompte des pièces
1	Définition des exigences et du système	Spécification et fonctionnement des composants	Structure fonctionnelle du système	Fonctionnement du système et des sous-systèmes	Fonction des composants, structure fonctionnelle du système	Spécifications des composants et des données relatives aux défaillances
2	Définition de la panne du système	Défaillance du niveau fonctionnel du premier ordre	Evénement indésirable (de tête)	Critère de succès du système (défaillance)	Critère de succès et de défaillance du système	Défaillance du niveau fonctionnel de premier ordre
3	Allocation de la fiabiité	Si applicable aux composants	Si applicable aux sous-systèmes	Si applicable aux sous-systèmes	Si applicable aux sous-systèmes	Si applicable aux composants
4.1	Analyse qualitative et stratégie de maintenance	Inductive (tableau)	Déductive (Arbre de panne)	Déductive (diagramme)	Inductive/déductive (diagramme de transition)	Supposer une structure des systèmes en série, énumérer et évaluer les composants
4.2	Analyse quantitative (Evaluation numérique)	Analyse de la criticité/probabilité de la panne	Calcul des caractéristiques de fiabilité et de disponibilité du système	Calcul des caractéristiques de fiabilité et de disponibilité du système	Calcul des caractéristiques de fiabilité et de disponibilité du système	Calcul des taux de défaillance du système et des composants
5	Exigences satisfaites (fin de la procédure?)	Criticité des défaillances et probabilité de défaillance dans les limites prescrites?	Probabilité de l'événement indésirable conformément aux exigences?	Exigences de fiabilité/disponibilité satisfaites?	Exigences de fiabilité/disponibilité satisfaites?	Le taux de défaillance estimé du système correspond-il aux exigences?
5.1	Revoir la conception et trouver les points faibles	Mode de défaillance des composants, taux de défaillance, etc.	Mode de défaillance des sous-systèmes/ composants, taux de défaillance, structure du système	Fiabilité/disponibilité des sous-systèmes, taux de défaillance des sous-systèmes/ composants, structure du système, etc.	Fiabilité et disponibilité des systèmes/ sous-systèmes, composants, mesures pour la maintenance et la réparation, structure du système	Calculer les plus forts taux de défaillance des composants
5.2	Elaborer d'autres conceptions	Sélection et maintenance des composants, etc.	Structure du système, attribution de redondance, détection de la panne, maintenance, etc.	Structure du système, attribution de redondance, sélection des composants, maintenance, réparation, etc	Structure du système, attribution de redondance, sélection des composants, politique de réparation, nouvelle configuration du système, etc.	Revoir le choix des composants les plus vulnérables
5.3	Faire des études de coût/bénéfice et évaluer le coût des autres conceptions	Déterminer la solution la plus rentable	Déterminer la solution la plus rentable	Déterminer la solution la plus rentable	Déterminer la solution la plus rentable	Evaluer le coût

Table 1 – Correspondence of methods to general analysis procedure

Steps of general procedure		Analysis methods				
No.	Activity	FMEA/FMECA Fault mode and effects/criticality analysis	FTA Fault tree analysis	RBD Reliability block diagram	MA Markov analysis	PC Parts count reliability prediction
1	Requirements and system definition	Component specification and operation	Functional system structure	System and sub-system operation	Component function, functional system structure	Component specification and failure data
2	Definition of system fault	Failure of first order functional level	Undesired (top) event	Criteria of system success (failure)	Criteria of system success and failure	Failure of first order functional level
3	Reliability apportionment	If applicable to components	If applicable to sub-systems	If applicable to sub-systems	If applicable to sub-systems	If applicable to components
4.1	Qualitative analysis, maintenance strategy	Inductive (table)	Deductive (fault tree)	Deductive (block diagram)	Inductive/deductive (state transition diagram)	Assume series system structure, list and evaluate components
4.2	Quantitative analysis (numerical evaluation)	Fault criticality/probability analysis	Calculation of system reliability and availability measures	Calculation of system reliability and availability measures	Calculation of system reliability and availability measures	Calculation of components and system failure rates
5	Requirements met (terminate procedure?)	Criticality of failures and failure probabilities within limits?	Probability of undesired event within requirement?	Reliability/availability requirement met?	Reliability/availability requirements met?	Does estimated system failure rate meet requirements?
5.1	Review design, determine weaknesses	Component failure modes, failure rates etc.	Sub-system/component failure modes, failure rates, system structure etc.	Sub-system reliability/ availability, sub-system/ component failure rates, system structure etc.	Component/sub-system/system reliability and availability, maintenance and repair policy, system structure	Determine highest component failure rates
5.2	Develop alternative designs	Component selection and maintenance etc.	System structure, redundancy allocation, fault detection, maintenance, etc.	System structure, redundancy allocation, component selection, maintenance etc.	System structure, redundancy allocation, component selection, repair policy, system reconfiguration etc.	Re-evaluate choice of weakest components
5.3	Perform trade-off studies and cost-evaluation	Determine most economical solution	Determine most economical solution	Determine most economical solution	Determine most economical solution	Estimate cost

5.2 *Analyse de la structure fonctionnelle*

Il est nécessaire d'établir et de décrire en détail la manière dont le système est supposé fonctionner, les conditions ambiantes dans lesquelles il est placé ainsi que ses conditions de fonctionnement si l'on veut analyser, sans risque d'erreur, le comportement à long terme dudit système. Il s'avérera peut-être nécessaire de procéder à une analyse séparée de la structure fonctionnelle du système afin de trouver tous les cas où il n'exécute pas correctement sa fonction.

