NORME INTERNATIONALE
INTERNATIONAL STANDARD

CEI
IEC
1025

Première édition
First edition
1990-10

Analyse par arbre de panne (AAP)

Fault tree analysis (FTA)

Numéro de référence
Reference number
CEI/IEC 1025: 1990

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
1025

Première édition
First edition
1990-10

Analyse par arbre de panne (AAP)

Fault tree analysis (FTA)

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

Pages

AVANT–PROPOS 4

INTRODUCTION 6

Articles

1 Domaine d'application 8

2 Références normatives 8

3 Définitions 8

4 Symboles 8

5 Généralités 10

5.1 Structure de l'arbre de panne 10
5.2 Objectifs 10
5.3 Applications 10

6 Principes 12

6.1 Considérations générales 12
6.2 Structure du système 12
6.3 Evénements étudiés 14
6.4 Principes généraux 14

7 Procédures 16

7.1 Portée de l'analyse 16
7.2 Approfondissement de la connaissance du système 16
7.3 Identification de l'événement de tête 16
7.4 Construction de l'arbre de panne 16
7.5 Évaluation de l'arbre de panne 22

8 Repères et libellés 28

9 Rapport 30

Annexe A (Normative): Symboles 34

CONTENTS

Page

FOREWORD 5

INTRODUCTION 7

Clause

1 Scope 9

2 Normative references 9

3 Definitions 9

4 Symbols 9

5 General 11

5.1 Fault tree structure 11
5.2 Objectives 11
5.3 Applications 11

6 Principles 13

6.1 General considerations 13
6.2 System structure 13
6.3 Events considered 15
6.4 Approaches 15

7 Procedures 17

7.1 Scope of analysis 17
7.2 System familiarization 17
7.3 Top event identification 17
7.4 Fault tree construction 17
7.5 Fault tree evaluation 23

8 Identification and labelling 29

9 Report 31

Annex A (Normative): Symbols 35

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

ANALYSE PAR ARBRE DE PANNE (AAP)

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: Fiabilité et maintenabilité.

Le texte de cette norme est issu des documents suivants:

Règle des Six Mois	Rapport de vote	Procédure des Deux Mois	Rapport de vote
56(BC)121	56(BC)129	56(BC)133	56(BC)139

Les rapports de vote indiqués dans le tableau ci-dessus donnent toute information sur les votes ayant abouti à l'approbation de cette norme.

L'annexe A, Symboles, est normative et fait partie intégrante de la présente norme internationale.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FAULT TREE ANALYSIS (FTA)

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 take 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: Reliability and Maintainability.

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

Six Months' Rule	Report on Voting	Two Months' Procedure	Report on Voting
56(CO)121	56(CO)129	56(CO)133	56(CO)139

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

Annex A: Symbols, is normative and forms an integral part of this International Standard.

INTRODUCTION

Il existe plusieurs méthodes d'analyse de la sûreté de fonctionnement, dont l'analyse par arbre de panne (AAP). Avant d'entreprendre une analyse par arbre de panne, l'analyste devra étudier les objectifs de chaque méthode ainsi que les possibilités d'utiliser ces méthodes, seules ou combinées à d'autres, pour évaluer la fiabilité et la disponibilité d'un système ou d'un composant. Il devra également tenir compte des résultats que chaque méthode pourra apporter, des données dont il aura besoin pour effectuer l'analyse, de la complexité de l'analyse ainsi que d'autres facteurs indiqués dans cette norme.

L'analyse par arbre de panne sert à déterminer et à analyser les conditions et les facteurs qui produisent ou contribuent à produire un événement indésirable défini, c'est-à-dire, habituellement, un événement qui influe notablement sur le fonctionnement du système, sur les paramètres économiques, la sécurité ou d'autres caractéristiques requises. L'AAP est souvent employée dans les analyses pour la sécurité des systèmes.

INTRODUCTION

Several analytical methods of dependability analysis are available, of which fault tree analysis (FTA) is one. The purpose of each method and their individual or combined applicability in evaluating the reliability and availability of a given system or component should be examined by the analyst before starting the FTA. Consideration should also be given to the results available from each method, data required to perform the analysis, complexity of analysis, and other factors identified in this standard.

Fault tree analysis is concerned with the identification and analysis of conditions and factors which cause or contribute to the occurrence of a defined undesirable event, usually one which significantly affects system performance, economy, safety or other required characteristics. FTA is often applied to the safety analysis of systems.

ANALYSE PAR ARBRE DE PANNE (AAP)

1 Domaine d'application

La présente Norme internationale contient une description de l'analyse par arbre de panne ainsi que quelques directives sur son application:

- en définissant les principes de base;
- en fournissant la procédure à suivre pour réaliser une analyse;
- en spécifiant les hypothèses appropriées, les événements et les modes de défaillance;
- en indiquant les règles de repérage et les symboles.

2 Références normatives

Les normes suivantes 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. Toute norme est sujette à révision et les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur actuellement.

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

CEI 617-12: 1983, *Symboles graphiques pour schémas, Douzième partie: Opérateurs logiques binaires.*

3 Définitions

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

4 Symboles

La représentation de l'arbre de panne requiert l'utilisation d'un ensemble cohérent de symboles, de repères et de libellés. Les règles détaillées sont données dans l'article 8 et dans l'annexe A.

FAULT TREE ANALYSIS (FTA)

1 Scope

This International Standard describes fault tree analysis, and gives guidance on its application, as follows:

- by defining basic principles;
- by providing the steps necessary to perform an analysis;
- by identifying appropriate assumptions, events and failure modes;
- by providing identification rules and symbols.

2 Normative references

The following standards 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 standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

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

IEC 617-12: 1983, *Graphical symbols for diagrams, Part 12: Binary logic elements.*

3 Definitions

Terms and definitions are in accordance with International Electrotechnical Vocabulary (IEV), Chapter 191.

4 Symbols

The graphical representation of the fault tree requires that symbols, identifiers and labels be used in a consistent manner. The detailed rules are given in clause 8 and annex A.

5 Généralités

5.1 *Structure de l'arbre de panne*

L'arbre de panne constitue une représentation graphique organisée des conditions ou des facteurs produisant ou contribuant à produire un événement indésirable appelé «événement de tête». Cette représentation est établie sous une forme compréhensible, analysable et, si nécessaire, modifiable pour faciliter l'identification:

- des facteurs influant sur la fiabilité et sur les caractéristiques fonctionnelles du système, par exemple modes de panne des composants, erreurs humaines, conditions ambiantes, erreurs dans le logiciel;
- des impératifs ou des spécifications incompatibles qui peuvent nuire au fonctionnement du système;
- des événements communs influant sur plus d'un composant fonctionnel et qui pourraient annuler le bénéfice apporté par les redondances spécifiques.

L'analyse par arbre de panne est essentiellement une méthode d'analyse déductive qui a pour but de faire apparaître les causes ou les combinaisons de causes qui peuvent produire l'événement de tête défini. Cette analyse est surtout qualitative bien qu'elle puisse aussi être quantitative dans certains cas (voir 7.5.2).

