SLOVENSKI STANDARD
SIST EN 61025:2008

01-januar-2008

Nadomešča:
SIST HD 617 S1:2004

Analiza drevesa okvar (FTA) (IEC 61025:2006)

Fault tree analysis (FTA)

Fehlzustandsbaumanalyse

Analyse par arbre de panne (AAP)

Ta slovenski standard je istoveten z: **EN 61025:2007**

ICS:

03.120.01	Kakovost na splošno	Quality in general
21.020	Značilnosti in načrtovanje strojev, aparatov, opreme	Characteristics and design of machines, apparatus, equipment

SIST EN 61025:2008 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61025

April 2007

ICS 03.120.01; 03.120.99

Supersedes HD 617 S1:1992

English version

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

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

Fehlzustandsbaumanalyse
(IEC 61025:2006)

This European Standard was approved by CENELEC on 2007-03-01. 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, 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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 61025:2007 E

Foreword

The text of document 56/1142/FDIS, future edition 2 of IEC 61025, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61025 on 2007-03-01.

This European Standard supersedes HD 617 S1:1992.

The main changes with respect to HD 617 S1:1992 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.

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) 2007-12-01

– latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2010-03-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61025:2006 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:

IEC 60300-3-1	NOTE	Harmonized as EN 60300-3-1:2004 (not modified).
IEC 60812	NOTE	Harmonized as EN 60812:2006 (not modified).
IEC 61078	NOTE	Harmonized as EN 61078:2006 (not modified).

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.

Publication	Year	Title	EN/HD	Year
IEC 60050-191	-[1)]	International Electrotechnical Vocabulary (IEV) - Chapter 191: Dependability and quality of service	-	-
IEC 61165	-[1)]	Application of Markov techniques	EN 61165	2006[2)]

[1)] Undated reference.

[2)] Valid edition at date of issue.

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

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050(191) apply.

In fault tree methodology and applications, many terms are used to better explain the intent of analysis or the thought process behind such analysis. There are terms used also as synonyms to those that are considered analytically correct by various authors. The following additional terms are used in this standard.

3.1
outcome
result of an action or other input; a consequence of a cause

NOTE 1 An outcome can be an event or a state. Within a fault tree, an outcome from a combination of corresponding input events represented by a gate may be either an intermediate event or a top event.

NOTE 2 Within a fault tree, an outcome may also be an input to an intermediate event, or it can be the top event.

3.2
top event
outcome of combinations of all input events

NOTE 1 It is the event of interest under which a fault tree is developed. The top event is often referred to as the **final event,** or as **the top outcome**.

NOTE 2 It is pre-defined and is a starting point of a fault tree. It has the top position in the hierarchy of events.

3.3
final event
final result of combinations of all of the input, intermediate and basic events

NOTE It is a result of input events or states (see 3.2).

3.4
top outcome
outcome that is investigated by building the fault tree

NOTE Final result of combinations of all of the input, intermediate and basic events; it is a result of input events or states (see 3.2).

3.5
gate
symbol which is used to establish symbolic link between the output event and the corresponding inputs

NOTE A given gate symbol reflects the type of relationship required between the input events for the output event to occur.

3.6
cut set
group of events that, if all occur, would cause occurrence of the top event

3.7
minimal cut set
minimum, or the smallest set of events needed to occur to cause the top event

NOTE The non-occurrence of any one of the events in the set would prevent the occurrence of the top event.

3.8
event
occurrence of a condition or an action

3.9
basic event
event or state that cannot be further developed

3.10
primary event
event that is at the bottom of the fault tree

NOTE In this standard, primary event can mean a basic event that need not be developed any more, or it can be an event that, although a product of groups of events and gates, may be developed elsewhere, or may not be developed at all (undeveloped event).

3.11
intermediate event
event that is neither a top event nor a primary event

NOTE It is usually a result of one or more primary and/or other intermediate events.

3.12
undeveloped event
event that does not have any input events

NOTE It is not developed in the analysis for various possible reasons, such as lack of more detailed information, or it is developed in another analysis and then annotated in the current analysis as undeveloped. An example of undeveloped gates could be Commercial Off The Shelf Items (or COTS).

3.13
single point failure (event)
failure event which, if it occurs, would cause overall system failure or would, by itself regardless of other events or their combinations, cause the top unfavourable event (outcome)

3.14
common cause events
different events in a system or a fault tree that have the same cause for their occurrence

NOTE An example of such an event would be shorting of ceramic capacitors due to flexing of the printed circuit board; thus, even though these might be different capacitors having different functions in their design, their shorting would have the same cause – the same input event.

3.15
common cause
cause of occurrence of multiple events

NOTE In the above example it would be board flexing that itself can be an intermediate event resulting from multiple events such as environmental shock, vibrations or manual printing circuit board break during product manufacturing.

3.16
replicated or repeated event
event that is an input to more than one higher level event

NOTE This event can be a common cause or a failure mode of a component, shared by more than one part of a design.

Figure 1 illustrates some of the above definitions. This figure contains annotations and description of events to better explain the practical application of a fault tree. Omitted from Figure 1 are the graphical explanations of cut sets or minimal cut sets, for simplicity of the graphical representation of other pertinent terms. The symbols in Figure 1 and all of the subsequent figures appear somewhat different to those in Tables A.1, A.2, A.3, and A.4 because of the added box above the gate symbol for description of individual events.