La fonction d'un système peut être représentée par des diagrammes fonctionnels, des diagrammes de flux d'information, des diagrammes de transition, des séquences d'événements, des tableaux, etc.

Enfin, l'analyse qualitative (de la défaillance) pourra être réalisée selon l'une des deux méthodes formalisées suivantes:

– méthode déductive (du sommet à la base), par exemple l'analyse par arbre de panne;

– méthode inductive (de la base au sommet), par exemple AMPE.

Toutefois, dans la pratique, il est beaucoup plus fréquent d'employer une démarche itérative faisant appel à la fois à l'analyse déductive et à l'analyse inductive de façon qu'elles se complètent l'une l'autre.

5.3 *Analyse déductive*

La démarche déductive consiste essentiellement à partir du niveau d'intérêt le plus haut, c'est-à-dire, le niveau du système ou du sous-système, pour descendre de niveau en niveau afin de trouver les fonctionnements indésirables du système.

L'analyse est ensuite effectuée au niveau immédiatement inférieur de façon à déceler toute panne et mode de panne associé qui pourraient entraîner l'effet de la panne initialement identifié. On répète l'analyse pour chacune de ces pannes du deuxième niveau en suivant les chemins et relations fonctionnels jusqu'au niveau immédiatement inférieur. Ce processus se poursuit jusqu'à ce que le niveau le plus bas voulu soit atteint.

La méthode déductive se concentre sur l'événement. Elle est utile au début de la phase de réflexion qui précède la conception du système quand toutes les particularités du système n'ont pas encore été définies. Elle permet aussi d'évaluer les défaillances multiples (y compris les défaillances se produisant en séquence) et de détecter l'existence de pannes de cause commune. Elle est également utilisée à chaque fois que le système est tellement complexe qu'il est plus commode de partir d'une liste des pannes ou des missions réussies du système.

En tous cas, il convient de préciser l'événement unique indésirable ou la mission réussie se trouvant au niveau le plus élevé (événement de tête). On détermine et on analyse ensuite toutes les causes, à tous niveaux, qui contribuent à créer cet événement.

5.4 *Analyse inductive*

La méthode inductive consiste essentiellement à découvrir les modes de panne au niveau des composants. On établit, pour chacun de ces modes de panne, son effet sur le fonctionnement du niveau immédiatement supérieur du système. L'effet de la panne ainsi trouvé devient le mode de panne du niveau immédiatement supérieur, et les effets de chacun des modes de panne sont analysés à ce niveau. Par itérations successives, on

5.2 *Analysis of functional structure*

In order to analyze the long-term operating behaviour of a system with confidence, the precise way a system is required to function, as well as its operational and environmental conditions should be determined and described in detail. A separate analysis of the functional system structure may be necessary to identify any departure from the required function.

The system function may be represented by functional block diagrams, signal flow diagrams, state-transition diagrams, event sequences, tables etc.

Finally, the qualitative failure or success analysis may be conducted in accordance with either of two formal methods:

- deductive methodology (top-down), for example fault tree analysis;
- inductive methodology (bottom-up), for example fault mode and effects analysis.

However, in practice, an iterative approach is more usual with deductive and inductive analysis complementing one another.

5.3 *Deductive analysis*

The essence of the deductive approach is to proceed from the highest level of interest, that is, the system or sub-system level, to successively lower levels in order to identify undesirable system operation.

The analysis is performed at the next lower system level to identify any fault and its associated fault mode which could result in the fault effect as originally identified. For each of these second level faults, the analysis is repeated by tracing back along the functional paths and relationships to the next lower level. This process is continued as far as the lowest level desired.

The deductive method is an event-oriented method which is useful during the early conceptual phase of system design when the details of the system are not yet fully defined. It is also used for evaluating multiple failures including sequentially related failures, the existence of faults due to a common-cause, or wherever system complexity makes it more convenient to begin by listing system faults or system success.

In all cases, the undesirable single event or system success at the highest level of interest (the top event), should be given. The contributory causes of that event at all levels are then identified and analyzed.

5.4 *Inductive analysis*

The essence of the inductive method is to identify fault modes at the component level. For each fault mode the corresponding effect on performance is deduced for the next higher system level. The resulting fault effect becomes the fault mode at the next higher system level, and the fault effects of each fault mode are analyzed at this level. Successive iterations result in the eventual identification of the fault effects at all functional levels up

parvient finalement à déterminer les effets des pannes à tous les niveaux fonctionnels jusqu'au système lui-même. Cette méthode inductive permet de trouver tous les modes de panne unique de façon très rigoureuse. Comme il faut connaître les modes de panne des pièces, on emploie normalement cette méthode à des stades ultérieurs de la conception lorsque l'on travaille sur un matériel déjà assez élaboré.

5.5 *Analyse et examen de la maintenance et des réparations*

Le fonctionnement à long terme d'un système réparable est très influencé par la maintenabilité du système ainsi que par les stratégies choisies en matière de réparation et de maintenance. La disponibilité est la caractéristique appropriée lorsque l'on évalue l'influence de la maintenance et des réparations d'un système.

On ne peut normalement réparer un système pendant son fonctionnement, sans l'empêcher de remplir sa fonction, que si une structure redondante du système a été prévue avec des composants redondants accessibles. Dans ce cas, une réparation ou un remplacement augmente la fiabilité et la disponibilité du système.

Il est habituellement nécessaire d'effectuer une analyse séparée pour évaluer les aspects de réparation et de maintenance du système (voir la CEI 706-1).