5.2 *Objectifs*

L'analyse par arbre de panne s'entreprend, seule ou combinée à une autre analyse de sûreté de fonctionnement, pour plusieurs raisons. Il s'agit entre autres:

- de rechercher toutes les causes et les combinaisons de causes conduisant à l'événement de tête;
- de déterminer si une des caractéristiques de fiabilité du système est conforme à un impératif prescrit;
- de prouver que les hypothèses faites au cours d'autres analyses à propos de l'indépendance des systèmes et de la non prise en compte de certaines défaillances se vérifient;
- d'identifier le(les) facteur(s) qui a (ont) les conséquences les plus néfastes sur une caractéristique de fiabilité ainsi que les modifications nécessaires pour améliorer cette caractéristique;
- d'identifier les événements communs ou les défaillances de cause commune.

5.3 *Applications*

L'arbre de panne est particulièrement adapté à l'analyse de systèmes complexes constitués de plusieurs sous-systèmes dépendants ou entre lesquels existent des relations fonctionnelles et dont les performances satisfont à des objectifs divers. Cela est d'autant plus vrai lorsque la conception du système suppose la collaboration de nombreuses équipes de concepteurs spécialisés. On peut citer, parmi les systèmes couramment soumis à des analyses par arbre de panne, les centrales nucléaires, les avions, les systèmes de communication, les procédés chimiques et autres procédés industriels, etc.

5 General

5.1 *Fault tree structure*

The fault tree itself is an organized graphical representation of the conditions or other factors causing or contributing to the occurrence of a defined undesirable event, referred to as the "top event". The representation is in a form which can be understood, analyzed and, as necessary, rearranged to facilitate the identification of:

- factors affecting the reliability and performance characteristics of the system, for example component fault modes, operator mistakes, environmental conditions, software faults;
- conflicting requirements or specifications which may affect reliable performance;
- common events affecting more than one functional component, which could cancel the benefits of specific redundancies.

Fault tree analysis is basically a deductive (top-down) method of analysis aimed at pinpointing the causes or combinations of causes that can lead to the defined top event. The analysis is mainly qualitative but, depending on certain conditions, it may also be quantitative (see 7.5.2).

5.2 *Objectives*

There are several reasons for performing a fault tree analysis independently of, or in conjunction with, other dependability analyses. These include:

- the identification of the causes or combinations of causes leading to the top event;
- the determination of whether a particular system reliability measure meets a stated requirement;
- the demonstration that assumptions made in other analyses, regarding the independence of systems and non-relevance of failures, are not violated;
- the determination of the factor(s) which most seriously affect a particular reliability measure and the changes required to improve that measure;
- the identification of common events or common cause failures.

5.3 *Applications*

The fault tree is particularly suited to the analysis of complex systems comprising several functionally related or dependent subsystems with different performance objectives. This is especially true whenever the system design requires the collaboration of many specialized technical design groups. Examples of systems to which fault tree analysis is commonly applied include nuclear power generating stations, aeroplanes, communication systems, chemical and other industrial processes, etc.

6 Principes

6.1 *Considérations générales*

Il est recommandé de commencer à construire l'arbre de panne dès les premiers stades de la conception. Le développement de l'arbre de panne reflétera les progrès de la conception et permettra de mieux comprendre les modes de panne au fur et à mesure de la conception. L'analyse concomitante de la conception permet de modifier la conception du système très tôt quand on détecte les modes de panne importants. Beaucoup d'arbres de panne complets sont grands, ce qui nécessite l'emploi d'un ordinateur. Il existe des logiciels qui facilitent l'analyse. Il convient de remarquer que les événements portés sur l'arbre de panne ne se limitent pas à des pannes de logiciels ou des pannes de matériel. Ces événements comprennent en effet toutes les conditions ou tous les facteurs qui ont un rapport avec l'événement de tête correspondant au système étudié.

Si l'on veut employer de manière efficace l'arbre de panne comme méthode d'analyse d'un système, il faut respecter au moins les étapes suivantes:

- définir la portée de l'analyse;
- se familiariser avec la conception, les fonctions et la marche du système;
- définir l'événement de tête;
- construire l'arbre de panne;
- analyser la logique de l'arbre de panne;
- faire un rapport sur les résultats de l'analyse.

Si l'on envisage d'effectuer une analyse numérique, il faut définir une technique d'évaluation numérique. En plus des étapes décrites plus haut, il faudra choisir les données à utiliser et procéder à un calcul numérique des caractéristiques de fiabilité.

6.2 *Structure du système*

Tout système sera défini en décrivant sa fonction et en établissant ses interfaces. Cette définition devra comporter les éléments suivants:

- un résumé des objectifs recherchés dans la conception;
- les limites du système, comme les interfaces électriques, mécaniques et fonctionnelles. Ces limites dépendront de l'interaction et des interfaces avec d'autres systèmes et devront être décrites en identifiant les fonctions particulières, par exemple l'alimentation électrique et les pièces, par exemple fusible, qui constituent les interfaces;
- la structure matérielle du système, par opposition à sa structure fonctionnelle;
- l'identification des modes de fonctionnement et une description du fonctionnement du système ainsi que de ses performances, prévues ou acceptables, pour chaque mode de fonctionnement;
- les conditions relatives à l'environnement du système et les aspects humains pertinents, etc;
- une liste des documents à prendre en compte, par exemple, dessins, spécifications, manuels de fonctionnement, qui contiennent une description détaillée de la conception et du fonctionnement du matériel. La durée des missions, les intervalles entre les

6 Principles

6.1 *General considerations*

The development of the fault tree should start early in the system design stage. The growth of the fault tree should be such that it reflects the progress of the design. Thus an increased understanding of the fault modes will be obtained as the design proceeds. The "analysis concurrent with design" allows for early systems design change as significant fault modes are identified. Many final fault trees will be large, in which case a computer may be needed to handle them. Software is available to facilitate analysis. It is important to note that fault tree events are not confined solely to software or hardware faults, but include all conditions or other factors which are relevant to the top event for the system concerned.

In order to use the fault tree technique effectively as a method for system analysis, the procedure shall consist of at least the following steps:

- definition of the scope of the analysis;
- familiarization with the design, functions, and operation of the system;
- definition of the top event;
- construction of the fault tree;
- analysis of the fault tree logic;
- reporting on results of the analysis.

If a numerical analysis is planned, it will be necessary to define a technique for numerical assessment. The selection of the data to be used and numerical evaluation of the reliability measures are additional requirements.

