

INTERNATIONAL STANDARD

IEC 61025

Second edition
2006-12

Fault tree analysis (FTA)

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[IEC 61025:2006](#)

<https://standards.iteh.ai/catalog/standards/iec/46e5ff05-4815-499e-9b05-4bf395d1714d/iec-61025-2006>

*This **English-language** version is derived from the original **bilingual** publication by leaving out all French-language pages. Missing page numbers correspond to the French-language pages.*



Reference number
IEC 61025:2006(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site** (www.iec.ch)

- **Catalogue of IEC publications**

The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

This summary of recently issued publications (www.iec.ch/online_news/justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

Email: custserv@iec.ch
Tel: +41 22 919 02 11
Fax: +41 22 919 03 00

<https://standards.iteh.ai/catalog/standards/iec/46e5ff05-4815-499e-9b05-4b1395d1714d/iec-61025-2006>

INTERNATIONAL STANDARD

IEC 61025

Second edition
2006-12

Fault tree analysis (FTA)

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[IEC 61025:2006](#)

<https://standards.iteh.ai/catalog/standards/iec/46e5ff05-4815-499e-9b05-4b395d1714d/iec-61025-2006>

© IEC 2006 Copyright - all rights reserved

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Electrotechnical Commission, 3, rue de Varembe, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CONTENTS

FOREWORD.....	7
INTRODUCTION.....	11
1 Scope.....	13
2 Normative references	13
3 Terms and definitions	13
4 Symbols	19
5 General	21
5.1 Fault tree description and structure	21
5.2 Objectives	23
5.3 Applications.....	23
5.4 Combinations with other reliability analysis techniques.....	25
6 Development and evaluation	29
6.1 General considerations.....	29
6.2 Required system information	35
6.3 Fault tree graphical description and structure	37
7 Fault tree development and evaluation	39
7.1 General.....	39
7.2 Scope of analysis	39
7.3 System familiarization	39
7.4 Fault tree development.....	39
7.5 Fault tree construction.....	41
7.6 Failure rates in fault tree analysis.....	75
8 Identification and labelling in a fault tree	75
9 Report.....	77
Annex A (informative) Symbols	81
Annex B (informative) Detailed procedure for disjointing	95
Bibliography.....	103
Figure 1 – Explanation of terms used in fault tree analyses.....	19
Figure 2 – Fault tree representation of a series structure	45
Figure 3 – Fault tree representation of parallel, active redundancy	47
Figure 4 – An example of fault tree showing different gate types.....	51
Figure 5 – Rectangular gate and events representation	53
Figure 6 – An example fault tree containing a repeated and a transfer event	55
Figure 7 – Example showing common cause considerations in rectangular gate representation.....	55
Figure 8 – Bridge circuit example to be analysed by a fault tree.....	63
Figure 9 – Fault tree representation of the bridge circuit	65
Figure 10 – Bridge system FTA, Esary-Proschan, no disjointing.....	69

Figure 11 – Bridge system probability of failure calculated with rare-event approximation	71
Figure 12 – Probability of occurrence of the top event with disjointing.....	73
Figure A.1 – Example of a PAND gate	93
Table A.1 – Frequently used symbols for a fault tree.....	81
Table A.2 – Common symbols for events and event description	87
Table A.3 – Static gates.....	89
Table A.4 – Dynamic gates	91

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[IEC 61025:2006](#)

<https://standards.iteh.ai/catalog/standards/iec/46e5ff05-4815-499e-9b05-4b395d1714d/iec-61025-2006>

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.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[IEC 61025:2006](#)

<https://standards.itih.ai/catalog/standards/iec/46e5ff05-4815-499e-9b05-4b395d1714d/iec-61025-2006>

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 performance, 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.

(<https://standards.iteh.ai>)

Document Preview

[IEC 61025:2006](https://standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/iec/46e5ff05-4815-499e-9b05-4b395d1714d/iec-61025-2006>

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

[IEC 61025:2006](https://standards.iteh.ai/catalog/standards/iec/46e5ff05-4815-499e-9b05-4b395d1714d/iec-61025-2006)

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 [IEC 61025:2006](https://standards.iteh.ai/iec/61025-2006)

