

Analysis techniques for dependability - Event tree analysis (ETA)

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 62502:2010 sisaldab Euroopa standardi EN 62502:2010 ingliskeelset teksti.

Standard on kinnitatud Eesti Standardikeskuse 31.12.2010 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.

Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 12.11.2010.

Standard on kättesaadav Eesti standardiorganisatsioonist.

This Estonian standard EVS-EN 62502:2010 consists of the English text of the European standard EN 62502:2010.

This standard is ratified with the order of Estonian Centre for Standardisation dated 31.12.2010 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.

Date of Availability of the European standard text 12.11.2010.

The standard is available from Estonian standardisation organisation.

ICS 21.020

Standardite reprodutseerimis- ja levitamisoigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:
Aru 10 Tallinn 10317 Eesti; www.evs.ee; Telefon: 605 5050; E-post: info@evs.ee

**Analysis techniques for dependability -
Event tree analysis (ETA)**
(IEC 62502:2010)

Techniques d'analyse de la sûreté de
fonctionnement -
Analyse par arbre d'événement (AAE)
(CEI 62502:2010)

Verfahren zur Analyse
der Zuverlässigkeit -
Ereignisbaumanalyse (ETA)
(IEC 62502:2010)

This European Standard was approved by CENELEC on 2010-11-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 56/1380/FDIS, future edition 1 of IEC 62502, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 62502 on 2010-11-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

- | | | |
|--|-------|------------|
| – latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement | (dop) | 2011-08-01 |
| – latest date by which the national standards conflicting with the EN have to be withdrawn | (dow) | 2013-11-01 |

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 62502:2010 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

[12] ISO/IEC 31010	NOTE Harmonized as EN 31010.
[13] IEC 60300-3-1:2003	NOTE Harmonized as EN 60300-3-1:2004 (not modified).
[15] IEC 60812:2006	NOTE Harmonized as EN 60812:2006 (not modified)
[16] IEC 61078:2006	NOTE Harmonized as EN 61078:2006 (not modified)
[17] IEC 61165:2006	NOTE Harmonized as EN 61165:2006 (not modified)
[18] IEC 61508 series	NOTE Harmonized in EN 61508 series (not modified)
[19] IEC 61511-3:2003	NOTE Harmonized as EN 61511-3:2004 (not modified)
[20] IEC 61703:2001	NOTE Harmonized as EN 61703:2002 (not modified)
[22] IEC 62429:2007	NOTE Harmonized as EN 62429:2008 (not modified)
[23] IEC 62508:2010	NOTE Harmonized as EN 62508:2010 (not modified)
[24] IEC 62551 ¹⁾	NOTE Harmonized as EN 62551 ²⁾ (not modified)

¹⁾ To be published.

²⁾ At draft stage.

Annex ZA

(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60050-191	1990	International Electrotechnical Vocabulary (IEV) - Chapter 191: Dependability and quality of service	-	-
IEC 61025	2006	Fault Tree Analysis (FTA)	EN 61025	2007

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

preview generated by EVS

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)*

3 Terms, definitions, abbreviations and symbols

For the purposes of this document, the following terms and definitions, as well as those given in IEC 60050-191, apply.

3.1 Terms and definitions

3.1.1

node

point in the graphical representation of the event tree depicting two or more possible outcomes for the mitigating factor

NOTE The top event of the corresponding fault tree can directly be linked to a node.

3.1.2

common cause

cause of occurrence of multiple events

[IEC 61025:2006, 3.15]