Draft for Public Comment

Form 36

DPC: 18/30378905 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000
Fax: +44 (0)20 8996 7400
www.bsigroup.com

Date: 07 June 2018
Origin: International

Latest date for receipt of comments: 30 July 2018

Project No. 2018/01662

Responsible committee: DS/1 Dependability

Interested committees:

Title: Draft BS EN 61025 Fault tree analysis (FTA).

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

i) has any issues related to 3rd party IPR, patent or copyright
ii) affects other national standard(s)
iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 30 July 2018

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop http://shop.bsigroup.com or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from https://standardsdevelopment.bsigroup.com/.

Responsible Committee Secretary: Mrs Philippa Younas (BSI)
Direct tel: 020 8996 7239
E-mail: philippa.younas@bsigroup.com

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at **https://standardsdevelopment.bsigroup.com/**. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex **(e.g. 3.1)**	Paragraph/Figure/ Table/Note	**Type of comment**	**Commend (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations on each comment submitted**
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

Documents
Document Sharing Hub

Full document details: 18/30378905 DC

56/1778/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER: **IEC 61025 ED3**	
DATE OF CIRCULATION: **2018-06-01**	CLOSING DATE FOR COMMENTS: **2018-08-24**
SUPERSEDES DOCUMENTS: **56/1777/RR**	

IEC TC 56 : DEPENDABILITY	
SECRETARIAT: United Kingdom	SECRETARY: Mr Mick Maghar
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	

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

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

TITLE:

Fault tree analysis (FTA)

NOTE FROM TC/SC OFFICERS:

Copyright © 2018 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

AVA Documents Document Sharing Hub

Full document details: 18/30378905 DC

CONTENTS

FOREWORD 7
INTRODUCTION 9
1 Scope 11
2 Normative references 11
3 Terms and definitions 11
4 Symbols and abbreviated terms 21
5 General considerations 29
5.1 Fault tree within the dependability framework 29
5.2 Objectives 30
5.3 Applications 31
6 Fault tree analysis development 31
6.1 Simple example to help the clause understanding 31
6.2 Steps of a FTA 32
6.3 Required information to undertake a FTA 34
6.4 Identification and labelling in a fault tree 34
6.5 Report 35
7 Elementary models 36
7.1 Developing the models 36
7.2 Series system configuration 37
7.3 Parallel system configuration 39
7.4 Mix of series and parallel structures 40
7.5 *k*/*n* architectures 40
7.6 NOT, NOR, and NAND logic gates 43
7.7 Sub-trees and transfer gates 44
8 Qualitative analysis 46
8.1 Electrical analogy and notion of minimal tie sets and cut sets 46
8.2 Identification of minimal cut sets of a FT 47
8.3 Qualitative analysis with minimal cut sets 47
9 Quantitative analysis with constant probabilities 48
9.1 Sylvester-Poincaré formula 48
9.2 Semi-quantitative analysis with minimal cut sets 49
9.3 Quantitative calculations with disjointed terms 50
10 Quantitative analysis with time dependent probabilities 51
10.1 General 51
10.2 Non repaired items 54
10.2.1 General 54
10.2.2 Simple non-repaired item 54
10.2.3 Small sub trees related to non-repaired items 55
10.2.4 Probabilistic calculation of FT modelling non-repaired components 56
10.3 Repaired items 57
10.3.1 Unavailability calculations 57
10.3.1.1 Simple repaired item 57
10.3.1.2 Small sub trees related to repaired items 57
10.3.1.3 Periodically tested primary events 58