6 Caractéristiques de diverses méthodes d'analyse de la sûreté de fonctionnement

6.1 *Choix de la méthode appropriée d'analyse*

Si l'on veut faciliter l'évaluation économique de la fiabilité du système, il convient de choisir une méthode d'analyse qui:

- puisse modéliser et évaluer un large spectre de problèmes de sûreté de fonctionnement;
- permettre une analyse quantitative et qualitative qui soit à la fois directe et systématique et qui puisse être effectuée par des ingénieurs expérimentés dans les domaines de la conception et de la sûreté de fonctionnement;
- fournisse des évaluations numériques de la sûreté de fonctionnement si des données sont disponibles.

Il convient de choisir une méthode d'analyse de la sûreté de fonctionnement qui permette d'obtenir les résultats voulus et qui ait les caractéristiques désirées.

Le tableau 2 donne un aperçu des diverses méthodes d'analyse de la sûreté de fonctionnement et de leurs caractéristiques et propriétés. Pour avoir une analyse complète d'un système, il faut parfois utiliser plusieurs de ces méthodes.

6.2 *Description résumée des méthodes d'analyse*

6.2.1 *Analyse des modes de panne et de leurs effets*

L'analyse des modes de panne et de leurs effets (AMPE) est une méthode d'analyse inductive (de la base au sommet) de la sûreté de fonctionnement qui est adaptée à l'étude des pannes des matériaux, des composants et des équipements ainsi qu'à l'étude de leurs effets et mécanismes sur les niveaux fonctionnels supérieurs. En procédant à des itérations successives de la démarche, à l'identification des modes de panne unique et à l'évaluation des effets de la panne sur le niveau immédiatement supérieur du système, on détermine tous les modes de panne unique du système. L'AMPE se prête à l'analyse de différentes technologies (électriques, mécaniques, hydrauliques, logiciel, etc.) caractérisées par des structures fonctionnelles simples.

to the system level. This "bottom-up" method is rigorous in identifying all single fault modes. Because component fault modes must be identified, this method is normally used during the later stages of design where equipment has become mature.

5.5 *Maintenance and repair analysis and considerations*

The long-term operating behaviour of a repairable system is greatly influenced by the system maintainability as well as the repair or maintenance strategies employed. An availability performance measure is the appropriate measure for evaluating the influence of maintenance and repair on system dependability.

Repair of a system during operation without interruption of its function is normally possible only for a redundant system structure with accessible redundant components. If so, then repair or replacement increase system reliability performance and availability performance.

It is usually necessary to perform a separate analysis to evaluate repair and maintenance aspects of a system (see IEC 706-1).

6 Characteristics of various dependability analysis methods

6.1 *Selecting the appropriate analysis method*

In order to enable a system dependability evaluation to be economically performed, an analysis method should be chosen which:

- models and evaluates a wide range of dependability problems;
- allows a straightforward, systematic, qualitative and quantitative analysis to be performed by trained design and dependability engineers;
- predicts measures of the dependability characteristics numerically, if data are available.

A dependability analysis method should be selected which will give the desired results and encompass all relevant attributes.

Table 2 gives an overview of various dependability analysis methods and their characteristics and features. More than one method may be required to provide a complete analysis of the system.

6.2 *Short descriptions of analysis methods*

6.2.1 *Fault mode and effects analysis*

Fault mode and effect analysis (FMEA) is an inductive (bottom-up), qualitative dependability analysis method, which is particularly suited to the study of material, component and equipment faults and their effects and mechanisms on the next higher functional system level. Iterations of the step (identification of single fault modes and the evaluation of their effects on the next higher system level) result in the eventual identification of all the system single fault modes. FMEA lends itself to the analysis of systems of different technologies (electrical, mechanical, hydraulic, software, etc.) with simple functional structures.

L'analyse des modes de panne, de leurs effets et de leur criticité (AMPEC) est une extension de l'AMPE qui inclut l'analyse de la criticité dans la mesure où les effets des pannes sont affectés d'une probabilité et d'une gravité. Le taux de défaillance est estimé directement à l'aide d'une méthode de prévision de la fiabilité en utilisant les données obtenues avec l'AMPE (probabilité d'un mode de panne, taux de défaillance, etc.). La gravité est évaluée par référence à une échelle spécifiée.

6.2.2 *Analyse par arbre de panne*

L'analyse par arbre de panne est une méthode d'analyse déductive (du sommet à la base) de la sûreté de fonctionnement d'un système. Elle sert à déterminer et à analyser les conditions et les facteurs qui produisent ou contribuent à produire un événement indésirable défini qui influe notablement sur les performances, la sécurité, les paramètres économiques ou sur d'autres caractéristiques requises du système.

En partant de l'événement de tête, on recherche les causes ou modes de panne possibles au niveau fonctionnel immédiatement inférieur du système. Après avoir identifié pas à pas les fonctionnements indésirables du système, en passant d'un niveau au niveau immédiatement inférieur, on parvient au niveau du système le plus bas que l'on souhaite étudier. Les causes, à ce niveau, sont habituellement les modes de panne des composants. Les résultats de l'analyse sont représentés graphiquement par un arbre de panne.

L'analyse quantitative est effectuée en partant de l'arbre de panne. Pour estimer la fiabilité et la disponibilité du système, on recourt à des réductions comme la réduction booléenne et l'analyse des coupes minimales. Les données de base nécessaires sont les taux de défaillance des composants, les taux de réparation, la probabilité des modes de panne, etc.

6.2.3 *Analyse par diagramme de fiabilité*

L'analyse par diagramme de fiabilité est une méthode d'analyse déductive (du sommet à la base) de la sûreté de fonctionnement d'un système. Un diagramme de fiabilité est la représentation graphique de l'organisation fonctionnelle d'un système en sous-systèmes et/ou composants. Ainsi, on peut déterminer les chemins de succès du système suivant la manière dont les blocs (sous-systèmes/composants) sont reliés entre eux.

