IEC 62502

Edition 1.0 2010-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Analysis techniques for dependability – Event tree analysis (ETA)

Techniques d'analyse de la sûreté de fonctionnement – Analyse par arbre d'événement (AAE)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

X

ICS 21.020

ISBN 978-2-88912-212-7

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms, definitions, abbreviations and symbols 7
3.1 Terms and definitions 7
3.2 Abbreviations and symbols 8
3.2.1 Abbreviations 8
3.2.2 Symbols 9
4 General description 9
5 Benefits and limitations of ETA 11
5.1 Benefits 11
5.2 Limitations 11
6 Relationship with other analysis techniques 12
6.1 Combination of ETA and FTA 12
6.2 Layer of protection analysis (LOPA) 13
6.3 Combination with other techniques 13
7 Development of event trees 14
7.1 General 14
7.2 Steps in ETA 14
7.2.1 Procedure 14
7.2.2 Step 1: Definition of the system or activity of interest 15
7.2.3 Step 2: Identification of the initiating events of interest 15
7.2.4 Step 3: Identification of mitigating factors and physical phenomena 16
7.2.5 Step 4: Definition of sequences and outcomes, and their quantification 16
7.2.6 Step 5: Analysis of the outcomes 17
7.2.7 Step 6: Uses of ETA results 17
8 Evaluation 18
8.1 Preliminary remarks 18
8.2 Qualitative analysis – Managing dependencies 18
8.2.1 General 18
8.2.2 Functional dependencies 19
8.2.3 Structural or physical dependencies 20
8.3 Quantitative analysis 22
8.3.1 Independent sequence of events 22
8.3.2 Fault tree linking and boolean reduction 23
9 Documentation 24
Annex A (informative) Graphical representation 26
Annex B (informative) Examples 27
Bibliography 41

Figure 1 – Process for development of event trees 10
Figure 2 – Simple graphical representation of an event tree 18
Figure 3 – Functional dependencies in event trees 20

Figure 4 – Modelling of structural or physical dependencies 21
Figure 5 – Sequence of events 22
Figure 6 – Fault tree linking 23
Figure A.1 – Frequently used graphical representation for event trees 26
Figure B.1 – Event tree for a typical fire incident in a diesel generator building 28
Figure B.2 – Simplified event tree for a fire event 29
Figure B.3 – Level-crossing system (LX) 31
Figure B.4 – ETA for the level-crossing system 33
Figure B.5 – Simple example 36
Figure B.6 – Fault Tree for the Failure of System 1 36
Figure B.7 – Fault Tree for the Failure of System 2 37
Figure B.8 – Modified event tree 38
Figure B.9 – Event tree with "grouped faults" 39

Table A.1 – Graphical elements 26
Table B.1 – Symbols used in Annex B 29
Table B.2 – System overview 31
Table B.3 – Risk reduction parameters for accidents from Figure B.4 34

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ANALYSIS TECHNIQUES FOR DEPENDABILITY – EVENT TREE ANALYSIS (ETA)

FOREWORD

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

International Standard IEC 62502 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1380/FDIS	56/1389/RVD

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

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

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

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

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

INTRODUCTION

This International Standard defines the basic principles and procedures for the dependability technique known as Event Tree Analysis (ETA).

IEC 60300-3-1 explicitly lists ETA as an applicable method for general dependability assessment. It is also used in risk and safety analysis studies. ETA is also briefly described in the IEC 60300-3-9.

The basic principles of this methodology have not changed since the conception of the technique in the 1960's. ETA was first successfully used in the nuclear industry in a study by the U.S. Nuclear Regulatory Commission, the so-called WASH 1400 report in the year 1975 [31][1].

Over the following years, ETA has gained widespread acceptance as a mature methodology for dependability and risk analysis and is applied in diverse industry branches ranging from the aviation industry, nuclear installations, the automotive industry, chemical processing, offshore oil and gas production, to defence industry and transportation systems.

In contrast to some other dependability techniques such as Markov modelling, ETA is based on relatively elementary mathematical principles. However, as mentioned in IEC 60300-3-1, the implementation of ETA requires a high degree of expertise in the application of the technique. This is due in part to the fact that particular care has to be taken when dealing with dependent events. Furthermore, one can utilize the close relationship between Fault Tree Analysis (FTA) and the qualitative and quantitative analysis of event trees.