Documents
Document Sharing Hub

10.3.1.4 FT driven Markov processes ... 59
10.3.2 Average unavailability calculations ... 60
10.3.3 Asymptotic unavailability calculations ... 60
10.3.4 Frequency calculations and METBF ... 62
10.3.5 Unreliability calculations ... 63
11 Boolean techniques for quantitative analysis of large models ... 65
11.1 General ... 65
11.2 Detailed procedure for disjointing minimal cut sets ... 66
11.3 Shannon decomposition and Binary decision diagram (BDD) ... 67
11.3.1 Shannon decomposition ... 67
11.3.2 Binary decision diagram (BDD) ... 69
11.3.2.1 Building of BDDs ... 69
11.3.2.2 Minimal cut sets identification ... 70
11.3.2.3 Probabilistic calculations with BDDs ... 71
11.3.2.4 Conditional probability calculations with BDD ... 72
12 Uncertainty propagation ... 73
13 Extension of fault tree technique ... 75
13.1 XOR gates and non-coherent fault trees ... 75
13.2 Dynamic fault trees ... 78
13.2.1 General ... 78
13.2.2 Local interactions ... 78
13.2.3 Systemic dynamic interactions ... 79
13.2.4 Graphical representations of dynamic interactions ... 80
13.2.5 Probabilistic calculations ... 83
13.2.5.1 Dynamic FT reducible to static FTs ... 83
13.2.5.2 Dynamic FT not reducible to static FTs ... 84
Annex A (informative/normative) Other Symbols ... 86
Annex B (informative) Combinations with other reliability analysis techniques ... 88
B.1 Combination of FTA and failure modes and effects analysis (FMEA) ... 88
B.2 Combination of FTA and event tree analysis (ETA) or cause-consequence analysis (CCA) ... 88
B.3 Combination of FTA and Markov analysis ... 90
B.4 Combination of FTA and binary decision diagram (BDD) techniques ... 90
B.5 Combination with the reliability block diagram ... 91
Annex C (informative) Automated fault tree construction ... 92
Annex D (informative) Importance factors ... 93
D.1 General ... 93
D.2 Vesely-Fussell importance factor ... 93
D.3 Birnbaum importance factor or marginal importance factor ... 93
D.4 Lambert importance factor or critical importance factor ... 94
D.5 Diagnostic importance factor ... 95
D.6 Risk achievement worth ... 95
D.7 Risk reduction worth ... 95
D.8 Differential importance measure ... 96
D.9 Remarks about importance factors ... 96
Annex E (informative) FT driven Petri nets ... 98
E.1 General ... 98
E.2 Example of sub-PN to be used within RBD driven PN models ... 99

AVA Documents
Document Sharing Hub
Full document details: 18/30378905 DC

E.3 Evaluation of the DFT state 100
E.4 Availability, reliability, frequency and MTTF calculations 102
Annex F (informative) Numerical examples and curves 104
F.1 General 104
F.2 Typical series structures (OR gates) 104
F.2.1 Non-repaired components 104
F.2.2 Repaired components 105
F.3 Typical parallel structure (AND gate) 107
F.3.1 Non-repaired components 107
F.3.2 Repaired components 108
F.4 Series-parallel structures 109
F.5 Complex structures 110
F.5.1 Fault tree with a repeated event 110
F.5.2 Convergence to asymptotic values versus MTTR 112
F.5.3 System with periodically tested components 112
F.6 Dynamic fault tree example 114
F.6.1 Comparison between analytical and Monte Carlo simulation results 114
F.6.2 Dynamic RBD example 115
Bibliography 118

Figure 1 – Shannon decomposition of a simple Boolean expression and resulting BDD 21
Figure 2 – Simple pumping system 31
Figure 3 – FT related to the system illustrated in Figure 2 37
Figure 4 – Series configuration: equivalence between RBD and FT 38
Figure 5 – Parallel configuration: equivalence between RBD and FT 39
Figure 6 – Example of mix between series and parallel structures 40
Figure 7 – Majority vote structure: equivalence between RBD and FT 41
Figure 8 – Equivalent 2/4 majority vote logic with common OR and AND gates 41
Figure 9 – Equivalence between inverted blocks and complementary primary events 43
Figure 10 – Equivalence NOR and AND gates with complementary events 43
Figure 11 – Equivalence NAND and OR gates with complementary events 44
Figure 12 – Use of transfer gates to split a large FT into sub-FTs 45
Figure 13 – Global FT related to Figure B.1 and Figure B.2 45
Figure 14 – Example of minimal cut and tie sets 46
Figure 15 – Example of minimal cut sets from a FT 47
Figure 16 – Principle of unavailability calculations: classical example 52
Figure 17 – Principle of unavailability calculations: example with periodically tested components 52
Figure 18 – Typical example of primary event related to a non repaired item 54
Figure 19 – Example of dependent primary events gathered into a single primary event. 55
Figure 20 – Equivalent Markov model for a PAND gate 56
Figure 21 – "Availability" Markov graph for a simple repaired item 57
Figure 22 – Standby redundancy 58
Figure 23 – Typical unavailability of a periodically tested component 59
Figure 24 – Average unavailability over [0, *T*] 60