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

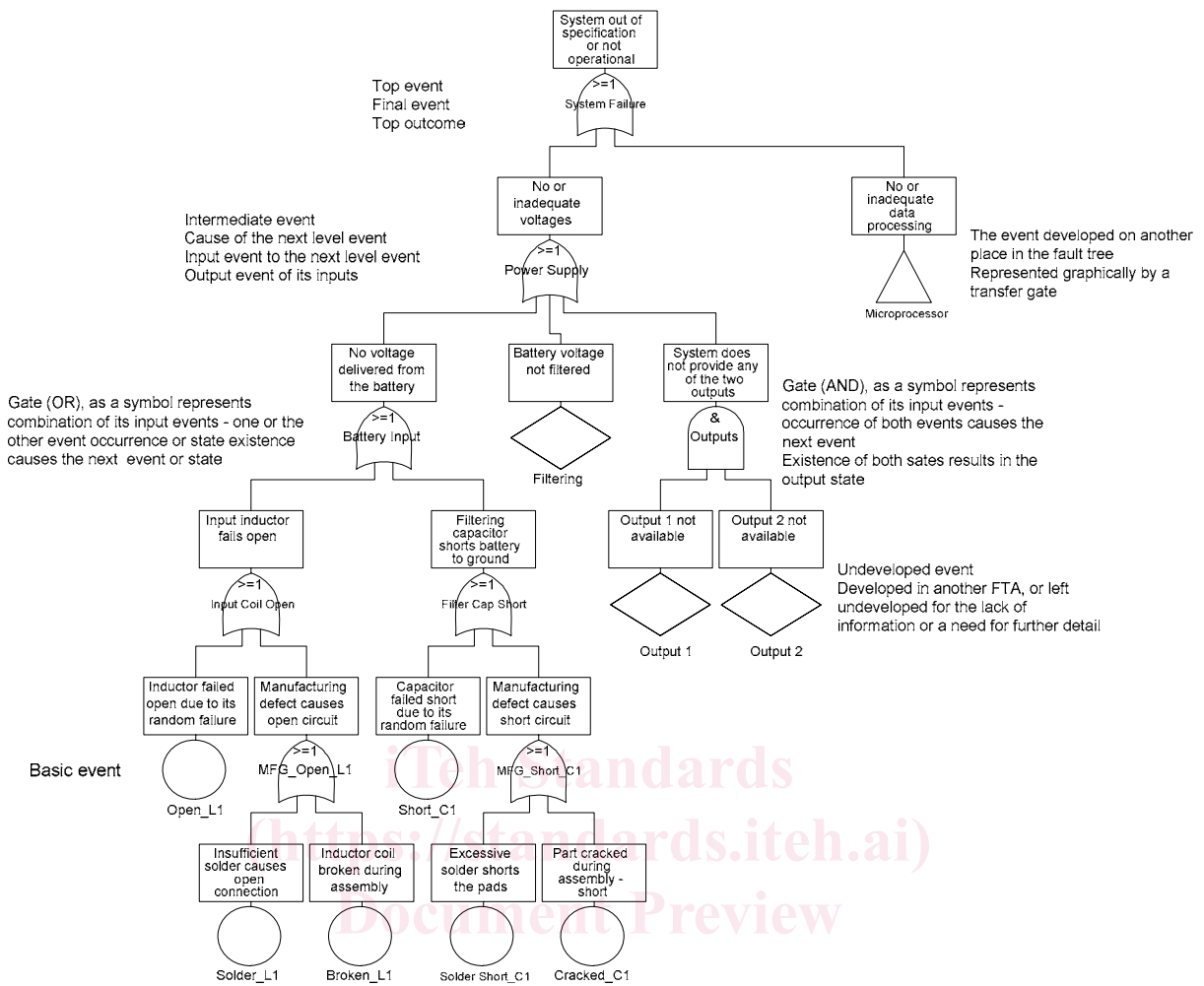
NOTE In the above example it would be board flexing that itself can be an intermediate event resulting from multiple events such as environmental shock, vibrations or manual printing circuit board break during product manufacturing.

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.



IEC 2118/06

IEC 61025:2006

Figure 1 – Explanation of terms used in fault tree analyses

NOTE Symbols in Figure 1 and all other figures might slightly differ from the symbols shown in Annex A. This is because description blocks are added to better explain the relationship of various events

4 Symbols

The graphical representation of a fault tree requires that symbols, identifiers and labels be used in a consistent manner. Symbols describing fault tree events vary with user preferences and software packages, when used. General guidance is given in Clause 8 and in Annex A.

Other symbols used in this standard are standard dependability symbols such as $F(t)$ or just probability of an event occurring F . For that reason, a separate list of symbols is not provided.