This standard aims at defining the consolidated basic principles of the ETA and the current usage of the technique as a means for assessing the dependability and risk related measures of a system.

---

[1] Figures in square brackets refer to the bibliography.

ANALYSIS TECHNIQUES FOR DEPENDABILITY – EVENT TREE ANALYSIS (ETA)

1 Scope

This International Standard specifies the consolidated basic principles of Event Tree Analysis (ETA) and provides guidance on modelling the consequences of an initiating event as well as analysing these consequences qualitatively and quantitatively in the context of dependability and risk related measures.

More specifically, this standard deals with the following topics in relation to event trees:

a) defining the essential terms and describing the usage of symbols and ways of graphical representation;

b) specifying the procedural steps involved in the construction of the event tree;

c) elaborating on the assumptions, limitations and benefits of performing the analysis;

d) identifying relationships with other dependability and risk-related techniques and elucidating suitable fields of applications;

e) giving guidelines for the qualitative and quantitative aspects of the evaluation;

f) providing practical examples.

This standard is applicable to all industries where the dependability and risk-related measures for the consequences of an initiating event have to be assessed.

2 Normative references

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

IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 61025:2006*, Fault tree analysis (FTA)*

SOMMAIRE

AVANT-PROPOS 46
INTRODUCTION 48
1 Domaine d'application 49
2 Références normatives 49
3 Termes, définitions, abréviations et symboles 49
3.1 Termes et définitions 49
3.2 Abréviations et symboles 51
3.2.1 Abréviations 51
3.2.2 Symboles 51
4 Description générale 52
5 Avantages et limites de l'AAE 53
5.1 Avantages 53
5.2 Limites 53
6 Relation avec d'autres techniques d'analyse 54
6.1 Combinaison de l'AAE et de l'AAP 54
6.2 Analyse des niveaux de protection (LOPA) 56
6.3 Combinaison avec d'autres techniques 56
7 Développement des arbres d'événement 56
7.1 Généralités 56
7.2 Étapes de l'analyse par arbre d'événement 57
7.2.1 Mode opératoire 57
7.2.2 Étape 1: Définition du système ou de l'activité considéré(e) 57
7.2.3 Étape 2: Identification des événements initiateurs considérés 58
7.2.4 Étape 3: Identification des facteurs d'atténuation et des phénomènes physiques 59
7.2.5 Étape 4: Définition des séquences et conséquences et leur quantification 59
7.2.6 Étape 5: Analyse des conséquences 60
7.2.7 Étape 6: Utilisation des résultats de l'AAE 61
8 Évaluation 61
8.1 Remarques préliminaires 61
8.2 Analyse qualitative – Gestion des dépendances 62
8.2.1 Généralités 62
8.2.2 Dépendances fonctionnelles 62
8.2.3 Dépendances structurelles ou physiques 63
8.3 Analyse quantitative 65
8.3.1 Séquence indépendante d'événements 65
8.3.2 Liaison d'arbre de panne et réduction booléenne 66
9 Documentation 68
Annexe A (informative) Représentation graphique 69
Annexe B (informative) Exemples 71
Bibliographie 85

Figure 1 – Processus de développement des arbres d'événement 53
Figure 2 – Représentation graphique de base d'un arbre d'événement 62

Figure 3 – Dépendances fonctionnelles dans les arbres d'événement 63
Figure 4 – Modélisation des dépendances structurelles ou physiques 64
Figure 5 – Séquence d'événements 65
Figure 6 – Liaison d'arbre de panne 67
Figure A.1 – Représentation graphique souvent utilisée des arbres d'événement 69
Figure B.1 – Arbre d'événement d'un incendie classique dans un bâtiment de générateur diesel 73
Figure B.2 – Arbre d'événement simplifié en cas d'incendie 74
Figure B.3 – Système de passage à niveau (LX) 75
Figure B.4 – AAE d'un système de passage à niveau 77
Figure B.5 – Exemple simple 80
Figure B.6 – Arbre de panne pour la défaillance du système 1 80
Figure B.7 – Arbre de panne pour la défaillance du système 2 81
Figure B.8 – Arbre d'événement modifié 82
Figure B.9 – Arbre d'événement avec « pannes groupées » 83