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

142 Figure 25 – Asymptotic unavailability 61
143 Figure 26 – $U_S^{avg}(0,t)$ for a system with periodically tested components 61
144 Figure 27 – RBD, FT and equivalent Markov graph for reliability calculations 63
145 Figure 28 – Simplified notations for the example in Figure 6 66
146 Figure 29 – Shannon decomposition of a 2/4 logical structure 68
147 Figure 30 – Shannon decomposition (reduced graph) 69
148 Figure 31 – Binary decision diagram related to the FT in Figure 29 69
149 Figure 32 – Minimal cut set identification 70
150 Figure 33 – Probabilistic calculations from a BDD 71
151 Figure 34 – Calculation of conditional probabilities by using BDDs 72
152 Figure 35 – Example of distribution of a failure rate considered as a random variable 73
153 Figure 36 – Principle of Monte Carlo simulation 73
154 Figure 37 – Example of uncertainty handling by using Monte Carlo simulation 74
155 Figure 38 – Results highlighting the impact of input parameters uncertainties 75
156 Figure 39 – Equivalence XOR gate with a combination of AND and OR gates 75
157 Figure 40 – Example of non coherent Fault tree and of ITE gate 76
158 Figure 41 – BDD equivalent to the example of Figure 40 77
159 Figure 42 – Symbol for external elements 78
160 Figure 43 – Dynamic interaction between a CCF and primary events 80
161 Figure 44 – Various ways to indicate dynamic interaction between primary events 81
162 Figure 45 – Example of functional dependency due to a single repair team 81
163 Figure 46 – Implementation of a PAND gate 82
164 Figure 47 – Implementation of a SEQ gate 83
165 Figure 48 – CCF as a repeated event 83
166 Figure 49 – PAND gate modelled with a Markov process 84
167 Figure 50 – SEQ gate modelled with a Markov process 84
168 Figure B.1 – Analysis of a procedure by cause consequence diagram 89
169 Figure B.2 – Event tree equivalent to the cause consequence diagram in Figure B.1 89
170 Figure C.1 – Example of a sub-PN modelling a primary event 98
171 Figure C.2 – Example of a sub-PN modelling a common cause failure 99
172 Figure C.3 – Example of DFT based on FT driven PN 100
173 Figure C.4 – Logical calculation of classical FT structures 100
174 Figure C.5 – Example of logical calculation for an 2/3 gate 101
175 Figure C.6 – Example of sub-PN modelling a PAND gate with 2 inputs 101
176 Figure C.7 – Example of the inhibition of a primary event 102
177 Figure C.8 – Sub-PN for availability, reliability and frequency calculations 102
178 Figure D.1 – Unavailability/unreliability of a typical non-repaired series structure 104
179 Figure D.2 – Failure rate and failure frequency/failure density related to Figure D.1 105
180 Figure D.3 – Equivalence of a non-repaired series structure to a single component 105
181 Figure D.4 – Unavailability/unreliability of a typical repaired series structure 106
182 Figure D.5 – Failure rate and failure frequency related to 106
183 Figure D.6 – Unavailability/unreliability of a typical non-repaired parallel structure 107
184 Figure D.7 – Failure rate and failure frequency related to Figure D.6 108

AVA Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Figure D.8 – Unavailability/unreliability of a typical repaired parallel structure 108
Figure D.9 – Vesely failure rate and failure frequency related to Figure D.8 109
Figure D.10 – Example of mixing series and parallel structures..... 110
Figure D.11 – Vesely failure rate and failure frequency related to Figure D.10 110
Figure D.12 – FT with a repeated event 111
Figure D.13 – Unavailabilities and reliability from Figure D.12 111
Figure D.14 – Failure rate and failure frequency related to Figure D.12 111
Figure D.15 – Impact of the MTTR on the convergence quickness 112
Figure D.16 – Typical safety instrumented system 113
Figure D.17 – Unavailabilities related to primary events of the SIS (Figure D.16)..... 113
Figure D.18 – SIS unavailability and reliability 114
Figure D.19 –Vesely failure rate and failure frequency of the SIS (Figure D.16) 114
Figure D.20 –Parallel-series system..... 114
Figure D.21 – Analytical versus Monte Carlo simulation results according to the number of simulations..... 115
Figure D.22 – Parallel-series system with common cause failures and single maintenance team 115
Figure D.23 – Impact of CCFs and limited number of repair teams..... 115
Figure D.24 – Markov graphs modelling the impact of the number of repair teams 116
Figure D.25 – Approximation for two redundant components..... 117