5 General

5.1 Fault tree description and structure

Several analytical methods of dependability analysis are available, of which fault tree analysis (FTA) is one. The purpose of each method and their individual or combined applicability in evaluating the flow of events or states that would be the cause of an outcome, or reliability and availability of a given system or component should be examined by the analyst before starting FTA. Consideration should be given to the advantages and disadvantages of each method and their respective products, data required to perform the analysis, complexity of analysis and other factors identified in this standard.

A fault tree is an organized graphical representation of the conditions or other factors causing or contributing to the occurrence of a defined outcome, referred to as the "top event". When the outcome is a success, then the fault tree becomes a success tree, where the input events are those that contribute to the top success event. The representation of a fault tree is in a form that can be clearly understood, analysed and, as necessary, rearranged to facilitate the identification of:

- factors affecting the investigated top event as it is carried out in most of the traditional fault tree analyses;
- factors affecting the reliability and performance characteristics of the system, when the FTA technique is used for reliability analysis, for example design deficiencies, environmental or operational stresses, component failure modes, operator mistakes, software faults;
- events affecting more than one functional component, which could cancel the benefits of specific redundancies or affect two or more parts of a product that may otherwise seem operationally unrelated or independent (common cause events).

Fault tree analysis is a deductive (top-down) method of analysis aimed at pinpointing the causes or combinations of causes that can lead to the defined top event. The analysis can be qualitative or quantitative, depending on the scope of the analyses.

<https://standards.iteh.ai/catalog/standards/iec/46e5ff05-4815-499e-9b05-4b395d1714d/iec-61025-2006>

A fault tree can be developed as its complement, the success tree analysis, (STA), where the top event is a success, and its inputs are contributor to the success (desired) event.

In cases where the probability of occurrence of the primary events cannot be estimated, a qualitative FTA may be used to investigate causes of potential unfavourable outcomes with individual primary events marked with descriptive likelihood of occurrence such as: "highly probable", "very probable" "medium probability", "remote probability", etc. The primary goal of the qualitative FTA is to identify the minimal cut set in order to determine the ways in which the basic or primary events influence the top event.

A quantitative FTA can be used when the probabilities of primary events are known. Probabilities of occurrence of all intermediate events and the top event (outcome) can then be calculated in accordance with the model. Also, the quantitative FTA is very useful in reliability analysis of a product or a system in its development.

FTA can be used for analysis of systems with complex interactions between sub-systems including software/hardware interactions.

5.2 Objectives

FTA may be undertaken independently of, or in conjunction with, other reliability analyses. Objectives include:

- identification of the causes or combinations of causes leading to the top event;
- determination of whether a particular system reliability measure meets a stated requirement;
- determination of which potential failure mode(s) or factor(s) would be the highest contributor to the system probability of failure (unreliability) or unavailability, when a system is repairable, for identifying possible system reliability improvements;
- analysis and comparison of various design alternatives to improve system reliability;
- demonstration that assumptions made in other analyses (such as Markov and FMEA) are valid;
- identification of potential failure modes that might cause a safety issue, evaluation of corresponding probability of occurrence and possibility of mitigation;
- identification of common events (e.g. the middle branch of a bridge circuit, see Figure 10);
- search for an event or combinations of events which are the most likely to cause the top event to occur;
- assessment of the impact of the occurrence of a primary event on the probability of the top event;
- calculation of event probabilities;
- calculation of availabilities and failure rates of system or its components represented by a fault tree, if a steady state can be postulated, and eventual repairs are independent of each other (same limitation as for the success path diagram/reliability block diagram).

5.3 Applications

FTA is particularly suited to the analysis of systems comprising several functionally related or dependent subsystems. Benefits of FTA are apparent when a system design is the product of several independent specialized technical design groups and the separate fault trees are linked together. Fault tree analysis is commonly applied when designing nuclear power generating stations, transportation systems, communication systems, chemical and other industrial processes, railway systems, home entertainment systems, medical systems, computer systems, etc. Fault tree analysis is also of particular value when applied to systems comprising various component types and their interaction (mechanical, electronic and software components), which cannot be easily modelled with other techniques. An example of this would be a combination of events where their order of appearance is essential such as existence of vibration fatigue causing fracture cracks and failures of components.

FTA has a multitude of uses as a tool (to list a few):

- to determine the pertinent logic combination of events leading to the top event and, potentially, their prioritization;
- to investigate a system under development and anticipate and prevent, or mitigate, potential cause(s) of undesired top event;