6.2 *System structure*

Each system should be defined by a description of the system function and by an identification of the system interfaces. Such a definition should include:

- a summary of the design intent;
- the boundaries of the system, such as electrical, mechanical and operational interfaces; such boundaries will be governed by the interaction and interfaces with other systems and should be described by identifying the particular functions, for example power supply, and parts, for example fuse, which form the interfaces;
- the physical structure of the system, as opposed to the functional structure;
- the identification of operational modes together with a description of system operation and the expected or acceptable performance in each operational mode;
- the system's environmental conditions, and relevant human aspects, etc;
- a list of applicable documents, for example drawings, specifications, operating manuals, which give details of the equipment design and operation. Task duration, time interval between (periodic) tests, as well as time available for corrective maintenance

essais (périodiques), le temps disponible pour les actions de maintenance corrective, devront être connus ainsi que le matériel auxiliaire et le personnel nécessaires. Des informations spécifiques sur les procédures d'exploitation prescrites pour chaque phase de fonctionnement seront également fournies.

En plus de ce qui précède, il est recommandé de fournir une liste des symboles, des repères, des conventions et des formats des fichiers de données de façon que la structure et la description de l'arbre de panne puissent, si nécessaire, être échangées entre ordinateurs.

6.3 *Evénements étudiés*

Les événements dus à toutes sortes de causes doivent être portés sur l'arbre. Ces causes incluront les effets de toutes les conditions de l'environnement ou d'autres conditions auxquels pourra être soumise l'entité, y compris ceux que l'on peut rencontrer pendant le fonctionnement, même s'ils ne sont pas prévus dans les spécifications relatives à la conception.

Lorsque ce sera nécessaire, on tiendra compte, dans l'arbre de panne, des effets des erreurs humaines et des insuffisances du logiciel de commande et de surveillance de l'état du système.

Les événements que l'analyste a étudiés mais qu'il a écartés pour la suite de l'analyse parce que considérés comme ne devant pas être pris en compte, devront être signalés mais non portés sur l'arbre de panne définitif.

Si l'arbre de panne révèle un problème dû à une panne existante, l'événement qui correspond à cette panne devra être porté sur l'arbre de panne. Il devra être signalé comme étant un événement qui s'est déjà produit. C'est ce que l'on fait pour considérer l'effet et l'ordre de pannes multiples.

6.4 *Principes généraux*

L'élaboration de l'arbre de panne commence par la définition de l'événement de tête. Cet événement de tête est l'événement de sortie de la porte du sommet de l'arbre, alors que les événements d'entrée correspondants se rapportent à des causes et à des conditions possibles de l'apparition de l'événement de tête. Chaque événement d'entrée peut, lui-même, être un événement de sortie d'une porte se trouvant à un niveau inférieur.

Si l'événement de sortie d'une porte se rapporte à l'échec d'une fonction, les événements d'entrée correspondants peuvent être des pannes du matériel ou des limitations des performances de ce même matériel. Si l'événement de sortie désigne une panne du matériel, les événements d'entrée correspondants peuvent être des pannes du matériel, la perte des commandes et l'absence des principales alimentations, si c'est applicable et si ces événements ne sont pas déjà compris dans les limitations des performances.

L'élaboration d'un arbre de panne s'achève lorsque au moins l'un quelconque des types d'événements suivants a été atteint:

- événements de base, c'est-à-dire événements indépendants dont les caractéristiques à prendre en compte peuvent être définies par d'autres moyens qu'un arbre de panne;

actions should be known, as should the support equipment and personnel involved. Specific information on prescribed operating during each operational phase is also required.

In addition to the above, it is recommended to prepare a list of symbols, identification markings, conventions, and formats for data files, when necessary in a machine-readable form to permit the fault tree structure and description to be exchanged between computers.

6.3 *Events considered*

Events arising from all causes shall be included in the fault tree. Such causes should include the effects of all environmental or other conditions to which the item might be subjected including those which are possible during operation, even if outside the design specification.

Where relevant, fault trees should take into account the effects of mistakes and of deficiencies in computer software including that used for control and status monitoring.

Events which the analyst has considered, but excluded from further analysis as not applicable, should be documented but not included in the final fault tree.

If the fault tree highlights a system performance problem caused by an existing fault, then the event describing that fault should be included in the fault tree. It should be marked as an event which already exists. This should be done in order to consider the effect and order of multiple faults.

6.4 *Approaches*

Fault tree development starts with the definition of the top event. The top event is the output of the top gate, while the corresponding input events identify possible causes and conditions for the occurrence of the top event. Each input event may itself be an output event of a lower level gate.

If the output event of a gate defines the inability to perform of a function, the corresponding input events could be hardware faults or performance limitations. If the output event defines a hardware fault, the corresponding input events could be hardware faults, lack of control and essential supplies, if applicable and not already included as part of the performance limitations.

The development of a particular fault tree branch terminates after any one or more of the following have been reached:

- basic events; i.e. independent events for which the relevant characteristics can be defined by means other than a fault tree;

- événements qui n'ont pas besoin, selon l'analyste, d'être développés plus avant pour le moment;
- événements qui ont été ou seront développés plus avant dans un autre arbre de panne. Un événement qui fait l'objet d'une étude plus poussée dans un autre arbre de panne devra avoir le même repère que l'événement correspondant dans l'autre arbre de panne de sorte que le deuxième arbre soit bien le prolongement du premier.

7 Procédures

L'analyse par arbre de panne est effectuée par étapes. Les étapes particulières suivies pour un système donné peuvent ne pas être exactement les mêmes que celles qui sont suivies pour d'autres systèmes. Cependant, les étapes présentées ci-après sont des étapes fondamentales que l'on doit retrouver dans toutes les analyses par arbre de panne.

7.1 *Portée de l'analyse*

Pour définir la portée de l'analyse, il convient de préciser quel est le système à analyser, l'objectif et l'étendue de l'analyse ainsi que les hypothèses de base. Il est recommandé d'inclure dans ces hypothèses celles qui concernent les conditions prévues de fonctionnement et de maintenance ainsi que le fonctionnement du système dans toutes les conditions d'utilisation possibles.

7.2 *Approfondissement de la connaissance du système*

Pour réussir une analyse par arbre de panne, il faut avoir une connaissance approfondie du système. Cependant, certains systèmes sont trop complexes pour qu'une seule personne puisse en prendre pleinement connaissance. Dans ce cas, pour se familiariser avec le système, les analystes doivent acquérir les connaissances spécifiques nécessaires et les incorporer comme il convient à l'analyse par arbre de panne. Les informations dont on aura besoin pour ce faire sont énumérées en 5.2.

7.3 *Identification de l'événement de tête*

L'événement de tête est le point sur lequel est centrée toute l'analyse. Il peut s'agir de l'apparition ou de l'existence d'une condition dangereuse ou de l'incapacité du système à fonctionner comme prévu.

L'événement de tête sera défini, chaque fois que possible, en unités mesurables.

7.4 *Construction de l'arbre de panne*

7.4.1 *Présentation de l'arbre de panne*

Les arbres de panne peuvent être disposés soit verticalement soit horizontalement. Si l'on choisit la disposition verticale, il convient que l'événement de tête soit placé en haut de la page et les événements de base en bas. Dans le cas d'une présentation horizontale, l'événement de tête peut être situé à gauche ou à droite de la page.