Table 1 – Acronyms used in IEC 61025 21
Table 2 – Symbols used in IEC 61025 22
Table 3 – Graphical representation of Fault trees: events 25
Table 4 – Graphical representation of Fault trees: logic gates..... 26
Table 5 – Graphical representation of FTs: dynamic gates and functional dependencies..... 28
Table 6 – Semi-quantitative analysis of cut sets..... 49
Table 7 – Exact calculation with disjointed terms 51
Table A.1 – Other symbols..... 86
Table D.1 – Reliability parameters of the SIS in Figure D.16 113
Table D.2 – Impact of functional dependencies 116

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FAULT TREE ANALYSIS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61025 has been prepared by IEC technical committee 56: Dependability.

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

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

a) The structure of the document has been entirely reconsidered, the title modified and the content extended and improved. It has been merged with the mathematical content of the IEC 61078 (Reliability block diagram) about probabilistic calculations to provide more information about availability, reliability and failure frequency calculations. Same notations have been used to help cross reading of the standards;

b) Clause 3 has been extended and clauses have been introduced to describe the electrical analogy, the uncertainty propagation, the "non-coherent" fault trees and the "dynamic" fault trees;

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

c) Annex B (Combinations with other reliability analysis techniques), Annex C (Automated fault tree construction), Annex D (Importance factors), Annex E (FT driven Petri net models) and Annex F (Numerical examples and curves) have been introduced.

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

FDIS	Report on voting
56/XX/FDIS	56/XX/RVD

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

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

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

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

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

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

Documents
Document Sharing Hub

Full document details: 18/30378905 DC

INTRODUCTION

This standard is a support standard related to analysis techniques and it is primarily devoted to practitioners. The status of this technique within the dependability framework is analysed in management standards (e.g. [10]).

Fault tree analysis (FTA) is concerned with the identification and analysis of combinations of conditions and factors, referred as "primary events" or "leaves", that cause or may potentially cause or contribute to the occurrence of a defined undesirable outcome, referred as the "top event". It is a deductive (top-down / cause-effect) method which is very effective to analyse multiple failure combinations. This is why FTA is efficiently used to enhance the results obtained by other dependability methods like FMEA [9] or HAZOP [11] which, inductive in nature (bottom-up, effect-cause), are focused on single failure analysis. Depending of the scope, the analysis can be qualitative or quantitative. The qualitative identification of the critical paths (minimal cut sets) allows identify the weak points and to determine how the product or system can be brought back to operation. The quantitative results (unavailability, reliability, failure frequency, importance factors) provide information for more advanced analyses which can be used as decision aid for improving the performance and safety of products and systems in a cost efficient way. This approach has been introduced first in 1962 by the US air force within the Minuteman project framework ([1], [2]). While small FTA can be made by hand, FTA of large systems requires software support.

NOTE With FTA the top event is usually seizure or degradation of system perfomance, safety or other important operational attributes. Nevertheless a similar approach called STA (success tree analysis) can be used for success analysis and in this case the top event is the attribute describing the success.

The fault tree (FT) itself is an organized graphical representation that can be clearly understood and analyzed. Standardized symbols are used to show the logical connections between the primary events (e.g. components faults) needed for leading to the top event occurrence (e.g. system fault). In its simplest form it implements conventional logical gates and is equivalent to a logical equation giving the top event in function of the primary events, both being considered as Boolean variables. This is why FTA, like the reliability block diagram (RBD) [3] or event tree analysis (ETA) [4], is an analytic method belonging to the Boolean approaches. In this case the conventional rules of probabilistic calculations with constant values apply and provided that each primary event in the FT behaves independently from each other then the probabilistic calculations can be extended to time dependent probabilistic calculations involving non-repaired as well as repaired primary events (i.e. components). In this case three dependability measures related to the system unsuccessful functioning can be considered: the unreliability, $F_S(t)$, the unavailability, $U_S(t)$ and the failure frequency, $w_S(t)$. While, for systems involving repaired components, the calculations of $U_S(t)$ or $w_S(t)$ are quite straightforward, the calculation of $F_S(t)$ implies systemic dependencies (see definition 3.51) which cannot be taken into account within the mathematical framework of FTs. However, in particular cases, approximations of $F_S(t)$ are available.

