

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Fault tree analysis (FTA)

Analyse par arbre de panne (AAP)



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2006 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, 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 either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

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

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,...). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00



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
CODE PRIX

XA

ICS 03.120.01; 03.120.99

ISBN 2-8318-8918-9

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms and definitions	7
4 Symbols	10
5 General	11
5.1 Fault tree description and structure	11
5.2 Objectives	12
5.3 Applications.....	12
5.4 Combinations with other reliability analysis techniques.....	13
6 Development and evaluation	15
6.1 General considerations.....	15
6.2 Required system information	18
6.3 Fault tree graphical description and structure	19
7 Fault tree development and evaluation	20
7.1 General.....	20
7.2 Scope of analysis	20
7.3 System familiarization	20
7.4 Fault tree development.....	20
7.5 Fault tree construction.....	21
7.6 Failure rates in fault tree analysis.....	38
8 Identification and labelling in a fault tree	38
9 Report	39
Annex A (informative) Symbols	41
Annex B (informative) Detailed procedure for disjointing	48
Bibliography.....	52
Figure 1 – Explanation of terms used in fault tree analyses.....	10
Figure 2 – Fault tree representation of a series structure	23
Figure 3 – Fault tree representation of parallel, active redundancy	24
Figure 4 – En example of fault tree showing different gate types.....	26
Figure 5 – Rectangular gate and events representation	27
Figure 6 – An example fault tree containing a repeated and a transfer event	28
Figure 7 – Example showing common cause considerations in rectangular gate representation.....	28
Figure 8 – Bridge circuit example to be analysed by a fault tree.....	32
Figure 9 – Fault tree representation of the bridge circuit	33
Figure 10 – Bridge system FTA, Esary-Proschan, no disjointing.....	35

Figure 11 – Bridge system probability of failure calculated with rare-event approximation	36
Figure 12 – Probability of occurrence of the top event with disjointing.....	37
Figure A.1 – Example of a PAND gate	47
Table A.1 – Frequently used symbols for a fault tree.....	41
Table A.2 – Common symbols for events and event description	44
Table A.3 – Static gates.....	45
Table A.4 – Dynamic gates	46

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 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.

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

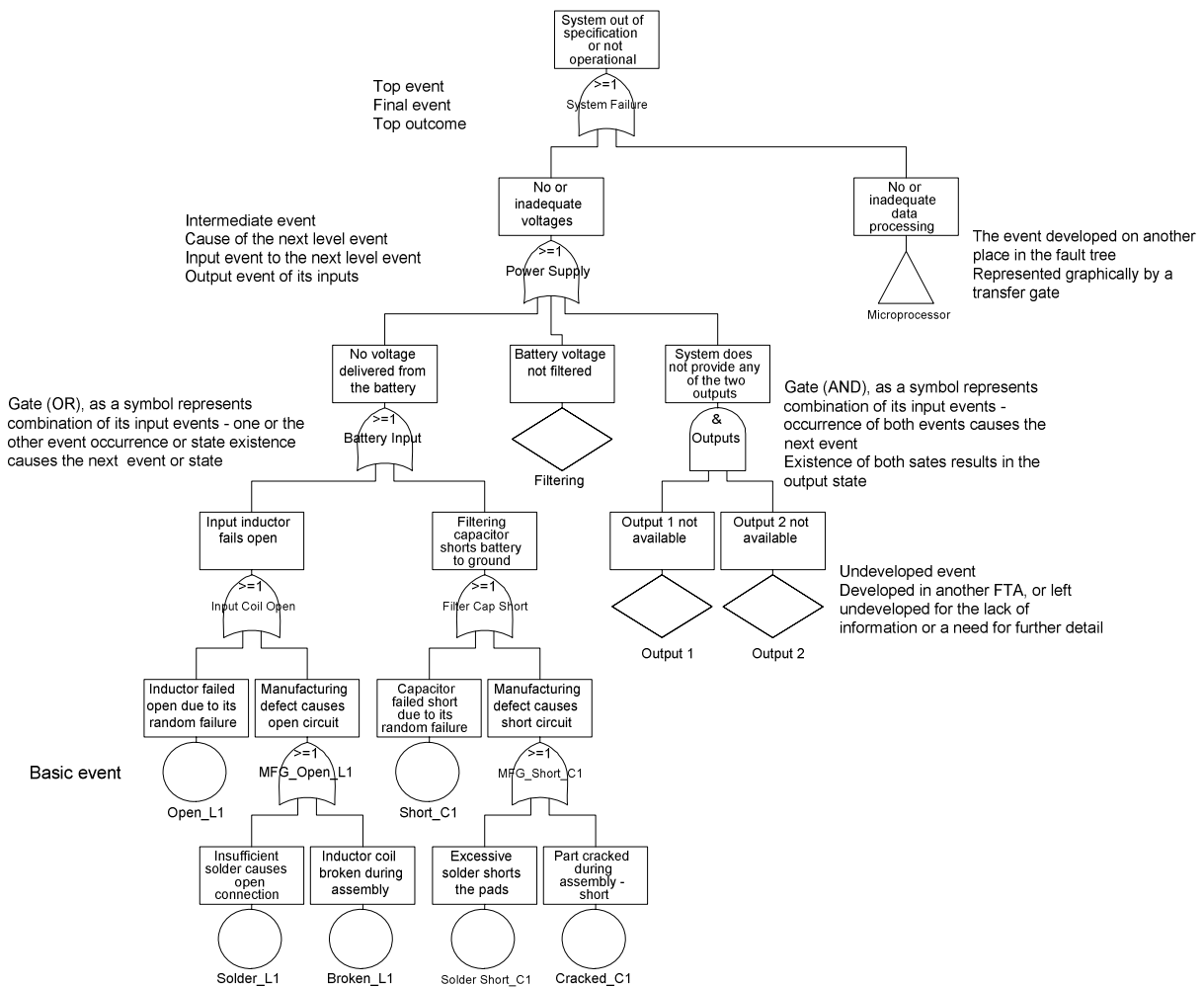
NOTE In the above example it would be board flexing that itself can be an intermediate event resulting from multiple events such as environmental shock, vibrations or manual printing circuit board break during product manufacturing.

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.



IEC 2118/06

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.

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;

- to analyze a system, determine its reliability, identify the major contributors to its unreliability and evaluate the design changes;
- to assist probabilistic risk assessment efforts.

FTA can be applied to all new or modified products in all design phases, as an analytical tool for identification of potential design problems, including those early phases where information on the design details is incomplete. Those early efforts would then be extended as more information on the system design and its components becomes available. FTA also identifies potential problems that may originate from the product's physical design, environmental or operational stresses, flaws in product manufacturing processes and from operational and maintenance procedures.