On peut employer diverses techniques d'analyse qualitative pour obtenir un diagramme de fiabilité. La première étape consiste à établir ce qu'est le succès du système. Dans l'étape suivante, on divise le système en blocs fonctionnels, adaptés à l'analyse de la fiabilité. Certains blocs peuvent correspondre à des sous-structures du système qui, à leur tour, peuvent être représentées par d'autres diagrammes de fiabilité (réduction du système).

Il existe plusieurs méthodes pour effectuer une évaluation quantitative d'un diagramme de fiabilité. Suivant le type de structure (réductible, irréductible), on peut recourir à des techniques booléennes simples et/ou à l'analyse des chemins ou des coupes, pour prévoir les valeurs de la fiabilité et de la disponibilité du système en partant des données de base sur les composants.

6.2.4 *Analyse par graphe de Markov*

L'analyse par graphe de Markov est essentiellement une méthode d'analyse inductive (de la base au sommet) adaptée à l'évaluation de structures complexes de systèmes et de stratégies complexes de maintenance et de réparation.

La méthode repose sur la théorie des chaînes de Markov. En principe, on évalue, à l'aide de modèles mathématiques, les probabilités pour des éléments du système (composants/sous-systèmes) de se trouver dans un état (fonctionnel) donné ou, pour des événements, de se produire à certains moments ou au cours de certaines périodes.

FMECA extends the FMEA to include criticality analysis by quantifying fault effects in terms of probability of occurrence and the severity of any effects. Estimates of the probability of failure are calculated directly from a reliability prediction using the data assessed by the FMEA (probability of occurrence of a fault mode, failure rates, etc.). The severity of effects is assessed by reference to a specified scale.

6.2.2 *Fault tree analysis*

Fault tree analysis (FTA) is a deductive (top-down) method for analyzing system dependability. It is concerned with the identification and analysis of conditions and factors which cause, or contribute to, the occurrence of a defined undesirable event and which significantly affect system performance, safety, economy or other specified characteristics.

Starting with the top event, the possible causes or fault modes on the next lowest functional system level are identified. Following stepwise identification of undesirable system operation to successively lower system levels will lead to the desired lowest system level. Causes at this level are usually the component fault modes. The results of the analysis are portrayed as a fault tree.

The quantitative analysis is performed on the basis of the fault tree. In order to estimate system reliability and availability, methods such as Boolean reduction and cut set analysis are employed. The basic data required are component failure rates, repair rates, probability of occurrence of fault modes etc.

6.2.3 *Reliability block diagram analysis*

Reliability block diagram (RBD) analysis is a deductive (top-down) system dependability analysis method. An RBD is the graphical representation of a system's logical structure in terms of sub-systems and/or components. This allows the system success paths to be represented by the way in which the blocks (sub-systems/components) are logically connected.

Various qualitative analysis techniques may be employed to construct an RBD. The first step is to establish the definition of system success. The next step is to divide the system in functional blocks appropriate to the purpose of the reliability analysis. Some blocks may represent system substructures, which in turn may be represented by other RBDs (system reduction).

For the quantitative evaluation of an RBD, various methods are available. Depending on the type of structure (reducible or irreducible) simple Boolean techniques, truth tables and/or path and cut set analysis may be employed for the prediction of system reliability and availability values calculated from basic component data.

6.2.4 *Markov analysis*

Markov analysis is mainly an inductive (bottom-up) analysis method suitable for the evaluation of functionally complex system structures and complex repair and maintenance strategies.

The method is based on the theory of Markov chains. In principle the probabilities of system elements (components, sub-systems) being in a particular (functional) state, or events to occur, at specific points or intervals of time are evaluated by mathematical models.

Tous les états intéressants doivent d'abord être définis ainsi que les probabilités de transition d'un état à un autre (taux de défaillance ou de réparation des composants, taux d'événements, etc.). On suppose normalement que les taux de transition (taux de défaillance, taux d'événements) sont constants, c'est-à-dire indépendants du temps ou des événements antérieurs.

Pour l'analyse qualitative, on doit définir tous les états possibles du système représentés de préférence par un diagramme de transition. Pour ce faire, on peut s'aider de la technique des tables de vérité.

A l'aide des taux de transition et des informations sur la structure du système (tirées des diagrammes de transition), il est possible de construire la matrice de transition voulue (modèle mathématique) afin de calculer les caractéristiques de fiabilité et de disponibilité du système. L'évaluation d'autres mesures intéressantes peut aussi être effectuée.

6.2.5 *Prévision de fiabilité par décompte des pièces*

La prévision de la fiabilité par décompte des pièces est essentiellement une méthode inductive (de la base au sommet), applicable surtout pendant la phase de proposition et au tout début de la conception pour obtenir une évaluation approximative du taux de défaillance d'un système.

On dresse la liste des composants du système et on calcule les taux de défaillance correspondants suivant leur niveau déterminé de contrainte.

La méthode est basée sur l'hypothèse que les composants sont logiquement connectés en série. C'est souvent une estimation du «pire cas». Si des redondances existent aux niveaux supérieurs, leurs effets peuvent être pris en compte.

Une analyse de fiabilité par décompte des pièces d'un système ayant une structure en série produira des prévisions avec un niveau de précision acceptable si une analyse détaillée des contraintes est effectuée. Par l'utilisation de ce type d'analyse, des taux de défaillance plus réalistes sont obtenus pour les composants.

6.3 *Explications pour le tableau 2*

6.3.1 *Généralités*

La partie gauche du tableau 2 contient une liste des méthodes d'analyse. Leurs caractéristiques, leurs propriétés et leur souplesse sont précisées afin de faciliter leur évaluation et leur comparaison.