The FT technique is linked to RBD [3][1] and Markov techniques [5]:

- The underlying mathematics is the same for FTs and RBDs: when a FT is focused on system fault, the RBD is focused on system success. It is always possible to translate a FT into an RBD and vice versa. Then FT and RBD models share dual logical expressions and the mathematical developments and limitations are similar.
- When the unavailability, $U_i(t)$, of one primary event, X_i, can be calculated by using an individual Markov process [5] independent of the other primary events, this unavailability, $U_i(t)$, can be used as input for the calculations related to a FT including this primary event.

[1] Numbers in square brackets refer to the Bibliography.

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

This approach where a FT provides the logic structure and Markov processes numerical values of the unavailabilities of the primary events is called "FT driven Markov processes"

However many non-Boolean extensions (e.g. ordered events, priority gates, dependent events etc.) are commonly implemented which are useful for qualitative analysis but for which Markov [5] or Monte Carlo simulation based on dynamic fault trees (DFT), or Petri net techniques [6], are more suitable for quantitative analysis.

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

FAULT TREE ANALYSIS

1 Scope

This International Standard describes fault tree analysis and provides guidance on its application by practitioners as follows:

– definition of basic principles;
  - explaining the relationships of FTA to other reliability modelling techniques;
  - identification of appropriate assumptions, events and failure modes;
  - identification and description and mathematical meaning of commonly used symbols;
– description of the steps involved in performing the FTA;
– description of the use of FT for qualitative analysis;
– description of the use of FT for quantitative analysis;
  - requirements, explanations and limitations of the associated mathematical modelling;
  - procedures for calculating dependability measures (unavailability, failure frequency and unreliability) for different type of systems simple or large, with constant or time dependent probabilities or with non-repaired or repaired faults;
  - the relationships with reliability block diagram analysis (see IEC 61078 [3]) and Markov techniques (see IEC 61165 [5]).
– extension of fault trees (non-coherent FTs and dynamic FTs)
– importance factors
– numerical examples

Examples are used to clarify the meaning of the clauses. Warnings about mathematical difficulties are raised. Explanations and solutions are provided for an effective and relevant application of this standard with full knowledge of the modelling and calculating properties of FTA.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* (available at http://www.electropedia.org)

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-192 as well as the following 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. Besides, some terms have been taken from IEC 60050-192 and modified for the needs of this standard.

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

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

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

3.1
Boolean related model
mathematical model where the state of a system is represented by a logical function of Boolean variables representing the states of its components

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

[Source IEC 61078:2016]

3.2
Fault tree
FT
Logic diagram showing the faults of sub items, external event, or combinations thereof, which cause a predefined, undesired event

Note 2 to entry: A FT is a directed acyclic graph (i.e. a graph without loops) representing the logical links between a system fault (called top event) and the faults (named primary events) of its constituting components. These links are mainly represented by conventional logical OR and AND gates (see Clause 4 and Clause 7).

Note 2 to entry: According to IEC 60050-192 [192-04-01], a fault is a state resulting from a previous failure which is an event. However in the FT context the failure (event) and the resulting fault (state) are merged and the primary events represent both aspects.

[SOURCE: IEC 60050-192:2015, 192-11-07 — Notes to entry have been added]

3.3
Static fault tree
Fault tree implementing only logical gates

3.4
sub-fault tree
fault tree related to an intermediate event of a larger fault tree

Note 1 to entry: sub-fault trees are used to split large fault trees in several parts. Transfer gates (see Table 4) are used to link the sub-fault tree to the upper fault tree.

3.5
FT driven Markov process
Markov process modelled by a FT made of primary events modelled by individual sub-Markov models behaving independently from each other

Note 1 to entry: The underlying logic of a FT allows to combine the individual unavailabilities of the primary events to obtain the system unavailability. When the primary events are modelled by small individual Markov processes (e.g. with less than 10 states) the FT is equivalent to the Markov process related to the system which may encompass millions of states. This is the basis for most of the probabilistic calculations achieved with FTs. Such Markov process built through the use of the FT as guideline is called "FT driven Markov process".

Note 2 to entry: The independent Markov process is developed in [5].

