IEC 61025

Edition 2.0 2006-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Fault tree analysis (FTA)

Analyse par arbre de panne (AAP)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XA
CODE PRIX

ICS 03.120.01; 03.120.99

ISBN 2-8318-8918-9

CONTENTS

FOREWORD 4
INTRODUCTION 6

1 Scope 7
2 Normative references 7
3 Terms and definitions 7
4 Symbols 10
5 General 11
5.1 Fault tree description and structure 11
5.2 Objectives 12
5.3 Applications 12
5.4 Combinations with other reliability analysis techniques 13
6 Development and evaluation 15
6.1 General considerations 15
6.2 Required system information 18
6.3 Fault tree graphical description and structure 19
7 Fault tree development and evaluation 20
7.1 General 20
7.2 Scope of analysis 20
7.3 System familiarization 20
7.4 Fault tree development 20
7.5 Fault tree construction 21
7.6 Failure rates in fault tree analysis 38
8 Identification and labelling in a fault tree 38
9 Report 39

Annex A (informative) Symbols 41
Annex B (informative) Detailed procedure for disjointing 48

Bibliography 52

Figure 1 – Explanation of terms used in fault tree analyses 10
Figure 2 – Fault tree representation of a series structure 23
Figure 3 – Fault tree representation of parallel, active redundancy 24
Figure 4 – En example of fault tree showing different gate types 26
Figure 5 – Rectangular gate and events representation 27
Figure 6 – An example fault tree containing a repeated and a transfer event 28
Figure 7 – Example showing common cause considerations in rectangular gate representation 28
Figure 8 – Bridge circuit example to be analysed by a fault tree 32
Figure 9 – Fault tree representation of the bridge circuit 33
Figure 10 – Bridge system FTA, Esary-Proschan, no disjointing 35

Figure 11 – Bridge system probability of failure calculated with rare-event approximation 36
Figure 12 – Probability of occurrence of the top event with disjointing 37
Figure A.1 – Example of a PAND gate 47

Table A.1 – Frequently used symbols for a fault tree 41
Table A.2 – Common symbols for events and event description 44
Table A.3 – Static gates 45
Table A.4 – Dynamic gates 46

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FAULT TREE ANALYSIS (FTA)

FOREWORD

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

International Standard IEC 61025 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1142/FDIS	56/1162/RVD

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

This second edition cancels and replaces the first edition, published in 1990, and constitutes a technical revision.

The main changes with respect to the previous edition are as follows:

– added detailed explanations of fault tree methodologies
– added quantitative and reliability aspects of Fault Tree Analysis (FTA)
– expanded relationship with other dependability techniques
– added examples of analyses and methods explained in this standard
– updated symbols currently in use

Clause 7, dealing with analysis, has been revised to address traditional logic fault tree analysis separately from the quantitative analysis that has been used for many years already, for reliability improvement of products in their development stage.

Some material included previously in the body of this standard has been transferred to Annexes A and B.

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

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

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

INTRODUCTION

Fault tree analysis (FTA) is concerned with the identification and analysis of conditions and factors that cause or may potentially cause or contribute to the occurrence of a defined top event. With FTA this event is usually seizure or degradation of system perfomance, safety or other important operational attributes, while with STA (success tree analysis) this event is the attribute describing the success.

FTA is often applied to the safety analysis of systems (such as transportation systems, power plants, or any other systems that might require evaluation of safety of their operation). Fault tree analysis can be also used for availability and maintainability analysis. However, for simplicity, in the rest of this standard the term “reliability” will be used to represent these aspects of system performance.

This standard addresses two approaches to FTA. One is a qualitative approach, where the probability of events and their contributing factors, – input events – or their frequency of occurrence is not addressed. This approach is a detailed analysis of events/faults and is known as a qualitative or traditional FTA. It is largely used in nuclear industry applications and many other instances where the potential causes or faults are sought out, without interest in their likelihood of occurrence. At times, some events in the traditional FTA are investigated quantitatively, but these calculations are disassociated with any overall reliability concepts, in which case, no attempt to calculate overall reliability using FTA is made. The second approach, adopted by many industries, is largely quantitative, where a detailed FTA models an entire product, process or system, and the vast majority of the basic events, whether faults or events, has a probability of occurrence determined by analysis or test. In this case, the final result is the probability of occurrence of a top event representing reliability or probability of fault or a failure.

FAULT TREE ANALYSIS (FTA)

1 Scope

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

– definition of basic principles;
  - describing and explaining the associated mathematical modelling;
  - explaining the relationships of FTA to other reliability modelling techniques;
– description of the steps involved in performing the FTA;
– identification of appropriate assumptions, events and failure modes;
– identification and description of commonly used symbols.

2 Normative references

The following referenced documents are indispensable for the application of this document. For the references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050(191), *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 61165, *Application of Markov techniques*

SOMMAIRE

AVANT-PROPOS 56
INTRODUCTION 58

1 Domaine d'application 59
2 Références normatives 59
3 Termes et définitions 59
4 Symboles 62
5 Généralités 63
5.1 Structure et description de l'arbre de panne 63
5.2 Objectifs 64
5.3 Applications 64
5.4 Combinaisons avec d'autres techniques d'analyse de fiabilité 65
6 Développement et évaluation 67
6.1 Considérations générales 67
6.2 Information du système exigée 70
6.3 Structure et description graphique de l'arbre de panne 71
7 Elaboration et évaluation de l'arbre de panne 72
7.1 Généralités 72
7.2 Portée de l'analyse 72
7.3 Approfondissement de la connaissance du système 72
7.4 Elaboration de l'arbre de panne 72
7.5 Construction de l'arbre de panne 73
7.6 Taux de défaillance dans l'analyse de l'arbre de panne 90
8 Repères et étiquettes dans un arbre de panne 90
9 Rapport 91