Tableau A.1 – Éléments graphiques 70
Tableau B.1 – Symboles utilisés dans l'Annexe B 74
Tableau B.2 – Présentation du système 76
Tableau B.3 – Paramètres de réduction des risques pour les accidents de la Figure B.4 78

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

TECHNIQUES D'ANALYSE DE LA SÛRETÉ DE FONCTIONNEMENT – ANALYSE PAR ARBRE D'ÉVÉNEMENT (AAE)

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 elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à 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 62502 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1380/FDIS	56/1389/RVD

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

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

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de 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.

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

INTRODUCTION

La présente Norme internationale définit les principes et procédures de base de la technique de sûreté de fonctionnement désignée Analyse par Arbre d'Evénement (AAE).

La CEI 60300-3-1 répertorie de manière explicite l'AAE comme une méthode destinée à la sûreté de fonctionnement générale, ainsi qu'aux tâches d'analyse des risques et de la sécurité. L'AAE est également brièvement présentée dans la CEI 60300-3-9.

Les principes de base de cette méthodologie n'ont pas changé depuis la conception de la technique dans les années 60. L'AAE a été la première fois utilisée avec succès dans l'industrie du nucléaire dans une étude de l'U.S. Nuclear Regulatory Commission, le rapport WASH 1400 publié en 1975 [31][1].

Au cours des années suivantes, l'AAE a été largement acceptée comme méthodologie éprouvée d'analyse de la sûreté de fonctionnement et des risques. Elle a été appliquée dans divers secteurs de l'industrie (aéronautique, nucléaire, automobile, chimie, l'exploitation littoral pétrolière et gazière, l'industrie de la défense, les systèmes de transport).

A l'inverse de certaines techniques de sûreté de fonctionnement (le modèle Markov, par exemple), l'AAE repose sur des principes mathématiques relativement élémentaires. Toutefois, comme indiqué dans la CEI 60300-3-1, la mise en œuvre de l'AAE requiert un niveau élevé d'expertise quant à l'application de la technique. Cela est dû au fait qu'il faut être particulièrement attentif au traitement des événements dépendants. De plus, il est possible d'utiliser la relation étroite entre l'Analyse par Arbre de Panne (AAP) et l'analyse qualitative et quantitative des arbres d'événement.

La présente norme a pour objet de définir les principes de base consolidés de l'AAE et l'usage courant de cette technique comme moyen d'évaluation des mesures liées à la sûreté de fonctionnement et aux risques d'un système.

---

1 Les chiffres entre crochets se réfèrent à la bibliographie.

TECHNIQUES D'ANALYSE DE LA SÛRETÉ DE FONCTIONNEMENT – ANALYSE PAR ARBRE D'ÉVÉNEMENT (AAE)

1 Domaine d'application

La présente Norme internationale spécifie les principes de base consolidés de l'Analyse par Arbre d'Evénement (AAE) et donne les lignes directrices pour la modélisation des conséquences d'un événement initiateur, ainsi que pour l'analyse de ces conséquences d'un point de vue qualitatif et quantitatif dans le cadre de mesures liées à la sûreté de fonctionnement et aux risques.

Plus particulièrement, la présente norme traite des points suivants liés aux arbres d'événement:

a) définition des termes essentiels et description de l'utilisation des symboles et moyens de représentation graphique;

b) spécification des modes opératoires de construction de l'arbre d'événement;

c) élaboration des hypothèses, limites et avantages de l'analyse;

d) identification des relations avec d'autres techniques liées à la sûreté de fonctionnement et aux risques et explication des domaines d'applications pertinents;

e) proposition de lignes directrices pour les aspects qualitatifs et quantitatifs de l'évaluation;

f) des exemples pratiques.

La présente norme s'applique à tous les secteurs de l'industrie dans lesquels il est indispensable d'évaluer les mesures liées à la sûreté de fonctionnement et aux risques pour déterminer les conséquences d'un événement initiateur.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60050-191:1990, *Vocabulaire Électrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 61025:2006, *Analyse par arbre de panne (AAP)*