5.4 Combinations with other reliability analysis techniques

5.4.1 Combination of FTA and failure modes and effects analysis (FMEA)

This analysis combination is often recommended by sector specific standards, in particular safety standards and transportation standards. The benefits of a combined analysis are the following:

- FTA is a top-down and FMEA a bottom-up analysis method and use of both deductive and inductive reasoning is regarded as a good argument for providing assurance for the completeness of an analysis;
- safety standards often demand a single failure and, in some cases, a multiple failure analysis, the first requirement being fulfilled by FMEA. Both single and multiple failure analysis are accomplished by FTA;
- FMEA is also a useful method for a comprehensive identification of basic events or hazards, while FTA is a practical method for causal analysis of the undesirable events.

Additionally there exists a simple consistency check between FMEA and FTA:

- any identified single failure in FMEA leading to the top event of the fault tree also has to appear as a single point failure (in the minimal cut set);

NOTE A single point failure is a failure that, if it occurs, would cause the entire system to fail.

- any single point failure identified in the FTA should also appear as such in the FMEA.

The value of this consistency check is increased if the analyses are performed separately and independently. This is especially important in safety analyses.

The IEC standard which explains this methodology is IEC 60300-3-1.

5.4.2 Combination of FTA and event tree analysis (ETA)

Any event could be analysed by FTA. However, in some cases this may be not appropriate for several reasons:

- it is sometimes easier to develop event sequences rather than causal relationships;
- the resulting tree may become very large;
- there are often separate teams dealing with different parts of the analysis.

In order to find a practical procedure, it is often not the top undesired event that is defined first, but potentially undesirable events at the interface between the functional and technical domain.

To give an illustration, consider the top event “loss of crew or vehicle” for a spacecraft mission. Instead of building a large fault tree based on “loss of crew or vehicle,” intermediate undesired events like “ignition fails” or “thrust failure” may be defined as top events and analysed as separate fault trees. These reduced top events would then, in turn, be used as inputs to an event tree in order to analyse operational consequences.

This combination of ETA and FTA is sometimes referred to as cause-consequence analysis (CCA).

5.4.3 Combination of FTA and Markov analysis

FTA that has only a combination of static events (timing – sequencing of the event combination is not considered or modelled – static gates) usually evaluates systems with no sequence dependency of events. However, it is possible to extend the FTA by defining additional gates that represent Markov models. These gates bear the name of “dynamic” gates and include PRIORITY AND gates, SEQUENTIAL gates, and SPARE gates. For such gates, it is necessary to evaluate the failure probability at a time t by using the appropriate Markov model or simulation. Once evaluated, the dynamic gate and its inputs may be replaced by a single primary event, with the probability of occurrence calculated by Markov analysis. Some commercial software allow for modelling of dynamic gates and the capability for calculation of probability of occurrence of the event they represent. An example of dynamic, PRIORITY AND gate is shown in Annex A.

Both static and dynamic gates of a fault tree are used, based on the assumption that the individual events are independent (unless defined as common). However, particular attention shall be given to independence properties between the events included in the Markov model and the events in the fault tree.

5.4.4 Combination of FTA and binary decision diagram (BDD) techniques

Calculation of the probability of occurrence for the top event of a fault tree with many cut sets requires calculation of probability for all cut set combinations. Because of its high complexity, this calculation will often need to be truncated. A BDD may be constructed recursively from a fault tree and it provides an efficient, exact calculation method. This method is well explained in the “NASA Fault Tree Handbook with Aerospace Applications version 1.1[1]¹”.

The BDD approach is useful where truncation of cut set probability calculations results in either unacceptable loss of accuracy or an FTA solution takes excessive time, particularly when many high-probability events appear in the model. Because the minimal paths generated in the BDD approach are disjointed (see 7.5.5.4), calculation of importance and sensitivities can also be performed efficiently and exactly.

¹ Figures in square brackets refer to the bibliography.

5.4.5 Combination with the reliability block diagram

A reliability block diagram is made up of blocks or modules, representing a group of components, or failure modes. Those groups are normally formed following the functional block diagram of a product, system or a process. These modules have either a determined failure rate, or a calculated reliability or probability of failure for given use or operational profile. Traditionally, the blocks would have a failure rate which would be the sum of failure rates of individual components. In that manner, the functional interaction of components within a module is not considered.

To augment correctness of functional modelling within a block (software/hardware, interaction of mechanical parts), reliability of certain blocks can be modelled with a fault tree, and then the resultant information on probability of occurrence of those blocks can be assigned to that specific block being part of a reliability block diagram. In this manner, reliability block diagrams, which normally assume independency of components failure within a block, would yield a more realistic prediction.

6 Development and evaluation

6.1 General considerations

6.1.1 Overview

A fault tree is an organized graphical representation of the conditions that cause, or contribute to, the occurrence of a defined undesirable outcome, referred to as the "top event". The representation is in a form that can be clearly understood, analysed and, as necessary, rearranged to facilitate the identification of:

- factors affecting the reliability and other performance characteristics of the system. These factors, for example, include design deficiencies, environmental or operational stresses, component fault modes, operator mistakes, software faults;
- common events that may contribute to more than one outcome of intermediate events in a fault tree. As an example, 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.

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, Method A, or quantitative, Method B, depending on the scope of the analyses.

In cases where the probability of occurrence of the basic events cannot be estimated, a qualitative FTA, Method A, may be used to investigate causes of potential unfavorable outcomes with individual basic events marked with descriptive likelihood of occurrence such as: "highly probable", "very probable", "medium probability", "remote probability", etc. as explained in 5.1.

A quantitative FTA, Method B, can be used when the probabilities of basic or primary events are known. Probabilities of occurrence of all intermediate events and the top event (outcome) can then be calculated using the appropriate mathematical expressions.

6.1.2 Concepts and combinations of events and states

The final outcome of a fault tree (top event) can be a fault in itself, or an event. Here, the fault tree describes a fault or an event resulting from the contributing events or other faults. In the fault tree analysis certain combination of events can be either states or events, while the others must match the outcome. For example, the inputs into an OR gate where the outcome is a state or an event, can be states or events. All inputs into an AND gate which as an outcome is an event must be events, while if as the outcome it represent a state all the inputs must be states.

The state can be characterized by the probability that the state will exist in time t , while the event can be characterized either by the failure rate or failure frequency, or by probability of event occurrence at time t .

6.1.3 Fault tree for investigation of faults leading to other faults or events

Traditionally, a fault tree is constructed to investigate faults or events leading to an outcome. This concept has been used for a long time in many industries, and is specifically efficient and applied in the nuclear industry. In this manner, it is a powerful and invaluable tool for investigation of potential problems, events, improvements and other preventive measures that preclude or mitigate an undesirable outcome.

An outcome, success or fault, is investigated, and the states or events leading to this outcome investigated, their probability of existence or occurrence determined, and the fault tree model constructed appropriately that would lead to the probability of existence or occurrence of the assumed outcome.