Ainsi, pour chaque méthode d'analyse, le tableau indique par «oui» ou «non» les points supplémentaires que cette méthode permet de traiter. En outre, les méthodes d'analyse se distinguent par des propriétés ou techniques spécifiques. Celles-ci sont énumérées et caractérisées pour chaque méthode d'analyse dans la partie droite du tableau 2.

Si l'on examine le tableau 2, on s'aperçoit qu'il n'existe pas de méthode d'analyse de la sûreté de fonctionnement qui, à elle seule, ait toutes les propriétés. L'analyste devra donc choisir la méthode qui est la mieux adaptée à un système particulier ou à un objectif donné.

Toutes ces méthodes permettent cependant d'analyser:

- les structures en série;
- les structures réductibles, s'il existe des structures redondantes;
- les composants indépendants (modèle à deux états);
- les pannes uniques;
- les distribution de défaillances exponentielles;
- les taux constants de réparation ou d'événements;
- la réparation d'un composant indépendant.

Initially all the states of interest shall be defined together with the probabilities of transition from one state to another (component failure or repair rates, event rates etc.). Transition rates (failure rates, event rates) are normally assumed to be constant, i.e. independent of time or previous history.

The qualitative analysis requires the determination of all the possible system states, preferably shown diagrammatically in a state-transition diagram. A major supporting analysis technique is the truth table.

The transition probabilities and the way in which the states are related, represented by the state-transition diagram, allow the construction of the desired transition matrix (mathematical model) for the purpose of system reliability/availability calculations. The evaluation of other measures of interest may also be accomplished.

6.2.5 *Parts count reliability prediction*

Parts count reliability prediction is basically an inductive (bottom-up) method applicable mostly during the proposal and early design phases, to estimate an approximate system failure rate.

The components of the system need to be listed and the appropriate failure rates determined according to their stress levels.

The method is based upon the assumption that the components are logically connected in series. This is often a worst case estimate. Where redundancies at the higher levels of assembly are known, their effects may be taken into account.

A parts count reliability prediction of a system with a series type of structure will yield predictions at an acceptable precison level, provided a thorough "Parts Stress Analysis" is carried out. Use of the parts stress analysis gives more realistic component failure rates.

6.3 *Explanations to table 2*

6.3.1 *General*

On the left hand side of table 2, the analysis methods are listed. In order to facilitate evaluation and comparison, their characteristics, attributes, flexibility, etc., are stated.

For each analysis method the matrix thus gives an indication as to which additional characteristics each method can handle as indicated by "yes" and "no" entries. Further, the analysis methods are distinguished by particular attributes or techniques. These are listed and rated on the right hand side of table 2.

Table 2 indicates that there is no single, comprehensive dependability analysis method. The analyst should choose the method which best fits the particular system or analysis objective.

All these methods are capable of analyzing:

- series structures;
- reducible structures if redundant structures are applicable;
- independent components (two-state model);
- single faults;
- exponential distribution of times to failure;
- constant repair or event rates;
- independent component repair.

Tableau 2 – Caractéristiques de diverses méthodes d'analyse

Méthode d'analyse	Caractéristiques															Norme CEI
	Aptitude de la méthode à traiter les caractéristiques du modèle telles que:								Propriétés							
	Nombre de composants	Structures redondantes	Structures irréductibles	Combinaisons et dépendances de défaillance/ événement	Taux de défaillance/ événement variant avec le temps	Stratégie complexe de maintenance	Simulation d'un processus de fonctionnement	Représentation symbolique	Démarche		Analyse		Effort d'analyse (coût)			
									déductive	inductive	qualitative	quantitative	qualitatif	quantitatif		
AMPE	Jusqu'à plusieurs milliers	(non)	non	(non)	oui	non	non	Liste	(i)	c	c	i	grand	–		812
AMPEC	Jusqu'à plusieurs milliers	(non)	non	(non)	oui	non	non	Liste	i	c	c	(c)	grand	faible		812
Analyse par arbre de panne	Jusqu'à plusieurs milliers	oui	(oui)[1)]	(oui)	oui	non	non	Arbre de panne	c	i	c	c	grand	moyen		1025
Diagramme de fiabilité	Jusqu'à plusieurs milliers	oui	(oui)[1)]	(oui)	(oui)	non	non	Diagramme de fiabilité	c	i	(c)	c	moyen	moyen		1078
Prévision par graphe de Markov	de 2 à 100[5)]	oui	oui	oui[6)]	(non)[7)]	oui	(oui)	Diagramme d'état de synthèse	(i)	c	c	c	grand	moyen		–
Analyse de fiabilité des pièces	1 à des milliers	(non)	(oui)	non	(non)	–	–	Liste	i	c	(i)	c	faible	faible		–
Cause/conséquence	Jusqu'à plusieurs centaines	oui	oui	(oui)	(oui)	oui[2)]	non	Diagramme cause/ conséquence	(c)	c	c	c	grand	faible/ grand[4)]		–
Simulation de l'événement	Jusqu'à plusieurs centaines[8)]	oui	oui	oui	oui	oui	oui	Toutes	c	c	c	c	grand	grand		–
Réduction de synthèse	Jusqu'à plusieurs milliers[9)]	oui	non	(oui)	(oui)	(oui)	non	Diagramme de fiabilité	i	c	(i)[10)]	c[10)]	moyen	moyen		–
Arbre d'événement	2 à 50	oui	oui	(oui)	oui	non	oui	Arbre d'événement	c	c	(i)	c	faible	moyen		–
Table de vérité[3)]	2 à 50[5)]	oui	oui	oui[6)]	–	–	–	Tableau	i	c	c	i	grand[5)]	–		–

NOTE - Pour les abréviations et les remarques, voir 6.3.3.