Deux exemples (voir figures 1 et 2) permettent d'illustrer la manière dont un arbre de panne est élaboré et représenté. Les symboles utilisés pour ces exemples comprennent:

- une case comportant le libellé de l'événement;
- un symbole logique utilisé pour représenter les liaisons entre événements (portes);

- events which need not be developed further, as defined by the analyst;

- events which have been or will be developed further in another fault tree; if an event is developed further such an event must bear the same identification as the corresponding event on the other fault tree so that the latter tree effectively forms a continuation of the former.

7 Procedures

Fault tree analysis proceeds in steps. The specific steps followed for a particular system may not be exactly the same as those followed for another system. However, the following fundamental steps shall be common to all fault tree analyses.

7.1 *Scope of analysis*

The definition of the scope should include the definition of the system to be analyzed, the purpose and extent of the analysis and the basic assumptions made. These assumptions should include those related to the expected operating and maintenance conditions as well as to system performance under all possible conditions of use.

7.2 *System familiarization*

In order that a fault tree analysis may be carried out successfully, a detailed knowledge of the system is required. However, some systems may be too complex to be understood fully by one person. In this case, the process of familiarization requires that the necessary specialized knowledge be obtained and incorporated as appropriate into the fault tree analysis. The information necessary is noted in 5.2.

7.3 *Top event identification*

The top event is the focus of the entire analysis. Such an event may be the onset or existence of a dangerous condition, or the inability of the system to provide a desired performance.

The top event should be defined in measurable units, whenever possible.

7.4 *Fault tree construction*

7.4.1 *Fault tree format*

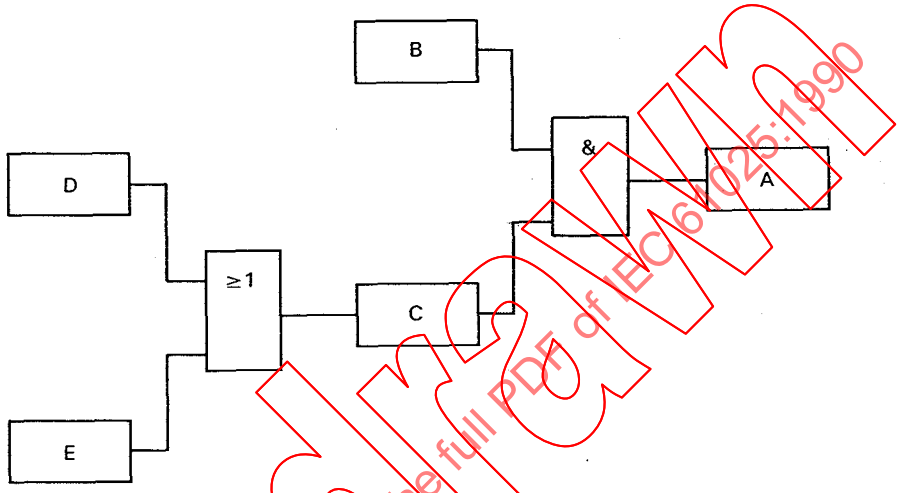
Fault trees may be drawn either vertically or horizontally. If the vertical arrangement is used, the top event should be at the top of the page and the basic events at the bottom. If the horizontal arrangement is used, the top event may be on the left or right of the page.

Two examples (see figures 1 and 2) are used to show the development and representation of a fault tree. Symbols used in these examples include:

- event description box;
- fault tree logic symbol (gates);

- une ligne d'entrée des portes;
- un symbole de report différé (cause commune);
- un symbole de report;
- un symbole de fin d'information (par exemple événement de base).

Sur la figure 1, l'événement A ne se produit que si les événements B et C ont lieu. L'événement C arrive si l'un des événements D ou E est survenu.



NOTE - Les informations qu'il convient d'inscrire pour chaque événement A, B, etc., dans la case de libellé de l'événement sont:

- code de l'événement;
- probabilité (s'il y a lieu);
- nom et description de l'événement.

Figure 1 - Exemple d'arbre de panne

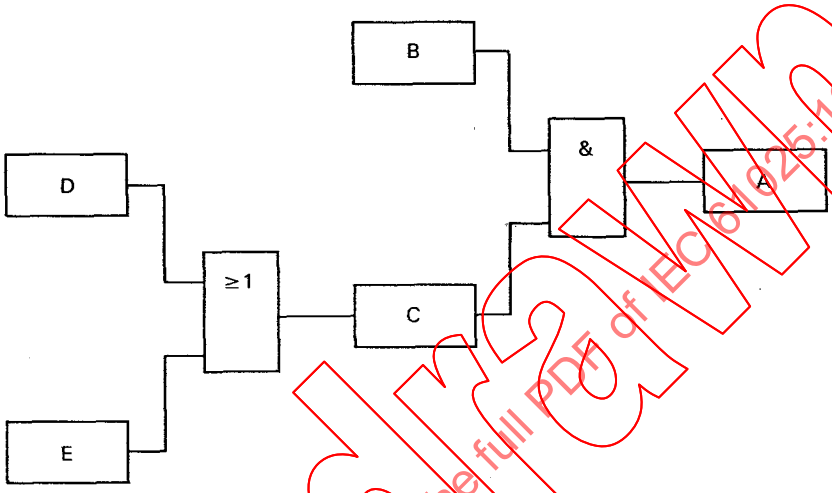
Si un événement correspond à une cause commune, il apparaît au niveau de l'arbre de panne sous forme d'un ensemble d'événements. Ces événements sont liés à tous les événements sur lesquels ils influent. Tous les événements communs de cet ensemble doivent posséder le même code et être désignés par un symbole de report, sauf l'événement de l'ensemble se trouvant au niveau le plus bas, qui est représenté par le symbole report différé.

Si l'arbre de panne est formé de plusieurs sous-arbres, un événement correspondant à une cause commune et apparaissant dans deux sous-arbres ou plus doit être représenté de la façon suivante:

- l'événement doit être indiqué par un symbole de fin d'information ou, s'il est plus développé ailleurs, par un symbole de report différé, dans un seul sous-arbre;
- dans le sous-arbre où le symbole de fin d'information ou de porte est utilisé, l'apparition d'un événement de cause commune dans les autres sous-arbres doit être signalé par un symbole de report.

- gate input connection line;
- transfer-out symbol (common cause);
- transfer-in symbol;
- terminating symbol (for example basic event).

In figure 1, event A will occur only if both events B and C occur. Event C is present if either event D or E occurs.



NOTE - For each event, A, B, etc., information to be included in the event description box includes

- event code;
- probability of occurrence (if required);
- name or description of event.