In this application, the fault tree is constructed and evaluated as described in Clause 7, having in mind that the outcome is characterized by probability of fault existence or event occurrence, and is not related to reliability of the analysed item or a system.

It is possible that the basic or any other events in this type of analysis are not given any real probability value, and are only used in investigation of an event that potentially might take place (Method A). In such a case, they might be marked with a descriptive probability of “high, medium, or low”, and are evaluated as potential contributors to the top event or fault. Such types of fault trees are often used for identification of a primary fault or event that was the single or a major contributor to the top fault or event, and are used in a vast variety of industries: automotive, nuclear, manufacturing plants, etc.

6.1.4 FTA use in reliability assessment and improvement during product development

In this application which is based on the FTA Method B, a fault tree can model the entire product, or parts of a product that might pose a risk to its reliability or operational safety. In this case, Method B analysis probability of occurrence can be determined in a traditional manner, such as in analysis of a safety-related fault or event of a product, or the detailed analysis of potential product failure within a certain time period may lead to expression of its unreliability or probability of failure within that period of interest. In this application, the fault tree methodology follows the principles of a top down failure modes and effects analysis, where each potential failure mode may result in an event or a fault leading to the product failure.

The FTA is specifically convenient here as the modelling can reflect the dynamics of events in a product, software/hardware interaction, as well as the interaction between faults or events representing the potential failure modes. This interaction is not possible to represent in a regular FMEA, and is very difficult to model using traditional reliability block diagrams. Also, the product reliability estimates are more realistic, as only the failure modes that contribute to failure of a product, as defined, are considered.

The development of a fault tree should start early in the system design stage and be continued in all of the development stages of a product. The evolution of the fault tree should be such that it reflects the progress of the design. Thus an increased understanding of the failure modes will be obtained as the design proceeds. "Analysis concurrent with design" allows for early systems design change. Many fault trees will be large, in which case fault tree analysis software may be needed to handle them. Software is available to facilitate analysis and allow easy and quick estimates of probability of occurrence of the top event. There are many FTA software programs available and perhaps many more being created. All of them are sufficiently different to suit the needs of a specific use.

It is important to note that fault tree events are not confined solely to software or hardware failures, but include their interaction and other factors, e.g. human factors or actions and processes that are relevant to the top event.

Where quantitative analysis is carried out, but the probability of occurrence of some events cannot be determined, even if the faults or events (failures) are systematic, those events and their functional (logic) combination should be included in the analysis. In this case, these failure modes will not be accounted for in the reliability (or probability of failure) prediction, but their existence is accounted for even in the qualitative manner.

In order to use the fault tree technique effectively as a method for system analysis, the procedure should consist of at least the following steps:

- definition of the scope of the analysis;
- familiarization with the design, functions and operation of the system;
- definition of the top event;
- construction of the fault tree;
- analysis of the fault tree logic;
- reporting on results of the analysis;
- assessment of reliability improvements and trade-offs.

If a numerical analysis is planned, it will be necessary to define a technique for numerical assessment of primary event probabilities or other attributes such as failure intensity, mean time between failures (MTBF) or mean time to failure (MTTF), etc. The selection of the data to be used and numerical evaluation of the reliability or un-reliability measures are outside the scope of this standard.

There are multiple objectives in the FTA of a system design. One of the objectives is to model the product's architecture and functionality in a top-down manner, searching for the potential failure modes and their causes that might produce an outcome as defined by the top event. Based on this information, contributors to the probability of occurrence of the top event or system unreliability (both qualitatively and quantitatively to identify the contributing causes) follow the investigation down in order to identify their respective causes. This allows for trade-off and studies of possible solutions for mitigation of unacceptable potential failure modes, and finally, evaluation of the achieved reliability improvement.

Being a model of a product's architecture and functionality, the FTA should be carried out by personnel with detailed knowledge of the system, its design features and operation, and who are trained in FTA and other relevant reliability modelling techniques. The analyst has to be able to evaluate influences of potential failure modes and logically identify possible causes of abnormal product performance. Lack of engineering knowledge of the product design and potential failure modes will produce an FTA that might not be a true representation of the product functionality and, thus, the analytical results would become meaningless. When prepared, the FTA should be reviewed by the engineering team participating in the product design for correctness and completeness. The corrective actions agreed upon must be documented and followed up.

6.2 Required system information

The system to be analysed should be defined by a description of the system function and by an identification of the system interfaces. Such a definition should include:

- a summary of the design intent;
- a definition of what constitutes the system failure;
- a system functional structure usually represented by a functional block diagram;
- system boundaries, such as electrical, mechanical and operational interfaces, to be governed by the interaction and interfaces with other systems. Such boundaries should be described by identifying the particular functions for example electrical connections (internal or external), fuse, which form the interfaces;
- the physical structure of the system, as opposed to the functional structure;
- an identification of the system operational modes together with a description of system operation and the expected or acceptable system performance in each operational mode;
- a system operational profile;
- the system's environmental conditions, and relevant human aspects (i.e. degree of training for operators and maintenance personnel), etc.;
- a list of applicable documents, for example drawings, specifications, operating manuals, which give details of the equipment design and operation. Task duration, time interval between (periodic) tests, as well as time available for corrective maintenance actions should be known, as should details of the support equipment and personnel involved. Specific information on prescribed functions during each operational phase is also required.

6.3 Fault tree graphical description and structure

Components of a fault tree are as follows:

Gates:

- Symbols showing the logical relationship between input events and the output event
 - static gates – outcome not dependent on the order of occurrence of inputs,
 - dynamic gates – outcome dependent on the order of occurrence of inputs.

A table describing dynamic gates and comments about their use is shown in Annex A, Table A.3. An example of a PAND gate is shown in Figure A.1.

Events

- Lowest level of inputs in a fault tree. Commonly used event symbols and their definitions are shown in Annex A, Table A.1.

Graphical components of a fault tree are as follows:

- a) fault tree logic symbol (gates);
- b) gate input connection lines;
- c) intermediate event descriptions;
- d) transfer in or out symbols;
- e) primary event symbols.

All relevant events should be included in the fault tree. Such events should include the effects of environmental or other stress conditions to which the item might be subjected including the software, controls and status monitoring; those which are possible during operation, even if outside the design specification.

Events which the analyst has considered, but excluded from further analysis as not applicable, should be documented in the report but not included in the final fault tree.

If the fault tree highlights two or more system performance problems caused by one existing fault, then the event describing that fault should be included in the fault tree in multiple places. This event also should be marked as a common event. In quantitative analysis, the common event is included in calculations only once and all disjointing criteria shown in 7.5.5.4 should be applied. To avoid accidental inclusion of common events in multiple calculations, conventional labelling of such events should be established and used. This type of labelling has to be consistent. If computer software is used for fault tree evaluation assistance, appropriate conventions and settings shall be used.