Tableau 2 – Characteristics of analysis methods

Analysis method	Characteristics															
	Ability of method to handle model characteristics as:							Attributes								
	Number of components	Redundant structures	Irreducible structures	Failure/event combinations and dependencies	Time varying failure/event rates	Complex maintenance strategies	Simulation of functional process	Symbolic representation	Approach		Analysis		Analysis effort (cost)		IEC Standard
									deductive	inductive	qualitative	quantitative	qualitative	quantitative	
FMEA	Up to several thousands	(no)	no	(no)	yes	no	no	List	(nc)	c	c	nc	high	–	812
FMECA	Up to several thousands	(no)	no	(no)	yes	no	no	List	nc	c	c	(c)	high	low	812
Fault tree analysis	Up to several thousands	yes	(yes)[1)]	(yes)	yes	no	no	Fault tree	c	nc	c	c	high	medium	1025
Reliability block diagram	Up to several thousands	yes	(yes)[1)]	(yes)	(yes)	no	no	Reliability block diagram	c	nc	(c)	c	medium	medium	1078
Markov	2 to 100[5)]	yes	yes	yes[6)]	(no)[7)]	yes	(yes)	System state diagram	(nc)	c	c	c	high	medium	–
Parts count	1 to thousands	(no)	(yes)	no	(no)	–	–	List	nc	c	(nc)	c	low	low	–
Cause/consequence	Up to several hundreds	yes	yes	(yes)	(yes)	yes[2)]	no	Cause/consequence chart	(c)	c	c	c	high	low/ high[4)]	–
Event simulation	Up to several hundreds[8)]	yes	yes	yes	yes	yes	yes	Any	c	c	c	c	high	high	–
System reduction	Up to several thousands[9)]	yes	no	(yes)	(yes)	(yes)	no	Reliability block diagram	nc	c	(nc)[10)]	c[10)]	medium	medium	–
Event tree	2 to 50	yes	yes	(yes)	yes	no	yes	Event tree	c	c	(nc)	c	low	low	–
Truth table[3)]	2 to 50[5)]	yes	yes	yes[6)]	–	–	–	Table	nc	c	c	nc	high[5)]	–	–

NOTE - For abbreviations and remarks, see clause 6.3.3.

6.3.2 *Titres du tableau 2*

Nombre de composants:

Le nombre de composants du système qui peuvent être traités par une méthode d'analyse donnée est en fait limité par le nombre de combinaisons (états du système) qui sont créées par les états ou les modes de panne étudiés des composants. Le nombre des combinaisons dépend aussi, pour beaucoup, de la structure spécifique du système et des considérations de maintenance.

Structures redondantes:

La capacité fondamentale de traiter les structures redondantes du système.

Structures irréductibles:

Une structure est dite irréductible si l'on ne peut lui appliquer des techniques de réduction directe.

Combinaisons et dépendances de défaillance/événement:

Aptitude de la méthode à traiter des combinaisons de défaillances ou d'événements, comme les défaillances de cause commune ou de mode commun, les effets de défaillances multiples et les modes de panne statistiquement dépendants ou encore les effets et mécanismes de défaillances en séquence ou, enfin, les événements produits par des effets préjudiciables de l'environnement.

Taux d'événement ou de défaillance variant avec le temps:

Taux d'événement ou de défaillance non constants (ou distributions de défaillances non exponentielles).

Stratégies complexes de maintenance:

Aptitude de la méthode à traiter des cas de réparation et de maintenance statistiquement dépendants. Cela comprend les cas où les processus de renouvellement (files d'attente pour les réparations) devraient être considérés, par opposition à la situation courante où l'on suppose que chaque fois qu'un composant est défaillant, un réparateur intervient immédiatement pour le réparer, que le composant soit ou non accessible (réparation indépendante).

Simulation d'un processus de fonctionnement:

Aptitude d'une méthode à simuler des événements discrets. Par exemple, la défaillance et le processus de renouvellement sont simulés et les états dudit système sont évalués en fonction de l'influence qu'ils ont sur le système du niveau supérieur ou sur l'environnement (relation mutuelle).

Par conséquent, il est également nécessaire de simuler le fonctionnement du système au niveau supérieur, ou l'environnement, en même temps qu'on analyse le processus de fonctionnement ou de défaillance du système.

Démarche déductive/inductive:

Voir 5.3 et 5.4.

6.3.2 *Table 2 headings*

Number of components:

The number of components of the system which can be handled by a particular analysis method is basically limited by the number of combinations (system states) which arise from the possible component states or fault modes considered. The number of combinations is also heavily dependent on the specific system structure and maintenance considerations.

Redundant structures:

The basic capability to handling redundant system structures.

Irreducible structures:

A structure is called irreducible if straightforward reduction techniques are not possible.

Failure/event combinations and dependencies

The capability of the method to handle failure or event combinations. These include common cause or common mode failures, multiple failure effects and statistically dependent fault modes or sequential failure effects and mechanisms, or events caused by adverse environmental effects.

Time varying failure/event rates:

Non-constant failure and event rates (or non-exponential distribution of times to failure).

Complex maintenance strategies:

The capability of the method to handle statistically dependent repair and maintenance situations. These include cases where renewal processes (repair queues) should be considered, as compared to the assumption that, for each component failure, repair begins immediately after failure, independent of whether a component is accessible or not (independent repair).

Simulation of functional process:

The capability of a method to simulate discrete events; i.e. the failure and renewal processes are simulated and the particular system states evaluated according to the influence which they exert on any higher-level system or on the total environment (interrelation).

