SLOVENSKI STANDARD
oSIST prEN IEC 61025:2023

01-november-2023

Analiza drevesa okvar (FTA)

Fault tree analysis (FTA)

Fehlzustandsbaumanalyse

Analyse par arbre de panne (AAP)

Ta slovenski standard je istoveten z: prEN IEC 61025:2023

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

oSIST prEN IEC 61025:2023 en

IEC

56/1999/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 61025 ED3**	
DATE OF CIRCULATION: **2023-09-08**	CLOSING DATE FOR VOTING: **2023-12-01**
SUPERSEDES DOCUMENTS: **56/1916/CD, 56/1922A/CC**	

IEC TC 56 : DEPENDABILITY	
SECRETARIAT: United Kingdom	SECRETARY: Ms Stephanie Lavy
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING **Attention IEC-CENELEC parallel voting** The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE AC/22/2007 OR NEW GUIDANCE DOC).

TITLE:

Fault tree analysis (FTA)

PROPOSED STABILITY DATE: 2024

NOTE FROM TC/SC OFFICERS:

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

FAULT TREE ANALYSIS

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 IEC61025 has been prepared by Technical committee TC 56: Dependability.

This third edition cancels and replaces the second edition published in 2006. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) The structure of the document has been modified with general applications of fault trees discussed in the earlier clauses and applications specific to dependability in the later clauses.
b) The mathematical content relating to dependability has been written to align with IEC 61078 (Reliability block diagrams) and to provide more information about availability, reliability and failure frequency calculations.
c) Clauses have been introduced to describe non-coherent fault trees and dynamic fault trees.
d) Additional annexes have been added as follows: Annex A (Relationship with other dependability and risk assessment techniques), Annex B (Automated fault tree construction), Annex C (Use of Monte Carlo analysis for analysing uncertainty), Annex E

(Shannon decomposition and binary decision diagrams), Annex F (Importance factors), Annex G (FT driven Petri net models) and Annex H (Numerical examples and curves).

The text of this International Standard is based on the following documents:

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

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

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

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

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

The National Committees are requested to note that for this document the stability date is 20XX..

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

INTRODUCTION

Fault tree analysis (FTA) is used to identify and analyse combinations of events, conditions and factors that cause or can potentially cause or contribute to the occurrence of a defined undesirable outcome, referred to as the "top event".

The fault tree (FT) is an organized graphical representation of events leading to an undesired event that can be clearly understood and analysed. Standardized symbols are used to show the logical relationship among FT events (primary events or leaves and intermediate events) that lead to the occurrence of the top event.

It is a deductive (top-down, effect to cause) technique which is very effective in the analysis of multiple failure combinations. It can be used to complement the results obtained by other analysis techniques such as FMEA [3][1] or HAZOP [4] which are inductive in nature (bottom-up, cause to effect) and which consider each failure individually.

Depending on its scope, FTA can be qualitative or quantitative. Qualitative analysis identifies combinations of primary events (minimal cut sets or prime implicants) that lead to the top event. This enables weak points to be identified, gives guidance for failure prevention and helps to determine how a product or system can be brought back to operation.

Quantitative analysis provides calculations of the probability of the top event and the importance of primary events. For dependability applications the unavailability, unreliability and failure frequency, of the product or system under study can be calculated.

FTA can be used to inform decisions for improving the performance, dependability and safety of products and systems in a cost-effective way.

In its simplest form, an FT implements simple OR and AND logic gates and is equivalent to a logic equation giving the top event as a function of the primary events, with events being considered as Boolean variables. FTA, like the reliability block diagram (RBD) [5] or event tree analysis (ETA) [6] belongs to the Boolean approaches. For simple FTs, the conventional rules of probabilistic calculations with constant probability values apply.

Provided that each primary event in the FT can reasonably be assumed to behave independently the probabilistic calculations can be extended to time dependent probabilistic calculations so the FT can, for example, handle primary events involving non-repaired as well as repaired items. FTA can also be extended to deal with large FTs, more complex gates, sequence dependent behaviours and situations where an assumption that probability of the primary event is low is not valid. While small FTs can be developed and analysed manually, FTA of large or complicated systems generally requires software support.

NOTE FTA typically uses a top event that represents an undesirable event of some kind. Where the top event is a success or improvement a similar approach called STA (success tree analysis) can be used.

This document is intended for those who need to develop and use FTs to analyse undesired events.

[1] Numbers in square brackets refer to the Bibliography

FAULT TREE ANALYSIS

1 Scope

Fault tree analysis (FTA) is used to identify and analyse combinations of events, conditions and factors that cause or can potentially cause or contribute to the occurrence of a defined undesirable outcome, referred to as the "top event". This document describes the (FTA) technique and provides guidance on its application. This includes:

- definition and description of commonly used terms and symbols;
- purpose, applications and limitations of FTs;
- a description of basic concepts and principles;
- a description of the steps involved in scoping, constructing and developing the FT;
- guidance on performing qualitative and quantitative analysis of the FT, including discussion of requirements and limitations of the associated mathematical models;
- identification of basic items that should be included when documenting and reporting the FTA;
- methods for performing FTA when some of the commonly used assumptions are not satisfied (e.g., non-coherent FTs, dynamic FTs);
- example applications in support of the above;
- procedures for calculating dependability measures (unavailability, failure frequency and unreliability) for different types of system, with constant or time dependent probabilities or with non-repaired or repaired items).