When fault trees are created, they can be presented in a vertical form, from top to bottom, or in a horizontal form from left to right. When the fault tree is represented in horizontal form, all of the symbols shown in Tables A.1 through Table A.4 are rotated 90° counter clockwise.

The fault trees may also be read or investigated in opposite directions, e.g. dealing with occurred accidents, failures, etc.

7 Fault tree development and evaluation

7.1 General

Development of a fault tree starts with the definition of the top event. Development of a fault tree in its traditional application, or for a system reliability and the failure mode analysis, is a deductive method where the analysis starts from the top undesired event as it is defined for the scope of analysis. Once developed to the intended extent, the fault tree becomes a graphical representation of all events that either by themselves or in conjunction with other events contribute to the occurrence of the top event.

7.2 Scope of analysis

The definition of the scope of analysis should include the definition of the system to be analysed, the purpose and extent of the analysis and the basic assumptions to be made. These assumptions should include those related to the expected operating and maintenance conditions as well as to system performance under all possible conditions of use.

FTA can provide information on

- system reliability analysis, in cases where probabilities of occurrence of the primary events are known,
- the root cause(s) of an unfavourable outcome that has taken place that may require an appropriate corrective action.

FTA scope extends to a complex system when probability of a top event occurring has to be determined. Here, unlike other reliability modelling and prediction analytical methods, the scope of analysis extends to inclusion of only those failure modes or potential events that have influence on the system operation, that is, only those failure modes that are pertinent to the occurrence of the top event. This then results in a more focused system assessment that can be better compared to the field performance.

7.3 System familiarization

In order that a fault tree analysis can be carried out successfully, a detailed knowledge of the system is required. However, some systems may be too complex to be understood fully by one person. In this case, the process of familiarization requires that the necessary specialized knowledge be gathered by team activity.

7.4 Fault tree development

Fault tree development starts with the definition of the top event, or unfavourable outcome which should be defined unambiguously. The top event is the focus of the entire analysis. Such an event may be the onset or existence of a dangerous condition (safety analysis), or the inability of the system to provide a desired performance.

If, in a system performance or reliability analysis, an output event from a gate defines the inability to perform a function, the corresponding input events could represent appropriate causes: e.g. failure due to hardware faults, software faults, performance limitations, incorrect command (control failure) and human error.

The development of a particular fault tree branch terminates after any one or more of the following have been reached:

- primary events, i.e. independent events for which the relevant characteristics can be defined by means other than a fault tree;
- events which need not be developed further, as defined by the analyst;
- events which have been or will be developed further in another fault tree – transfers; if that event is developed further, such an event has to bear the same identification as the corresponding event on the other fault tree so that the latter tree effectively forms a continuation of the former.

7.5 Fault tree construction

7.5.1 Fault tree format

Fault trees may be drawn either vertically or horizontally. If the vertical arrangement is used, the top event should be at the top of the page and the basic events at the bottom. If the horizontal arrangement is used, the top event may be on the left or right of the page.

Examples in the standard (Figure 1 and others) show the development and representation of a fault tree. In addition to the defined symbols for the fault tree logic, the examples contain the event description box, as well as the function or state the event represents.

7.5.2 Use of quantitative (Method B) FTA in system or product development for reliability improvement

7.5.2.1 General

FTA is a systematic manner to identify events that contribute to the occurrence of the top event, and with proceeding deductive methods, to the intermediate events and ultimately to the primary events. This systematic analysis identifies failure modes of system components and the contributing factors to their own probability of occurrence, e.g. operational or environmental stresses including software commands, human factors etc.

The primary difference between FTA and other reliability modelling and analysis methods is that the FTA includes only the events that contribute to the occurrence of the top event, and models their functional combination and possible dynamic interaction and interdependency, while other methods deal with the component failure rates or probabilities (not the component failure mode probability) with the usual assumption of failure independency. As an example, a voltage-filtering capacitor can fail open (about 35 % of its failures), short (about 55 % of its failures) or can change capacitance (the remaining 10% of its failures), but only a failure mode *short* would cause the product failure, then only about 55 % of its failure probability is taken into account. This allows for realistic identification of those failure modes or their causes that need the designer's attention.

Capability of FTA to correctly model sequence of events (with the assistance of Markov analysis) primary or intermediate, as an input into another intermediate event makes it an instrumental tool to identify those primary events/functions or intermediate events that are major contributor to a product's unreliability. This allows design improvements that would mitigate such design flaws, and the revision of the FTA to verify the improvement or to do the trade-off study of two or more improvement options.

In all subsequent gate models, it is important to keep in mind that the probability values are those of failure modes and their contributing factors only, or are the probabilities of the static or dynamic combinations of the failure modes leading to loss of a function and system failure.

The use of FTA in this manner is explained in detail in the “NASA Fault Tree Handbook with Aerospace Applications version 1.1”, mentioned in Clause 6.

7.5.2.2 Series system configuration

In reliability modelling, the assemblies (blocks or components in the reliability block diagram) are in a series configuration in a system when a failure of any of them would constitute the system failure.

The corresponding model in the fault tree would be that all of those “blocks” (gates or events) flow into an OR gate.

The mathematics for reliability of the top “system” consisting of “n” independent blocks would be:

$$R_S(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) \cdot \dots \cdot R_i(t) \cdot \dots \cdot R_n(t) \quad (1)$$

The above expression in terms of reliability would be that block 1 **and** block 2, **and** the rest of the blocks have to be operational for the system to be operational.

In FTA, the opposite is used. The failure outcome is produced by either component 1 failure OR component 2 failure, and so on. This is why the OR gate represents a series system or assembly configuration.

The mathematics behind an OR gate is the same as the one shown for a series system, except expressed in terms of probability of failure $F(t)$, which is a probabilistic complement to the reliability.

$$F(t) = 1 - R(t) \quad (2)$$

The probability of an unfavourable outcome of an OR gate (“system”) consisting of n independent input gates or events is:

$$F_S(t) = 1 - (1 - F_1(t)) \cdot (1 - F_2(t)) \cdot \dots \cdot (1 - F_i(t)) \cdot \dots \cdot (1 - F_n(t)) \quad (3)$$

The system fails when any of the components (blocks) fail. An example of an OR gate is shown in Figure 2. In Figure 2, and all subsequent figures in this clause, the relevant failure mode of a component is the failure mode which, as an input event, causes occurrence of the output event.