Therefore, it is also necessary to simulate the functional behaviour of the higher-level system along with processes within the total environment while analyzing the operating and failure processes of the system itself.

Deductive/inductive approach:

See 5.3 and 5.4.

Analyse qualitative/quantitative:

La méthode se prête-t-elle à l'analyse qualitative et/ou quantitative de la fiabilité ?

Effort (coût) de l'analyse qualitative/quantitative:

Les entrées donnent une évaluation relative du coût de l'adoption d'une méthode donnée d'analyse pour résoudre un problème particulier. L'effort réel d'analyse dépend assurément de la complexité du système, du stade auquel est poussée l'analyse, de l'habileté de l'analyste et de l'existence de données de base sur le système et les composants.

6.3.3 *Remarques sur le tableau 2*

() Avec restrictions/exceptions.

i Incapable de ou inapplicable.

c Capable de.

1) Avec coupes ou réduction logique.

2) Par simulation de l'événement, intégration numérique ou théorie du renouvellement.

3) Méthode fondamentale, systématique (analyse combinatoire) comme complément de l'analyse qualitative des systèmes (s'applique, en particulier, aux graphes de Markov et à la simulation des événements pour déterminer les états possibles du système).

4) Faible en ce qui concerne le taux d'événements et grand pour ce qui est de l'indisponibilité (schémas avec boucles).

5) Dépend de la complexité du système (du processus stochastique à simuler) et des possibilités d'approximation (séquences d'événements tronquées).

6) Evénements particulièrement dépendants, par exemple structures parallèles avec composants passifs (en attente).

7) Distribution spéciale d'Erlang (introduction d'états fictifs) ou processus semi-markoviens.

8) Taille et complexité du système dépendent essentiellement des moyens de calcul disponibles, de l'efficacité de la procédure de simulation de l'événement (simulation de Monte Carlo) et de la précision souhaitée des caractéristiques à évaluer.

9) On suppose que les composants, à chaque niveau de réduction, sont indépendants. De ce fait, on peut recourir à n'importe quelle méthode d'analyse de la sûreté de fonctionnement pour évaluer les composants respectifs.

10) Essentiellement, calcul des caractéristiques de la sûreté de fonctionnement du système par la méthode de réduction (substitution) d'un diagramme de fiabilité donné.

Qualitative/quantitative analysis:

The capability of a method to handle qualitative and/or quantitative analysis.

Qualitative/quantitative analysis effort (cost):

The entries give relative estimates of the cost of applying a particular analysis method to a particular problem. The effective analysis effort is dependent on the system complexity, the depth of analysis, the skill of the analyst, the availability of basic system and component data, and the availability of suitable computing resources.

6.3.3 *Remarks with reference to table 2*

() With restrictions/exceptions.

nc Not capable, or not applicable.

c Capable.

1) With cut sets or logical reduction.

2) By event simulation, numerical integration or renewal theory.

3) A basic, systematic method (combinatorics) to support qualitative system analysis, in particular for Markov and event simulation to determine the possible system states.

4) Low for event rate, high for unavailability (diagrams with loops).

5) Depends on system complexity (stochastic process to be simulated) and possible approximations (truncation of event sequences).

6) Especially dependent events, for example, parallel structures with passive (standby) components.

7) Special Erlang distribution (introduction of virtual – "dummy"-states) or semi-Markov process.

8) System size and complexity which can be handled are mainly dependent on available computing means, efficiency of event (Monte Carlo) simulation procedure and required accuracy of measures to be estimated.

9) Independent components at each reduction level are assumed. Therefore, any dependability analysis method may be employed for the evaluation of the relevant components.

10) Mainly calculation of system dependability measures by the reduction (substitution) method of a given reliability block diagram.

6.4 *Avantages et inconvénients des méthodes*

On trouvera ci-après une comparaison entre quelques méthodes couramment utilisées.

6.4.1 *Analyse des modes de panne et de leurs effets*

6.4.1.1 *Avantages*

– permet de déterminer systématiquement les relations logiques entre cause et effet;

– peut fournir une première idée des modes de panne qui peuvent poser un problème grave, en particulier, des pannes uniques qui peuvent se propager;

– est utile quand il s'agit de rechercher des conséquences éventuelles lorsqu'on les ignore ou qu'on les connaît mal;

– est utile pour déterminer les conséquences de causes données ou d'événements initiateurs que l'on soupçonne de présenter un danger;

– peut mettre en évidence des conséquences intempestives ainsi que des dérèglements par rapport au fonctionnement normal;

– est utile pour l'analyse préliminaire de systèmes ou de composants nouveaux ou qui n'ont pas été éprouvés.

6.4.1.2 *Inconvénients*

– peut conduire à de très grands tableaux, même pour des systèmes assez simples;

– peut devenir compliquée et inexploitable à moins qu'il n'y ait une relation assez directe (ou «chaîne directe») entre la cause et l'effet (ne peut, par exemple, s'appliquer aisément aux relations parallèles ou complexes);

– peut difficilement traiter les séquences temporelles, les processus de rétablissement, les conditions ambiantes, les aspects de maintenance, etc.;

– ne donne pas directement, elle-même, un modèle pour l'évaluation quantitative;

– peut difficilement représenter les dépendances multiples ou les interactions complexes entre des pannes de différentes parties du système.