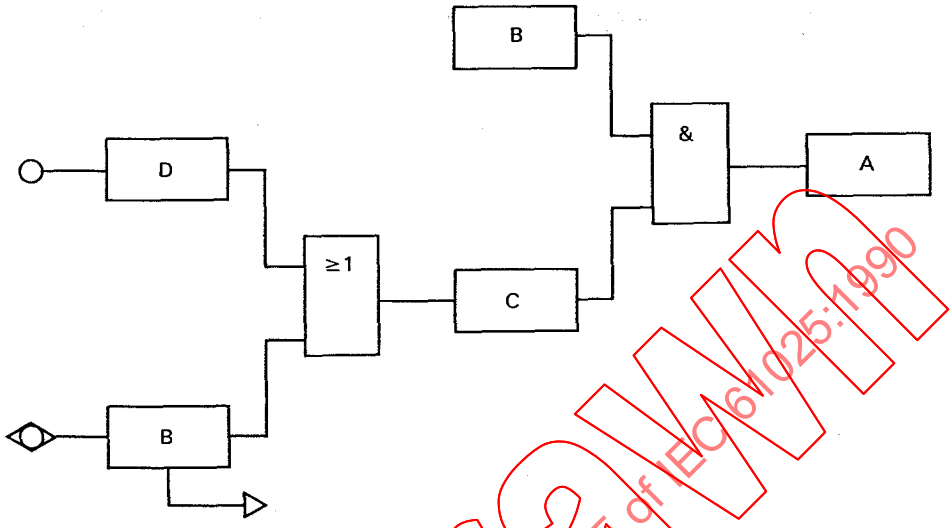
Figure 1 - Example of a fault tree

If an event represents a common cause, it is shown in the fault tree as a set of events. These events are linked to whatever events they affect. All common events in the set shall have the same event code and be marked by a transfer-in symbol, except the event on the lowest level in the set which is marked by a transfer-out symbol.

If the fault tree is presented in several sections, an event representing a common cause which appears on two or more of the sections shall be treated as follows:

- the event shall be marked with a terminating symbol or, if further developed, with a transfer-out gate symbol on only one of the sections;
- on the section where the terminating or gate symbol is used, the occurrence of the common event on other sections shall be indicated by a transfer-in gate symbol.

La figure 2 illustre un arbre de panne comportant des indications se rapportant à une cause commune. L'événement B est un événement de cause commune qui est développé plus avant dans un autre arbre de panne. L'événement D est un événement de base.



NOTE - Les informations qu'il convient d'inscrire pour chaque événement A, B, etc., dans la case de libellé de l'événement sont:

- code de l'événement;
- probabilité (s'il y a lieu);
- nom et description de l'événement.

Figure 2 - Exemple d'un arbre de panne comportant des indications se rapportant à la cause commune

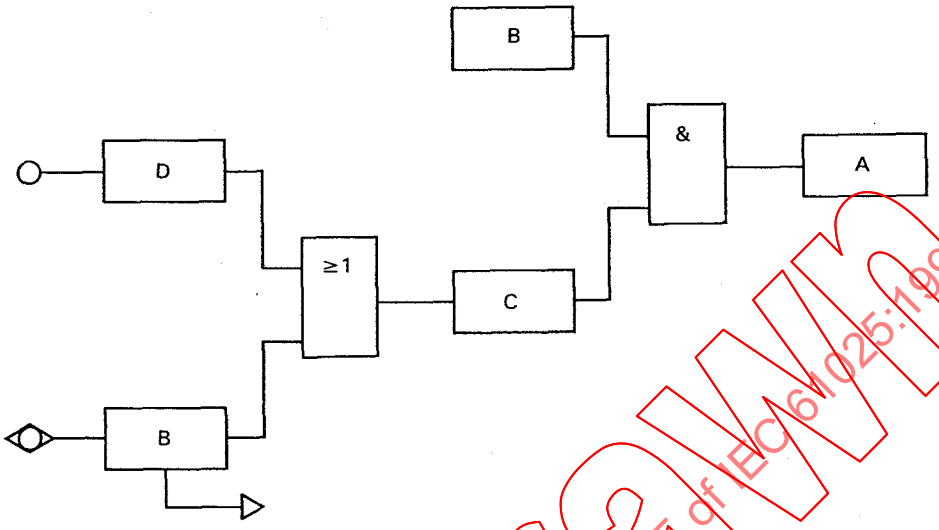
7.4.2 *Technique de construction*

Les documents fournis à l'appui des analyses de sûreté de fonctionnement seront présentés de sorte que l'on puisse revoir les résultats et incorporer toute modification jugée utile du fait de changement dans la conception et dans la procédure d'exploitation ou d'une meilleure compréhension des caractéristiques physiques de la défaillance. Pour cela, il faut que la construction puisse être effectuée de façon systématique. Une approche systématique implique la compréhension de deux concepts et leur emploi cohérent. Il s'agit des concepts de «cause immédiate» et «d'unité de base».

Le concept de «cause immédiate» nécessite que l'analyste détermine les causes immédiates nécessaires et suffisantes à l'apparition d'un événement de tête. Il y a lieu de noter qu'il ne s'agit pas des causes de base de l'événement mais des causes immédiates ou des mécanismes immédiats qui ont conduit à l'événement.

Les causes immédiates, nécessaires et suffisantes, d'un événement de tête sont maintenant traitées comme des événements situés directement en-dessous de l'événement de tête, et l'analyste cherche à déterminer leurs causes immédiates, nécessaires et suffisantes.

An example of a fault tree showing common cause considerations is shown in figure 2. Event B is a common cause event which is analyzed further on another fault tree. Event D is a basic event.



NOTE - For each event A, B, etc., information to be included in the event description box includes

- event code;
- probability of occurrence (if required);
- name or description of event.

Figure 2 - Example showing common cause considerations

7.4.2 *Construction procedure*

Dependability analyses should be documented in such a way that results can be reviewed and any changes needed can be incorporated in order to reflect changes in design, operating procedures or improved understanding of the physics of failure. In order that this may be done, a systematic approach to the construction is required. To implement this systematic approach, two concepts have to be understood and used consistently. These are the concepts of "immediate cause" and of "basic unit".

The "immediate cause" concept requires that the analyst determine the immediate necessary and sufficient causes for the occurrence of the top event. It should be noted that these are not the basic causes of the event but the immediate causes or immediate mechanisms for the event to occur.

The immediate, necessary and sufficient causes of the top event are now treated as sub-top events and the analyst proceeds to determine their immediate, necessary and sufficient causes.

Ainsi, l'analyste progresse vers le bas de l'arbre de panne, en passant sans cesse du mécanisme au mode et en affinant continuellement l'explication du mécanisme et des modes, jusqu'au moment où les limites de résolution de l'arbre sont atteintes.

Si l'on ne respecte pas strictement le concept de «cause immédiate», on risque d'omettre des modes de panne en croyant les avoir déjà inclus.

Le concept «d'unité de base» permet à l'analyste de ne pas élaborer des branches d'arbre de panne qui n'apporteraient pas d'informations nouvelles ou utiles. Une unité de base est traitée comme si elle était une unité ou un composant unique ou comme si elle était examinée séparément.