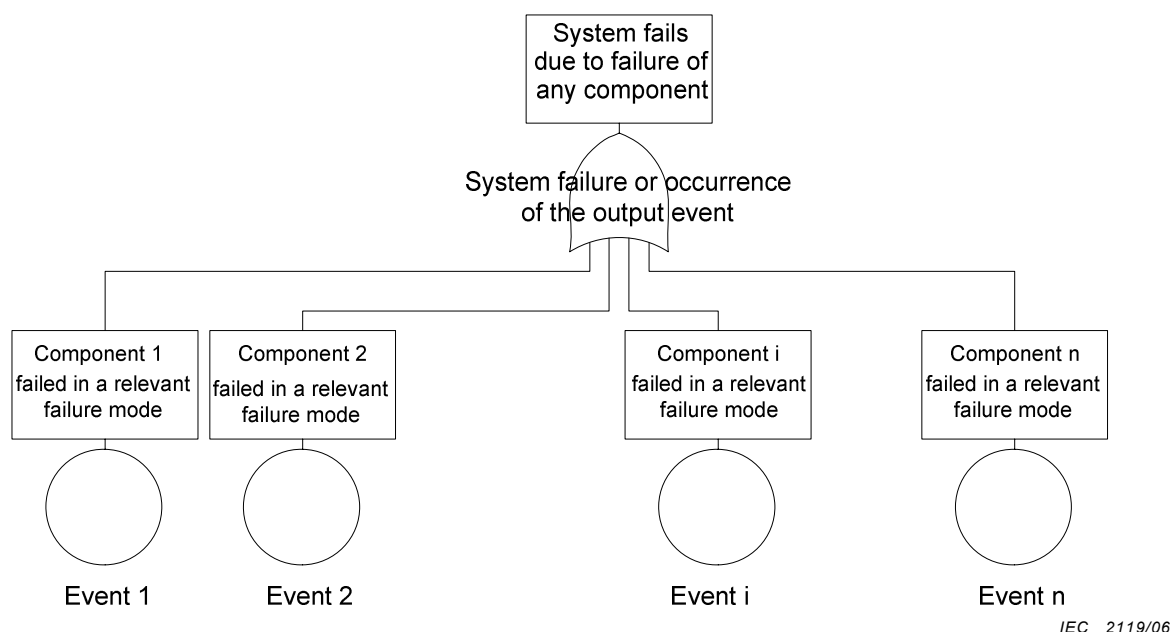


Figure 2 – Fault tree representation of a series structure

7.5.2.3 Parallel system configuration, redundant systems

7.5.2.3.1 Active redundancy

This subclause assumes that failure characteristics (models) for each input to the active redundancy remain the same, independent of how many other inputs are working. It also assumes that each input to the active redundancy block is independent. Where it is not independent, see disjointing (Annex B) for additional guidance.

If an output event were to occur only if all contributing independent events occur, then they should be linked by an AND gate. Such a configuration may be redundant. It is also referred to as a parallel system for reliability analysis, even though the physical configuration might be different.

The independence requirement is met when the probability of input events does not change, regardless of the state of other inputs.

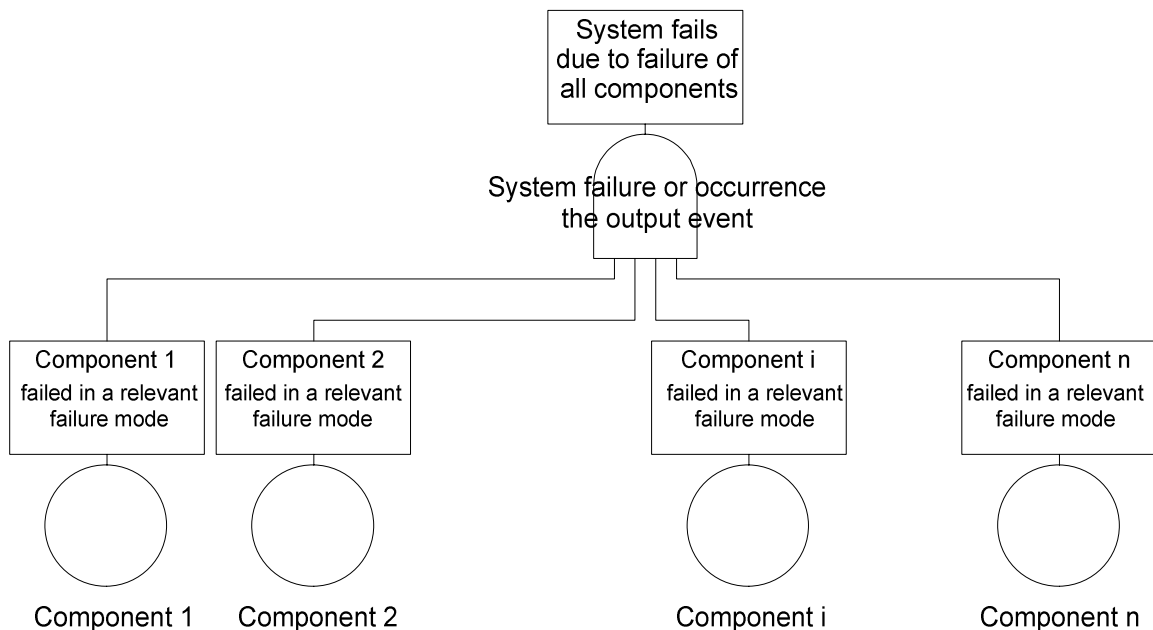
The associated mathematical expression in reliability is that the system is operational if component 1 OR component 2, OR out of any of the components, at least one of them remains operational, that is the system fails if all of the components fail.

$$R_S(t) = 1 - \prod_{i=1}^n (1 - R_i(t)) \quad (4)$$

With the FTA, this is represented by an AND gate, having “n” input gates or events, with the meaning that the system fails if component 1 AND component 2, AND the rest of the components fail, with similar mathematics. The probability of failure is then:

$$F_S(t) = \prod_{i=1}^n (F_i(t)) \quad (5)$$

An FTA representation of parallel redundancy, where only one component surviving is sufficient for the successful system operation, or the system fails only if all components fail, is shown in Figure 3.



IEC 2120/06

Figure 3 – Fault tree representation of parallel, active redundancy

Redundant components may operate in a load-sharing mode (e.g. generators to a power network), the failure event probability of surviving components may increase as each fails. Such changes in event probability would break the independence requirement for use of a simple AND gate.

If an output were to occur only if all contributing events occur, but the input events are dependent on each other, then an AND gate cannot be used. In that case, a dynamic gate is used.

When the redundancy is such that the condition of system success is that k out of n identical blocks remain operational, then the mathematical expression for unreliability as used in the FTA is as follows:

$$R_S(t) = 1 - \sum_{i=0}^{k-1} \frac{n!}{i!(n-i)!} \cdot [R_0(t)]^i \cdot [1 - R_0(t)]^{n-i}$$

or

$$F_S(t) = \sum_{i=0}^{k-1} \frac{n!}{i!(n-i)!} \cdot [1 - F_0(t)]^i \cdot [F_0(t)]^{n-i}$$

(6)

In FTA, this combination of events is represented by the majority vote gate, where the vote number is $m = n - k + 1$ and the symbol in the corresponding gate, m , designates how many events have to take place for the event to propagate further in the tree.