In annexes, the document also describes:

- the relationship of FTA with other related techniques such as Reliability Block Diagram analysis (IEC 61078), Failure Mode and Effects Analysis (FMEA) (IEC 60812), Event Tree Analysis (IEC 62502) and Markov techniques (IEC 61165);
- methods by which the importance of various events included in the FT can be established;
- automated fault tree construction;
- mathematical models required for large and more complex FTs;
- numerical examples demonstrating the use of FTs in dependability.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* (available at http://www.electropedia.org)

IEC 61703, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1 Definitions directly relating to a fault tree

NOTE Symbols for events are given in Table 3 and gates in Tables 4 and 5.

3.1.1
Boolean related model
mathematical model where the state of a system is represented by a logical function of Boolean variables representing the states of its components

Note 1 to entry: A Boolean variable only has two values and a logical function of several Boolean variables also has only two values. Those two values can be for example, {0, 1}, {up, down}, {true, false}, {working, failed}, etc. The underlying mathematics behind the logical functions is Boolean algebra.

[SOURCE: IEC 61078:2016]

3.1.2
fault tree
FT
a directed acyclic graph (i.e. a graph without loops) representing the logical links between a top event and the primary events that caused it

Note 1 to entry: The primary events could be component hardware failures, human errors, software failures or any other pertinent events that could contribute to the occurrence of the undesired event (top event).

Note 2 to entry: According to IEC 60050-192 [192-04-01] a fault is the state of being unable to perform as required and a failure is the loss of the ability to perform as required (i.e. an event) However, in an FT, the term event is used to refer to either a state or an event.

3.1.3
static fault tree
fault tree where it is reasonable to assume that the primary events are independent and their probabilities are constant

3.1.4
sub fault tree
fault tree related to an intermediate event within a fault tree

Note 1 to entry: Sub fault trees are used to split large fault trees into several parts, e.g. for readability, understandability or to fit on a page.

3.1.5
dynamic fault tree
DFT
fault tree implementing temporal interactions and where the assumption of independency between the primary events is not reasonably fulfilled

Note 1 to entry: The primary events of a DFT can have interactions with elements external to the FT itself (e.g. weather, night and day, repair team availability, spare parts provisioning, etc.).

Note 2 to entry: The symbols for DFTs are given in Table 5.

3.1.6
non coherent fault tree
fault tree where a failure path can become a success path by adding another fault or a success path can become a failure path by removing a fault

Note 1 to entry: A necessary but not sufficient condition to have a non-coherent FT is that some primary events appear both in direct (occurred) and complementary (non-occurred) states (see Table 3). In this case, the concept of minimal cut sets (see 3.1.22) is no longer valid and has to be replaced by the concept of prime implicants.

Note 2 to entry: Mathematically speaking a non-coherent FT models a non-monotonic logical function.

3.1.7
gate
logic gate
symbol used to represent the logical relationship that must exist among its input events for its output event to occur

Note 1 to entry: Each symbol represents a logic operator reflecting the type of relationship (e.g. OR, AND, 2/3) required between the input events for the output event to occur.

3.1.8
transfer symbol
transfer gate
an IN-OUT symbol used to indicate that a fault tree has been split into smaller sub-fault trees

3.1.9
top event
root
top outcome
final event
event of interest for which the FTA is performed

Note 1 to entry: It is pre-defined and is the starting point for building a fault tree. It has the top position in the hierarchy of events and it is the final logical combination of all of the input events (primary events) of the fault tree.

Note 2 to entry: The top event can be expressed either as a failure event or as a failed state.

3.1.10
primary event
leaf
an event in the FT which the FT analyst has chosen for some reason not to develop any further

Note 1 to entry: Primary events are the events at the bottom of the tree. They can include basic events (3.1.12) events that are developed elsewhere or undeveloped events (3.1.14).

3.1.11
complementary primary event
primary event repeated in the FT in its negated form

Note 1 to entry: If a primary event in an FT represents a failure of a component then its complementary primary event will be the success of the component.

3.1.12
basic event
primary event at the lowest level of resolution defined for the purpose of analysis

3.1.13
intermediate event
event that is neither a top event nor a primary event

Note 1 to entry: It is usually a result of one or more primary and/or other intermediate events.

3.1.14
undeveloped event
a primary event in the FT that the FT analyst has chosen not to develop further because its development is inconsequential or the information required to develop the event further is not available

Note 1 to entry: An undeveloped event is generally represented by a diamond symbol in the FT.

Note 2 to entry: In French an undeveloped event is sometimes referred to as an elementary event.

3.1.15
event to be developed
a primary event in the FT which the FT analyst has chosen not to develop further at the time of FT development but wants to indicate that it will be developed later for the completion of the FTA.

3.1.16 Note 1 to entry:
house event
primary event which is expected to occur

Note 1 to entry: A house event is sometimes used as a switch true/false to validate / inhibit some parts of the FT.

3.1.17
condition event
conditional event
primary event defining a condition which is referred to in an IF gate

Note 1 to entry: In the context of a fault tree, a condition event has the same property as a basic event.

3.1.18
repeated event
replicated event
primary event appearing more than once in a fault tree

Note 1 to entry: This event can be a common cause or a failure mode of a component shared by more than one part of a design.

Note 2 to entry: The primary events related to repeated events can appear in the direct or complementary form.

3.1.19
common cause events
different events in a fault tree that have the same cause for their occurrence

Note 1 to entry: 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, their shorting would have the same cause.

Note 2 to entry: In the context of fault tree, common cause events are generally common cause failures (see IEC 60050-192, definition [192-03-18]).

3.1.20
common cause
a single cause that results in the occurrence of several events

3.1.21
cut set
group of primary events that, if all occur, would result in the occurrence of the top event

3.1.22
minimal cut set
a group of primary events such that the occurrence of every primary event is necessary and sufficient to cause the top event