Pour qu'une unité soit considérée comme étant «de base», il faut et il suffit que les trois exigences suivantes soient satisfaites:

- les limites fonctionnelles et matérielles doivent être clairement définies;
- le fonctionnement de l'unité ne doit dépendre d'aucune fonction auxiliaire, ou bien tous les événements se rapportant à l'unité doivent être exprimés par une seule porte OU dont l'une des entrées représente une panne de l'unité, alors que les autres entrées représentent des incapacités à remplir les fonctions auxiliaires correspondantes;
- aucun événement ne doit se rapporter à la partie de l'unité qui apparaît ailleurs dans l'arbre de panne.

7.4.3 *Caractéristiques d'une panne*

L'analyste doit considérer soigneusement les pannes d'une entité, en particulier dans les catégories telles que panne première et panne seconde comme la conséquence des défaillance première et défaillance seconde.

Lorsque l'on cherche à classer une panne, on doit considérer les contraintes d'exploitation et d'environnement et les comparer aux contraintes maximales auxquelles le composant doit résister de par sa conception.

7.5 *Évaluation de l'arbre de panne*

Les analyses logiques (qualitatives) et numériques (quantitatives) ont essentiellement pour but:

- d'identifier les événements qui peuvent provoquer directement une défaillance du système, et la probabilité de ces événements;
- d'évaluer le niveau de défaillance toléré du système (capacité du système à continuer de fonctionner après qu'un nombre donné de défaillances ou d'événements mineurs conduisant à une défaillance du système soient survenus);
- de vérifier que la défaillance des systèmes, des sous-systèmes ou des composants est indépendante de toute autre;
- d'évaluer les données afin de pouvoir mettre en évidence les composants critiques et les mécanismes de défaillance;
- d'identifier les diagnostics de défaillance des dispositifs, les stratégies de réparation et de maintenance, etc.

In this way, the analyst proceeds down the tree transferring attention from mechanism to mode, and continually approaching a finer resolution of mechanism and modes, until ultimately the limit of resolution of the tree is reached.

Strict adherence to the concept of "immediate cause" is necessary to ensure that fault modes are not omitted by reason of the assumption that such modes have been included previously.

The concept of "basic units" can be used to save the analyst the effort of developing fault tree diagrams which do not yield new or useful information. A basic unit is treated as if it were a single unit or component or dealt with separately.

In order that the unit be considered "basic", it is necessary and sufficient that the following three requirements be satisfied:

- both the functional and physical boundaries shall be clearly defined;
- operation of the unit shall not depend on any supporting function, or all events related to the unit shall be expressed by a single OR gate having one of the inputs representing a fault of the unit, the remaining inputs representing inability to perform the corresponding support functions;
- no events shall be related to a part within the unit that appears elsewhere in the fault tree.

7.4.3 *Fault characteristics*

It is necessary for the analyst to consider carefully item faults, particularly in categories such as primary fault and secondary fault resulting from primary and secondary failures.

In determining the classification of a fault, consideration shall be given to the operating and environmental stresses and comparison made with the maximum stresses for which the item has been qualified.

7.5 *Fault tree evaluation*

The primary purposes of logical (qualitative) and numerical (quantitative) analyses of a system are:

- identification of events which can directly cause a system failure, and the probability of such events;
- assessment of fault tolerance of the system (ability to function even after a specified number of lower level failures or events contributing to the occurrence of a system failure have happened);
- verification of the independence of failure of systems, subsystems or components;
- assessment of data to locate critical components and failure mechanisms;
- identification of device failure diagnostics, inputs to repair and maintenance strategies, etc.

Pour évaluer le niveau de défaillance toléré d'un système, il faut déterminer le degré de redondance dans le système et vérifier que des événements de cause commune ne nuisent pas à cette redondance. Bien que l'on n'ait pas besoin d'utiliser de données numériques pour ce type d'analyse, celles-ci sont nécessaires pour trouver les combinaisons d'événements qui ont le plus de chances de se produire en provoquant une panne du système.

7.5.1 *Analyse logique*

Il existe trois techniques fondamentales pour effectuer l'analyse logique: l'investigation, la réduction booléenne et la définition de coupes minimales.

- Investigation

  L'investigation comprend l'étude de la structure de l'arbre de panne, l'identification des événements de cause commune et la recherche des branches indépendantes. L'investigation fournit à l'analyste des informations importantes qui, dans certains cas, sont suffisantes pour rendre inutile toute analyse complémentaire. Dans tous les autres cas, cette investigation est indispensable pour se prononcer sans se tromper sur le type et l'étendue des analyses complémentaires à effectuer. L'investigation visuelle directe d'un arbre tracé n'est réalisable qu'avec de petits arbres qui ne comportent pas plus d'environ 70 événements. L'investigation de plus grands arbres, comme ceux qui sont faits dans le cadre de l'analyse de systèmes réels, nécessite un outil informatique adapté, mais l'approche globale demeure la même.

  L'investigation commence par l'étude de la structure de l'arbre de panne. Tous les événements qui sont liés à l'événement de tête par une chaîne continue de portes OU sont des événements qui produisent l'événement de tête. De ce fait, si un arbre de panne n'est formé que de portes OU, toute analyse complémentaire est inutile. Si, par contre, l'arbre de panne comporte d'autres types de portes, le système analysé comprend un certain type de redondance ou d'autres éléments permettant d'éviter les défauts qui pourraient être rendus inopérants par des événements de cause commune. L'investigation devrait permettre de dépister des événements de cause commune mais ne devrait en aucune façon, amener l'analyste à conclure que leur présence est insignifiante. Il ne peut en effet aboutir à cette conclusion qu'après une analyse approfondie par réduction booléenne ou détermination de coupes minimales. Comme la difficulté de l'analyse croît rapidement avec la taille de l'arbre de panne, l'investigation de l'arbre aide l'analyste à savoir quelles branches sont indépendantes du reste de l'arbre et peuvent donc être analysées séparément.

- Réduction booléenne

  La réduction booléenne sert à évaluer les effets des événements de cause commune (événements identiques apparaissant dans des branches différentes) dans les arbres de panne où l'événement de tête est indépendant du moment et de l'ordre d'apparition des événements. Pour procéder à une réduction booléenne, on peut résoudre les équations de Boole se rapportant à l'arbre de panne.

- Méthode des coupes minimales

  Il existe plusieurs méthodes permettant de définir les coupes minimales, mais elles peuvent être difficiles à appliquer à des arbres plus grands et, dans ce cas, elles risquent d'être à l'origine de lacunes. C'est pourquoi il existe divers programmes informatiques pour aider l'analyste dans sa tâche.

The assessment of fault tolerance of the system includes a determination of the degree of redundancy in the system and a verification that the redundancy is not impaired through common events (common cause events). Although the major part of fault tolerance assessment does not require the use of numerical data, such numerical data are required to evaluate which combinations of events causing a system fault are the most likely to occur.

7.5.1 *Logical analysis*

Three basic techniques are used for logical analysis: investigation, boolean reduction and determination of minimal cut sets.