As an example, if the required redundancy is 3 out of 6, the majority vote is 4, as the occurrence of four input events would leave only two remaining components operational, which means that the system had failed, as the requirement was for three components to be operational out of 6.

The majority vote gate, along with other examples of gates used in reliability modelling, is shown in Figure 4.

7.5.2.3.2 Passive (stand-by) redundancy

Stand-by redundancy is when only the number of components required for operation is active, and in case of failure of one or more of those components one or more replacement spares is activated to take the function of the failed components. System failure is defined as the event when the total number of functional components is less than the number required for system operation. The redundant components (spares) may in analysis be considered not subject to failure (cold spares) or subject to some intermediate likelihood of failure (warm spares) until brought into the active operation, or may be equally subject to failure as when operational (hot spares).

Representation of stand-by redundancy is not possible with the static gates. However, a SPARE gate symbol may be used. Markov analysis shall be used to analyse this gate.

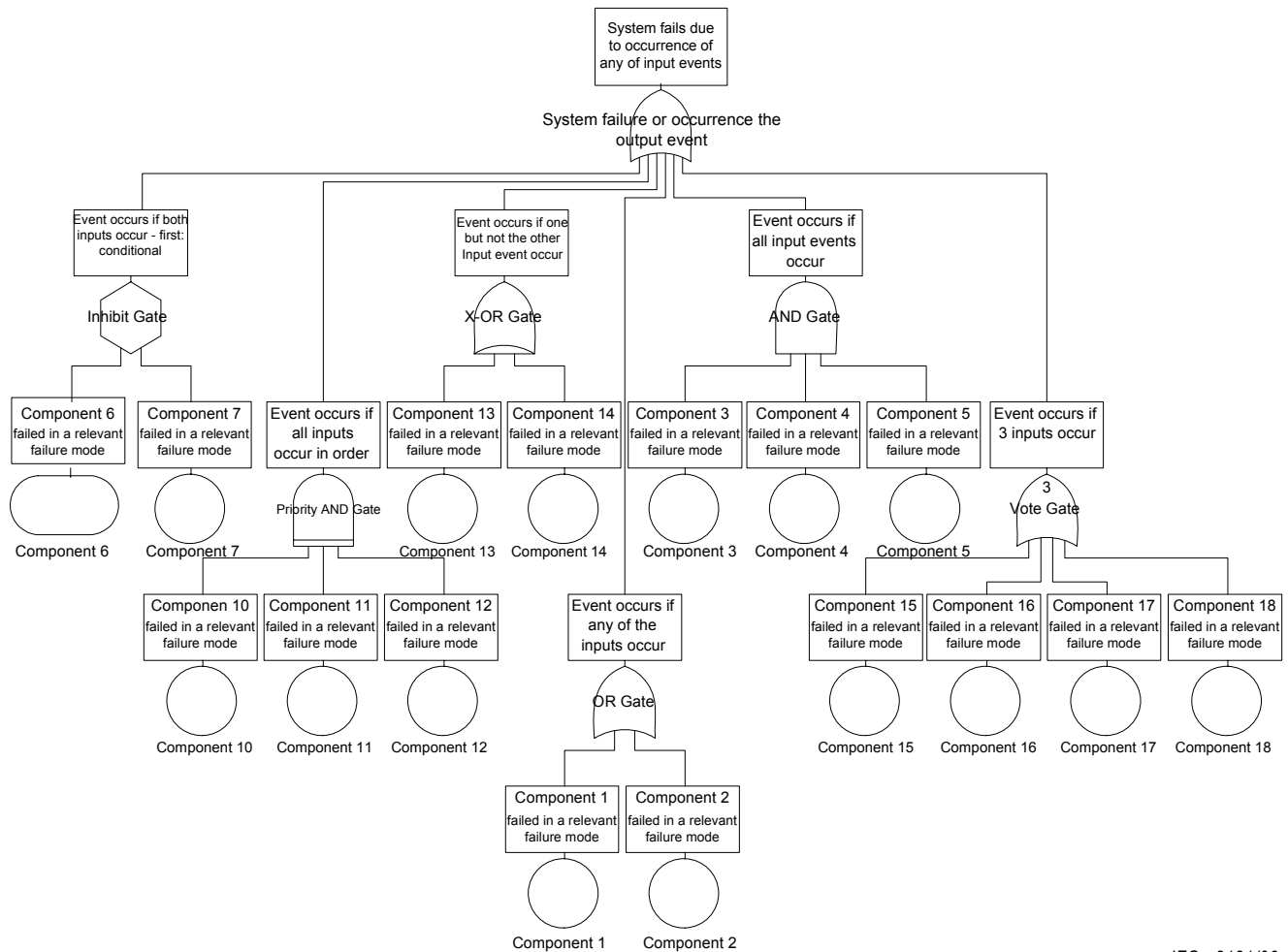
Stand-by redundancy is successfully addressed by dynamic gates. Here, the SPARE gate is used for redundant systems where event probabilities change.

7.5.2.4 Representation of conditional probability repeated (common cause) events, and transfer out events

Conditional probability is where the probability of an event taking place is dependent on occurrence of another, where the second event takes place only if the first event occurs.

Conditional probability is also expressed in terms of dynamic gates that use Markov state analysis, such as PRIORITY AND gates defined in Table A.4, Annex A.

An example of conditional probability is shown as a part of Figure 4.



IEC 2121/06

Figure 4 – Example of fault tree showing different gate types

The graphical representation of a fault trees shown in Figure 1 and other figures shown in this standard should be considered examples only.

7.5.2.5 Visual representation of fault trees

Fault trees may have various graphics, dependent on the preferences and customary representation in different countries and in different applications. Some representations use rectangular shapes with the symbols in them such as $\&$, for an AND gate, and $\geq$ for the OR gate. In this case, the null gate is also classified as an OR gate, except such an OR gate has only one input event, as null gates represent an outcome event having only one input event. Caution should be exercised when representing the gates and events as rectangles to ensure that the symbols in them are well defined and clearly marked.

The rectangular gates and events representation is shown in Figure 5.

In Figure 5, event A will occur only if both events B and C occur. Event C occurs if either event D or E occurs.