6.4.2 *Analyse par arbre de panne*

6.4.2.1 *Avantages*

– permet de trouver systématiquement les chemins logiques de pannes en partant d'un effet spécifique pour remonter jusqu'aux causes originelles;

– permet de traiter les chemins de pannes parallèles, redondants ou autres;

– permet d'étudier la plupart des formes de combinaisons d'événements et certaines formes de dépendances;

– permet d'étudier des systèmes qui ont des sous-systèmes en interaction;

– permet d'effectuer assez facilement un traitement des chemins de défaillance pour obtenir des modèles logiques minimaux (par exemple, à l'aide de l'algèbre de Boole);

6.4 *Advantages and disadvantages of methods*

A comparison of some of the commonly used methods follows.

6.4.1 *Fault mode and effects analysis*

6.4.1.1 *Advantages*

– identifies systematically the cause and effect relationships;

– gives an initial indication of those fault modes which are likely to be critical, especially single faults which may propagate;

– searches for possible outcomes not previously or precisely known;

– identifies outcomes arising from specific causes or initiating events which are believed to be important;

– highlights spurious outcomes as well as deviations from normal functional performance;

– useful in the preliminary analysis of new or untried systems or components.

6.4.1.2 *Disadvantages*

– the output data may be large even for relatively simple systems;

– may become complicated and unmanageable unless there is a fairly direct (or "single-chain") relationship between cause and effect, i.e. cannot conveniently deal with parallel or complex relationship;

– may not easily deal with time sequences, restoration processes, environmental conditions, maintenance aspects, etc.;

– does not, in itself, directly produce a model for quantitative evaluation;

– may not easily portray multiple dependencies or complex interactions between faults in different parts of the system.

6.4.2 *Fault tree analysis*

6.4.2.1 *Advantages*

– identifies and records systematically the logical fault paths from a specific effect, back to the prime causes;

– deals with parallel, redundant or alternative fault paths;

– deals with most forms of combinatorial events and some forms of dependencies as well;

– deals with systems which have several cross-linked sub-systems;

– provide for fairly easy manipulation of the fault paths to give minimal logical models (e.g. by using Boolean algebra);

– permet de passer facilement de modèles logiques aux mesures correspondantes de la probabilité;

– identifie les causes ou les modes de panne qui ont le plus de chances de produire l'effet final ou le résultat étudié;

– est utile quand il s'agit de rechercher les causes possibles d'un effet final lorsque ces causes n'ont pas été identifiées auparavant;

– est très utile dans toute analyse systématique globale des défaillances quand on part d'une ou de deux conséquences importantes préoccupantes.

6.4.2.2 *Inconvénients*

– peut souvent produire des arbres de taille considérable si l'analyse est très poussée;

– il peut arriver que le même événement soit décrit en plusieurs endroits de l'arbre. Cela peut entraîner quelque confusion ainsi que des erreurs, mais on peut y remédier de manière automatique et logique;

– ne représente pas, en elle-même, les transitions entre les états d'un événement quelconque;

– exige la construction d'un arbre de panne séparé pour chaque événement de tête. Les relations entre les différents arbres de panne peuvent alors nécessiter une attention particulière;

– les causes premières révélées par l'arbre de panne ne sont reliées qu'à l'événement précis que l'on analyse; ces causes risquent de produire d'autres événements qui peuvent ne pas apparaître;

– c'est une méthode orientée essentiellement sur l'analyse des pannes ou des défaillances. Elle ne traite pas vraiment les stratégies de réparation et de maintenance complexes ni l'analyse de la disponibilité globale.

6.4.3 *Analyse par diagramme de fiabilité*

6.4.3.1 *Avantages*

– peut être établie presque directement à partir des diagrammes fonctionnels du système. Grâce à cela, un nombre réduit d'erreurs est commis pendant l'établissement du diagramme et l'on obtient une représentation systématique des «chemins» fonctionnels pertinents pour la fiabilité du système;

– permet d'aborder la plupart des configurations de systèmes, y compris les chemins fonctionnels parallèles, redondants, en attente ou de rechange;

– permet d'étudier la majorité des combinaisons d'événements et quelques formes de dépendances;

– peut être employée pour effectuer une analyse paramétrique complète sur la base des modifications des paramètres de fonctionnement du système;

– permet (dans l'application à deux états) un traitement facile des chemins fonctionnels (ou non-fonctionnels) pour obtenir des modèles logiques minimaux (par exemple, par l'algèbre de Boole);

– allows easy conversion of logical models into corresponding probability measures;

– identifies the causes of fault modes with a major influence upon the top event or on the result studied;

– searches for possible causes of an end effect which may not have been foreseen;

– useful in overall systematic fault analysis where the starting points consist of one or two major outcomes.

6.4.2.2 *Disadvantages*

– may lead to very large trees if the analysis is extended in depth;

– the same event may appear in different parts of the tree, leading to some confusion and error although this situation can be handled automatically and logically;

– does not represent, in its own right, the transition paths between the states of any one event;

– requires a separate fault tree for each top event; inter-relationships between trees may then require careful consideration;

– the prime causes identified by the fault tree that lead to the top event are related only to the specific outcome being analyzed (such causes may lead to other outcomes which may not be shown);

– is primarily directed towards fault or failure analysis and does not deal effectively with complex repair and maintenance strategies or general availability analysis.

6.4.3 *Reliability block diagram*

6.4.3.1 *Advantages*

– often constructed almost directly from the system functional diagram; this has the further advantages of reducing constructional errors and/or systematic depiction of functional paths relevant to system reliability;

– deals with most types of system configuration including parallel, redundant, standby and alternative functional paths;

– deals with most forms of combinational events and some forms of dependencies;

– capable of complete analysis of variations and trade-offs with regard to changes in system performance parameters;

– provide (in the two-state application) for fairly easy manipulation of functional (or non-functional) paths to give minimal logical models (e.g. by using Boolean algebra);