- Investigation

  Investigation includes a review of the fault tree structure, identification of common events and a search for independent branches. Investigation provides the analyst with important information which, in some cases, may be sufficient to eliminate the need for further analyses. In all other cases, investigation is necessary for a correct decision on the type and extent of further analyses. Direct visual investigation of a plotted tree is possible only for small trees, not exceeding about 70 events. Investigation of larger trees, as arise from the analysis of actual systems, requires a suitable computer tool, but the overall approach remains the same.

  Investigation starts with the review of the fault tree structure. All events which are linked to the top event through a continuous chain of OR gates are events which cause the top event to occur. Therefore, if a fault tree consists only of OR gates, no further analysis is required. If the fault tree includes other gate types, the analyzed system incorporates some sort of redundancy or other fault prevention features which could be invalidated by common cause events. Investigation should identify common cause events, but should not assume that their presence is benign. Such conclusions can be drawn only after a thorough analysis using boolean reduction or determination of minimal cut sets. As the difficulty of the analysis increases rapidly with the size of the fault tree, inspection of the fault tree allows the analyst to identify which branches of the fault tree are independent and can thus be analyzed separately.

- Boolean reduction

  Boolean reduction is used for the evaluation of the effects of common events (identical events occurring in different branches) in fault trees where the occurrence of the top event does not depend on timing or sequencing of events. Boolean reduction can be carried out by solving boolean equations for the fault tree.

- Methods of minimal cut sets

  There are several methods of determining minimal cut sets but application to larger trees may be difficult and incomplete. Various computer programs are available to assist the analyst.

Une coupe est un groupe d'événements qui, lorsqu'ils se produisent conjointement, sont (peuvent être) à l'origine de l'événement de tête. Une coupe minimale est le plus petit de ces groupes dont tous les événements doivent se produire (dans le bon ordre) pour que l'événement de tête ait lieu. Si l'un de ces événements ne survient pas, l'événement de tête ne peut arriver. Les mots cités entre parenthèses dans la définition ci-avant permettent d'élargir la définition des coupes minimales à des arbres de panne qui dépendent de l'ordre des événements. Dans ces cas, la coupe minimale définit le groupe d'événements qui peut être à l'origine de l'événement de tête. Les effets de l'ordre des événements dans ce groupe peuvent être analysés à l'aide d'un diagramme de transition d'état qui, toutefois, n'entre pas dans le cadre de cette norme.

7.5.2 *Analyse numérique*

Cette analyse a pour but de parvenir à une estimation quantitative de l'apparition d'un événement de tête ou d'un ensemble choisi d'événements. L'analyse numérique est également une aide et un complément lorsqu'on effectue une analyse logique. Pour procéder à l'évaluation numérique d'un arbre de panne, on a besoin de données probabilistes sur les composants. Les techniques de prévision de fiabilité et disponibilité, les résultats des essais ou les données recueillies en exploitation peuvent servir à déterminer les valeurs quantitatives.

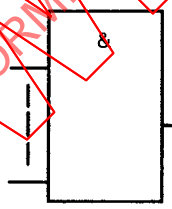
7.5.3 *Exemples d'une évaluation simple fondée sur l'algèbre de Boole appliquée à l'analyse par arbre de panne*

- Application à l'analyse par arbre de panne

Dans les arbres de panne qui ne sont constitués que de portes ET, OU et NON, chaque élément de la représentation booléenne correspond à un élément de la représentation par arbre de panne.

Le symbole 

employé dans l'arbre de panne est une porte OU qui traduit l'union des événements reliés à cette porte. La porte OU correspond au symbole booléen «+».

Le symbole 

employé dans l'arbre de panne est une porte ET qui représente l'intersection des événements reliés à cette porte. La porte ET correspond au symbole booléen «·».

Les symboles OU et ET de l'algèbre de Boole peuvent être remplacés par d'autres symboles, comme ceux qui sont utilisés dans de nombreux langages de programmation d'ordinateurs. Il faudra cependant s'assurer que l'ensemble est homogène.

Prenons l'arbre de panne présenté sur la figure 1. On peut écrire

$$C = D + E$$
$$A = B \cdot C = B \cdot (D + E)$$

A cut set is a group of events which, when occurring together, (may) cause the top event to happen. A minimal cut set is the smallest such group in which all events must occur (in proper sequence) for the top event to occur. If any of the events in a minimal cut set does not occur, it prevents the top event from occurring. The words in parentheses in the definition above extend the definition of minimal cut sets to fault trees dependent on sequencing of events. In those instances, the minimal cut set determines the group of events with the potential to cause the top event. The effects of sequencing of events in this group can be analyzed using the state-transition diagram, which, however, is beyond the scope of this standard.

7.5.2 *Numerical analysis*

The purpose of numerical analysis is to provide a quantitative assessment of the probability of occurrence of the top event or a selected set of events. Numerical analysis is also used to support and to supplement the logical analysis. In order to perform a numerical evaluation of a fault tree, probabilistic data at the component level are required. Reliability and availability prediction techniques, actual test or field use data may be used to establish the quantitative values.

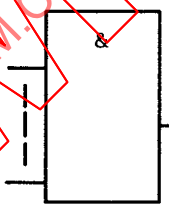
7.5.3 *Examples of a simple evaluation using boolean algebra applied to fault tree analysis*

- Application to fault tree analysis

In fault trees which consist only of AND, OR and NOT gates, there is a one-to-one correspondence between the boolean algebraic expression and the fault tree representation.

The fault tree symbol 

is an OR gate which represents the union of the events attached to the gate. The OR gate is equivalent to the boolean symbol "+".

The fault tree symbol 

is an AND gate which represents the intersection of the events attached to the gate. The AND gate is equivalent to the boolean symbol "·".

OR and AND symbols for boolean algebra may be expressed with other symbology, such as that used with many computer program languages. Consistency is required, however.

Considering the fault tree as shown in figure 1, we can write

$$C = D + E$$
$$A = B \cdot C = B \cdot (D + E)$$

Si l'on applique la loi de distributivité, on obtient

$$A = B \cdot D + B \cdot E$$

- Application aux coupes minimales

L'événement de tête peut être exprimé en fonction d'un nombre fini de coupes minimales qui n'appartiennent qu'à cet événement de tête.

La forme générale de cette expression est

$$T = M_1 + M_2 + ... + M_i + ... + M_p$$

où T est l'événement de tête et où M_i sont les coupes minimales. Chaque coupe minimale comprend une combinaison de défaillances spécifiques de composants, et la coupe minimale générale peut s'écrire:

$$M = X_1 \cdot X_2 \cdot ... \cdot X_i \cdot ... \cdot X_c$$

où X_i est un événement de base de l'arbre.

Prenons l'arbre de panne de la figure 1. Les coupes minimales de l'événement de tête sont, dans ce cas, B · D et B · E.

8 Repères et libellés

Chaque événement de l'arbre de panne doit avoir un repère qui lui soit propre. Il convient que les événements soient libellés de telle sorte que l'on puisse facilement retrouver, à l'aide de l'arbre de panne, la documentation sur la conception correspondante.