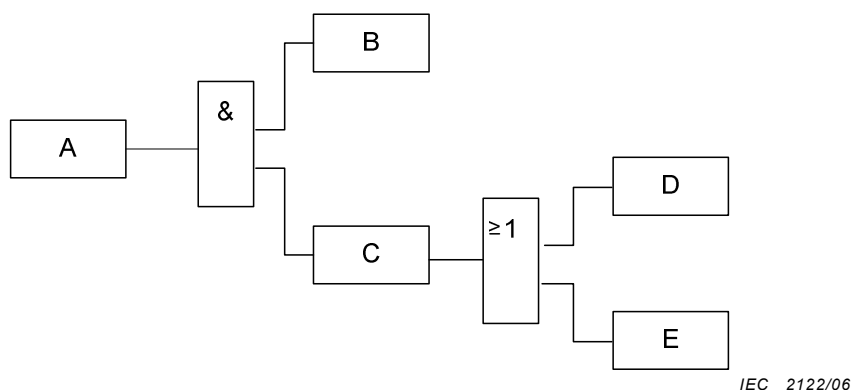
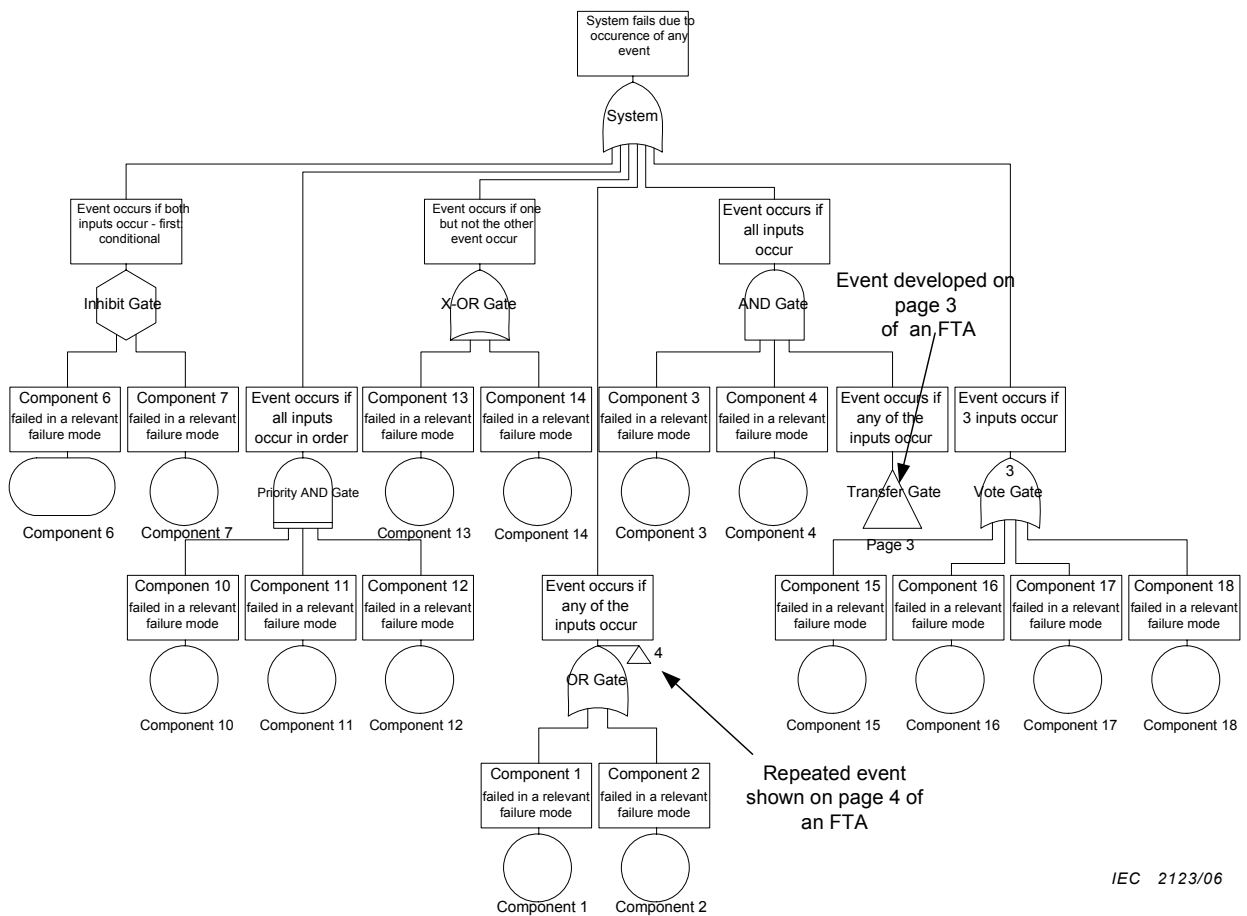


Figure 5 – Rectangular gate and events representation

NOTE For each event, A, B, etc., it is preferable to list the name or description of the event first, followed by event code and probability of occurrence.

If an event represents a repeated event or a common cause event, it is shown in the fault tree repeatedly, but with a flag that it is also shown as an input event to other events in the fault tree. All repeated or common cause events in the set shall have the same event code and be marked by a transfer-in symbol or a symbol normally used as such in a particular fault tree. This rule applies to all repeated or common cause events except the event on the lowest level in the set, which is marked by a transfer-out symbol. In some fault tree graphics, the symbols for the repeated primary events or higher levels, are the same.

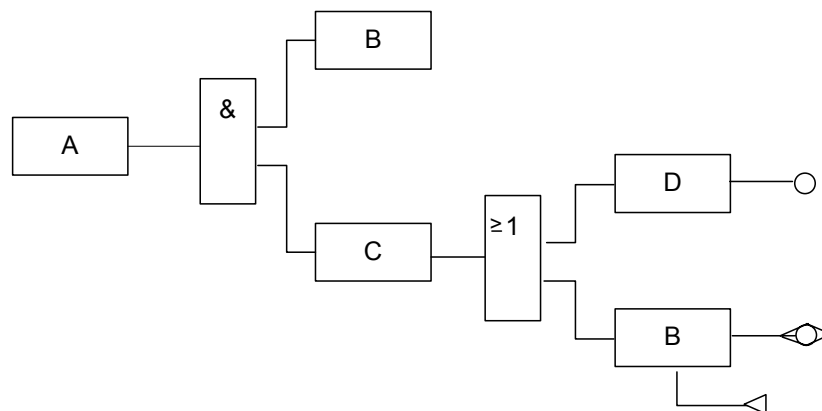
Figure 6 shows an example of graphical representation where the repeated event, represented as an OR gate and flagged with the page number, is found in another place of the fault tree, where it is an input event to a different, higher level event. This event can appear in more than two places of a fault tree. An example of such an event could be elevated temperature or humidity causing occurrence of two different events in a system. Disjointing is in this case applied to such event. Also in Figure 6, a transfer gate is shown to indicate that this event was developed in another place or page of a fault tree. This usually is the case when a more complex event is an input event to a higher level event, thus it has to be further developed on a separate sheet. A PRIORITY AND gate, shown in Figure 6, would be used when the output event is dependent on the ordering of input events.



IEC 2123/06

Figure 6 – Example fault tree containing a repeated and a transfer event

An example of a rectangular fault tree showing transfer out repeated or common cause event is shown in Figure 7. Event B is an event, which is analysed further on another fault tree. Event D is a basic event.



IEC 2124/06

Figure 7 – Example showing common cause considerations in rectangular gate representation

7.5.3 Construction procedure

The first steps in construction of a fault tree is to clearly define the top event, the scope and the objective of the fault tree, the boundaries of the system or object of analysis and the resolution of the analysis. This objective should be defined in terms of the definition of the top event.