Annexe A (informative) Symboles 93
Annexe B (informative) Procédure de disjonction détaillée 100

Bibliographie 104

Figure 1 – Explication des définitions utilisées dans les analyses par arbre de panne 62
Figure 2 – Représentation de l'arbre de panne d'une structure en série 75
Figure 3 – Représentation de l'arbre de panne de redondance parallèle, active 76
Figure 4 – Un exemple d'arbre de panne montrant différents types de porte 78
Figure 5 – Porte rectangulaire et représentation des événements 79
Figure 6 – Un exemple d'arbre de panne contenant un événement de transfert et un événement répété 80
Figure 7 – Exemple présentant des indications se rapportant à une cause commune dans une représentation de porte rectangulaire 80
Figure 8 – Exemple de circuit à embranchement à analyser par arbre de panne 84
Figure 9 – Représentation de l'arbre de panne du circuit à embranchement 85
Figure 10 – AAP Système à embranchement – Esary Proschan, pas de disjonction 87

Figure 11 – Probabilité de défaillance du système à embranchement calculée avec une approximation de l'événement rare 88
Figure 12 – Probabilité d'apparition de l'événement de tête avec disjonction 89
Figure A.1 – Exemple d'une porte PAND 99

Tableau A.1 – Symboles fréquemment utilisés pour un arbre de panne..... 93
Tableau A.2 – Symboles communs pour les événements et la description des événements..... 96
Tableau A.3 – Portes statiques 97
Tableau A.4 – Portes dynamiques..... 98

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

ANALYSE PAR ARBRE DE PANNE (AAP)

AVANT-PROPOS

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

La Norme internationale CEI 61025 a été préparée par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de la présente norme est issu des documents suivants:

FDIS	Rapport de vote
56/1142/FDIS	56/1162/FDIS

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

Cette deuxième édition annule et remplace la première édition publiée en 1990. Elle constitue une révision technique.

Les principaux changements par rapport à l'édition précédente sont les suivants:

– ajout d'explications détaillées sur les méthodologies de l'arbre de panne
– ajout d'aspects quantitatifs et d'aspects de fiabilité sur l'Analyse par Arbre de Panne (AAP)
– extension de la relation avec d'autres techniques de sûreté de fonctionnement
– ajout d'exemples d'analyses et de méthodes expliqués dans cette norme
– mise à jour des symboles couramment utilisés

L'Article 7 concernant les analyses a été modifié afin de traiter l'analyse par arbre de panne logique traditionnelle séparément de l'analyse quantitative utilisée depuis de nombreuses années, pour l'amélioration de la fiabilité des produits pendant leur développement.

Certaines parties intégrées précédemment dans le corps de cette norme, ont été transférées aux Annexes A et B.

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

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

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

INTRODUCTION

L'AAP sert à déterminer et à analyser les conditions et les facteurs qui produisent, peuvent potentiellement produire ou contribuent à produire un événement indésirable défini. Pour l'AAP, cet événement est généralement un «grippage» ou une dégradation des performances du système, de la sécurité ou d'autres attributs fonctionnels importants, alors qu'avec l'analyse par arbre de succès (STA = Success Tree Analysis) cet événement est l'attribut décrivant le succès.

L'AAP est souvent appliquée aux analyses pour la sécurité des systèmes (tels que les systèmes de transport, les centrales électriques, ou tout autre système pouvant nécessiter une évaluation de la sécurité de leur fonctionnement). L'analyse par arbre de panne peut également être utilisée pour les analyses de disponibilité et de maintenabilité. Cependant, dans le reste de cette norme, à fin de simplification, le terme de fiabilité sera utilisé pour représenter ces aspects de performance du système.

Dans cette norme, deux approches de l'AAP sont traitées. L'une d'elles est une approche qualitative, où la probabilité des événements et leurs facteurs de contribution – les événements d'entrée ou leur fréquence d'apparition n'est pas traitée. Cette approche est une analyse détaillée des événements/pannes et est connue comme AAP Qualitative ou traditionnelle. Elle est largement utilisée dans les applications de l'industrie nucléaire et de nombreuses autres instances où les causes potentielles, – les pannes sont recherchées quelque soit leur fréquence d'apparition. Parfois, certains événements dans l'analyse traditionnelle sont étudier quantitativement, mais ces calculs sont dissociés de tout autre concept de fiabilité d'ensemble, auquel cas, aucune tentative pour calculer la fiabilité d'ensemble en utilisant l'AAP n'est faite. La seconde approche adoptée par de nombreuses industries est largement quantitative, dans les cas d'AAP qui modélisent un produit complet, un procédé, ou un système et la grande majorité d'événements de base, pannes ou événements, qui a une probabilité d'apparition déterminée par analyse ou essai. Dans ce cas, le résultat final est la probabilité d'apparition d'un événement de tête représentant la fiabilité ou la probabilité d'une panne ou d'une défaillance.

ANALYSE PAR ARBRE DE PANNE (AAP)

1 Domaine d'application

La présente Norme internationale décrit l'analyse par arbre de panne et donne des lignes directrices sur son application comme suit:

– définition des principes de base;
  - en définissant et en expliquant la modélisation mathématique associée;
  - en expliquant les relations entre l'AAP et d'autres techniques de modèle de fiabilité;
– description des étapes impliquées dans la réalisation de l'AAP;
– identification des hypothèses appropriées, des événements et des modes de défaillance;
– identification et description des symboles couramment utilisés.

2 Références normatives

Les documents référencés suivants sont indispensables pour l'application de ce document. Pour des références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition du document référencé (y compris les amendements) qui s'applique.

CEI 60050(191), *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service.*

CEI 61165, *Application des techniques de Markov*