L'événement de tête de l'arbre de panne est l'événement indésirable qui constitue la raison d'être de l'analyse par arbre de panne. Il est à noter qu'un seul événement de tête peut être associé à un arbre de panne donné.

Si plusieurs événements de l'arbre de panne concernent tous différents modes de panne d'une même entité, il convient de désigner ces événements de façon à pouvoir les distinguer. En même temps, il convient de faire apparaître clairement qu'ils constituent un groupe d'événements se rapportant à la même entité.

Si un événement donné, par exemple l'incapacité de fermeture d'une vanne particulière revient en différents points de l'arbre ou si cet événement apparaît dans plusieurs arbres, tous ces événements doivent être libellés de la même manière. Toutefois, des événements similaires mais concernant différentes entités ne doivent pas avoir le même repère.

Le code d'un événement devra contenir des informations sur l'identification du système, l'identification du composant et le mode de panne.

L'arbre de panne est en fait un diagramme dans lequel les événements sont reliés par des portes logiques. A chaque porte correspond un seul événement de sortie mais un ou plusieurs événements d'entrée.

Applying the distributive law, we have

$$A = B \cdot D + B \cdot E$$

- Application to minimal cut sets

The expression for the top event can be written in terms of a finite number of minimal cut sets, which are unique to that top event.

The general form is

$$T = M_1 + M_2 + ... + M_i + ... + M_p$$

where T is the top event and M_i are the minimal cut sets. Each minimal cut set consists of a combination of specific component faults, and the general minimal cut set can be expressed as

$$M = X_1 \cdot X_2 \cdot ... \cdot X_i \cdot ... \cdot X_c$$

where X_i is a basic event on the tree.

Consider the fault tree shown in figure 1. The minimal cut sets of the top event are in this case B · D and B · E.

8 Identification and labelling

Each event in the fault tree shall be uniquely identified. Events should be labelled so that cross reference from the fault tree to the corresponding design documentation can easily be made.

The top event of the fault tree is the undesirable event which is the primary reason for undertaking the fault tree analysis. It should be noted that only a single top event may be associated with a given fault tree.

If several events in a fault tree all refer to different fault modes of the same item, then such events shall be labelled so as to enable them to be distinguished. At the same time it should be clear that they are a group of events related to the same item.

If a particular event, for example inability of a particular valve to close, occurs in several places in a tree, or if it occurs in several trees, all such occurrences shall bear the same label. However, events which are similar but which involve different items shall not bear the same identification.

A typical event code should contain information relating to system identification, component identification and fault mode.

The fault tree is in effect a diagram in which the events are linked by logic gates. Each gate has one output event but one or more input events.

Les événements d'entrée identifient des causes ou des conditions possibles de l'apparition des événements de sortie. Cependant, ce mode de liaison ne donne pas nécessairement une relation séquentielle (temporelle) entre les événements.

Dans l'arbre de panne courant on utilise essentiellement des portes ET, OU et NON. Toutefois, quand on analyse des systèmes complexes, il est parfois nécessaire d'utiliser d'autres symboles pour les portes afin d'être sûr que les arbres de panne sont lisibles et aussi simples que possible. On trouvera dans l'annexe A les principaux symboles normalisés qui sont conformes à la CEI 617-12 ainsi que d'autres symboles utilisables en alternative. Si besoin est, on pourra élaborer un éventail supplémentaire de symboles plus spécialisés. Toutefois, il importe que l'analyste définisse et signale les symboles qu'il utilise et s'assure que les mêmes symboles sont employés de façon cohérente tout au long d'une même analyse par arbre de panne. C'est d'autant plus vrai que les techniques employées s'appuient sur l'informatique (voir la fin de 6.2).

Pour l'élaboration de l'arbre de panne, il convient que l'analyste emploie, en outre, les symboles et les repères appropriés pour signaler, selon le cas

- que l'événement, ou une branche entière, est également utilisé dans une autre partie de l'arbre;
- que la partie de l'arbre qui est décrite contient des événements qui apparaissent également dans d'autres parties de l'arbre;
- qu'un événement commun apparaissant dans une partie de l'analyse est davantage développé ailleurs.

Il est nécessaire de suivre cette recommandation pour les représentations graphiques des arbres de panne.

9 Rapport

Il convient que le rapport sur l'analyse par arbre de panne comprenne au moins les éléments de base cités plus loin. Des informations complémentaires peuvent être fournies par souci de clarté, surtout dans le cas d'analyse de systèmes complexes. Aucun format spécial n'est proposé dans cette norme.

Il convient que le rapport comprenne les éléments de base suivants

- objectif et domaine d'application;
- description du système
  a) description de la conception
  b) fonctionnement du système
  c) définitions détaillées des limites du système;
- hypothèses
  a) hypothèses relatives à la conception du système
  b) hypothèses se rapportant aux contrôles, aux essais, à la maintenance et au fonctionnement
  c) hypothèses pour les modèles de fiabilité et de disponibilité;
- définition et critères de panne du système;

The input events identify possible causes and conditions for the occurrence of the output events. However, such linking does not necessarily define the sequential (time) relationship between the events.

The basic fault tree uses AND, OR and NOT gates. However, for complex systems analysis, additional gate symbols may be required to assure that the fault trees are readable and as simple as possible. Annex A shows the standardized basic symbols in accordance with IEC 617-12, together with possible alternatives. A supplementary set of more specialized symbols may be developed if required. However, it is important for the analyst to define and report those symbols being used and ensure uniform and consistent use throughout a given fault tree analysis. This is particularly true if computer-aided techniques are to be used (see end of 6.2).

In developing the fault tree, the analyst should also use appropriate symbology and identification to make it clear, when applicable, that

- the event or whole branch is also used elsewhere in the tree;
- the depicted part of the tree includes events used also in another part of the tree;
- a common cause event shown in one part of the analysis is further developed elsewhere.

This is necessary for the graphical presentation of fault trees.

9 Report

The report of the fault tree analysis should include as a minimum the basic items listed below. Additional and supplementary information may be provided to increase clarity, especially in cases of complex systems analyses. A prescribed format is not proposed by this standard.

Basic items in the report should be

- objective and scope;
- system description
  a) design description
  b) system operation
  c) detailed system boundaries definitions;
- assumptions
  a) system design assumptions
  b) operation, maintenance, test and inspection assumptions
  c) reliability and availability modelling assumptions;
- system fault definition and criteria;

- analyse par arbre de panne

  a) analyse
  b) données
  c) symboles utilisés;

- résultats et conclusions.

Les données complémentaires qui peuvent être incluses sont

- organigramme du système ou diagrammes du circuit;
- résumé des données de fiabilité et de maintenabilité et sources utilisées;
- description de l'arbre de panne exploitable par un ordinateur (pour les analyses de systèmes complexes).

- fault tree analysis
  a) analysis
  b) data
  c) symbols used;

- results and conclusions.

Supplementary data items which may be included are

- system block or circuit diagrams;
- summary of reliability and maintainability data and sources used;
- fault tree description in computer readable form (for complex systems analyses).