The top event must describe a problem that has to be analysed in order to determine contributing causes. In FTA application for reliability improvement of a system under development, the top event is a system failure and the objective of analysis is to determine contributors to this event and identify design weakness or unreliable components. In quantitative analysis the probability of occurrence of the top event and all, or most, inputs will be determined. In qualitative analysis, Method A, the inputs to the top event will be investigated in order to identify the causes of its occurrence (other events or faults). In quantitative analysis, Method B, for design improvement, the inputs to the top event are analysed to identify the major contributors to the top event and to improve design by systematic elimination of those weaknesses or mitigation of contributing failure modes.

The scope of analysis defines the events or the failure modes that will be included in the fault tree. The scope also covers the details of the problem being analysed, the revision level of the system design under analysis and the use profile of the system and other operational and environmental conditions, while the boundaries define what is included and what is excluded from that system (e.g., internal connections, mechanical enclosures, etc.).

A fault tree should be constructed in such way that it clearly represents the flow of events that cause occurrence of the top event.

Once the top event is clearly defined as well as the system boundaries or analysis extent, then the fault tree construction flows from the top down. The top event has inputs and their combination is modelled and represented by the appropriate gate. Inputs into the top event are then developed systematically to be results of their own input events. Each of the inputs, going down the fault tree, is developed separately and this development is completed when the primary events are reached.

The resolution will specify to what extent the system is to be analysed. As an example, an electronic system can be analysed down to its components and their failure modes and causes, or to a higher level of its assemblies (e.g., signal processor, power amplifier, specific supply voltage regulators, etc.). At times, the resolution can be a combination of detailed and assembly level analysis, dependent on availability of probability of occurrence information.

Strict adherence to the concept of "immediate cause" is necessary to ensure that failure modes are not omitted by reason of the assumption that such modes have been included previously.

The concept of "basic units" can be used to save the analyst the effort of developing fault tree diagrams that do not yield new or useful information. A basic unit is not developed further. It is treated as if it were a single unit or component or dealt with separately.

In order for the unit or event to be considered "primary", it is necessary and sufficient that the following three requirements be satisfied:

- both the functional and physical boundaries are clearly defined;

- operation of the unit does not depend on any supporting function, or all events related to the unit are expressed by a single OR gate having one of the inputs representing a fault of the unit, the remaining inputs representing inability to perform the corresponding support functions;
- no immediate causes can be determined for the occurrence of that event.

The nomenclature used in a fault tree should be standardized so as to minimize confusion and to clearly label and explain what the events are in an organized manner.

The actual construction of a fault tree follows the analytical logic of the flow of events.

- The "immediate cause" concept requires that the analyst determine the immediate necessary and sufficient causes for the occurrence of the top event. It should be noted that these are not the basic causes of the top outcome or top event, but the immediate causes or immediate mechanisms for the top event to occur. These may be the lower level (intermediate) events.
- The immediate, necessary and sufficient causes of the top event are now treated as intermediate events, and the analysis continues to determine their immediate and sufficient causes (input events) to determine their necessary and sufficient causes.
- The construction proceeds down the tree, transferring attention from mechanism to mode, and continually approaching a lower level of mechanism and mode, until ultimately the appropriate or defined level of resolution is reached. The individual basic events or primary (bottom) events are those that represent individual causes of potential failures or faults.

7.5.4 Fault tree evaluation

7.5.4.1 Investigation and analysis

Investigation includes a review of the fault tree structure by comparison with available information such as schematics, drawings, functional diagrams, software commands, identification of common events and a search for independent branches. Investigation should identify common cause events, but should not assume that their presence is benign. Such conclusions can be drawn only after a thorough analysis, using Boolean reduction or determination of minimal cut sets when the static gates are present, as the cut sets do not exist in dynamic gates, unless approximation is applied to ignore sequencing. As the difficulty of the analysis increases rapidly with the size of the fault tree, inspection of the fault tree allows the analyst to identify which branches of the fault tree are independent and can thus be analysed separately if needed.

Analysis of a fault tree follows the flow of events and identifies the causes of those events downward. Fault tree evaluation may be either logical (qualitative) or numerical (quantitative) or both. Analysis of a quantitative fault tree used in product development for reliability improvement identifies the high contributors to the probability of occurrence of the top event, and the causes for those with a high probability of occurrence. As an example, if the probability of failure of an assembly of a system is a high contributor to the probability of system failure, the cause is investigated and once identified, that failure mode can be mitigated. To illustrate this example, a high contributor to the probability of a failure of a system power supply can be identified as an overstressed capacitor. Replacement of that capacitor with another, with higher voltage rating, considerably reduces probability of failure of the assembly and subsequently of the system.

Analyses should be documented in such a way that results can be reviewed and any changes needed can be incorporated in order to reflect changes in design, operating procedures or improved understanding of the physics of failure. In order that this may be done, a systematic approach to the construction is required. To implement this systematic approach, two concepts have to be understood and used consistently. These are the concepts of "immediate cause" (input events) and of "basic unit".

The primary purposes of logical (qualitative) and numerical (quantitative) analyses of a system can be summarized as follows:

- identification of events or faults which can directly cause a system failure, and contribute to the probability of such events and, in that manner, improve dependability (reliability) of a system;
- mitigation of faults that may be contributors to the outcomes that may be potential safety hazards;
- assessment of fault tolerance of the system (ability to function even after a specified number of lower level failures or events contributing to the occurrence of a system failure have happened);
- assessment of information to locate critical components and failure mechanisms;
- identification of device failure diagnostics, inputs to repair and maintenance strategies, etc.

The assessment of fault tolerance of the system includes a determination of the degree of redundancy in the system and a verification that the redundancy is not impaired through common events. Although the major part of fault tolerance assessment does not require the use of numerical data, such numerical data are required to evaluate which combinations of events causing a system fault are the most likely to occur.

7.5.4.2 Logical analysis

7.5.4.2.1 General

Three basic techniques are used for logical analysis: investigation, Boolean reduction and determination of minimal cut sets. The basis of logical analysis is modelling which provides fault tree representation of a structure, be it functional, architectural, or a mixture of the two. Correct modelling means representing the functions or components of a system in such a way as to establish their interactions, dependencies, immediate causes of unfavourable outcomes, etc.

7.5.4.2.2 Boolean reduction

Boolean reduction can be used for the evaluation of the effects of common events (identical events occurring in different branches) in fault trees where the occurrence of the top event does not depend on timing or sequencing of events. Boolean reduction can be carried out by solving Boolean equations for the fault tree. Boolean reduction can also be used to identify minimal cut sets.

7.5.4.2.3 Identification of minimal cut sets

There are several methods of determining minimal cut sets, but application of larger trees may be difficult and incomplete. For this reason, various computer programs are available to assist the analyst.