3.6
dynamic FT
DFT
fault tree implementing temporal interactions and where the assumption of independency between the primary events is not fulfilled

Note 1 to entry: The primary events of a DFT can have interactions with elements external to the FT itself

IHS Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Note 2 to entry: the symbols for dynamic FTs are given in Table 5.

3.7
non-coherent FT
fault tree modelling a non-monotonic logical function

Note 1 to entry: A non-coherent FT is a FT where the primary events may appear both in direct and complementary states (see Table 3). In this case, some of the cut sets (see definition 3.35) can have some primary events in complementary state. The concepts of minimal tie and cut sets (see 3.33 and 3.35) are no longer valid and have to be replaced by the concept of prime implicants.

Note 2 to entry: In a non-coherent FT, a failure path can become a success path by adding another fault or a success path can become a failure path by removing a fault. This is why it is named "non-coherent".

3.8
item
subject being considered

Note 1 to entry: In this international standard the word “item” covers mainly the system modelled by the FT and the “blocks” in the RBD.

[SOURCE: IEC 60050-192:2015, 192-01-01, modified — Notes to entry have been deleted, Note 1 to entry: has been added]

3.9
outcome
result of an action or other input; a consequence of a cause

Note 1 to entry: 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 to entry: Within a fault tree, an outcome may also be an input to an intermediate event, or it can be the top event.

3.10
event
occurrence of a condition or an action

3.11
top event
root
final event
top outcome
outcome that is investigated by building the fault tree

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

Note 2 to entry: the various names are synonymous but reflect several points of view. "Top event" or "top outcome" indicates that they are drafted at the top of the FT, "root" indicates that this is the starting point of the analysis and "final event" indicates that it is the result of the logical function embedded into the FT.

Note 3 to entry: the occurrence of the top event leads to the fault of the analysed item.

Note 4 to entry: the symbol for the top event is given in Table 3, line 2.

3.12
gate
logical gate
symbol which is used to establish symbolic link between the output event of a logical operator and the corresponding inputs of this logical operator

Note 1 to entry A given gate symbol reflects the type of logical relationship (e.g OR, AND, two out of three) required between the input events for the output event to occur.

AVA Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Note 2 to entry: the symbols for logic gates are given in Table 4.

3.13
Transfer gate
symbol used to split a large fault tree in smaller sub-fault trees

Note 1 to entry: the symbols for transfer gates are given in Table 4, lines 1 to 4.

3.14
primary event
leaf
event used as input of a fault tree

Note 1 to entry: The term leaf is used by analogy with a vegetal tree.

Note 2 to entry: In this standard, primary event can mean a basic event (3.16) 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). The various graphical forms of primary events are given in Table 3

Note 3 to entry: FTs and RBDs are dual approaches (see [3]). A fault tree primary event is generally equivalent to an RBD block in down state and a complementary primary event (see Table 3) to an RBD block in up state. These properties are used to transform a FT into an RBD and vice-versa.

Note 4 to entry: As the FT model is static, a primary event can represents the occurrence of a component failure mode (event) as well as the state (fault) reached when this failure mode has occurred. For example, a primary event labelled "Failure of pump P1" represents both the failure of the pump and the faulty state of the pump P1. This is why the failure modes included into a FT are described in terms of events (see definitions 3.11 and 3.16 to 3.21) when the approach is named "fault" tree analysis.

Note 5 to entry: the symbols for primary events are given in Table 3.

3.15
complementary primary event
Repeated and negated primary event

Note 1 to entry: A primary event is normally used in its direct form, e.g. $\overline{E}$, to describe an item fault but also in complementary form, e.g. $E = \text{NOT}(\overline{E})$ (see Table 3), to describe an item success state.

Note 2 to entry: the symbols for complementary events are given in Table 3, line 12.

3.16
basic event
primary event that cannot be further developed

Note 1 to entry: the symbol for basic events is given in Table 3, line 4.

3.17
intermediate event
event that is neither a top event nor a primary event

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

Note 2 to entry: the symbol for intermediate events is given in Table 3, line 3.

3.18
elementary event
undeveloped event
primary event that does not need to be developed in more detail

Note 1 to entry: It is not developed in the analysis for various possible reasons, such as lack of more detailed information or uselessness for the purpose of the study. It could be developed in more detail if it was needed in another analysis. An example of undeveloped event could be Commercial Off The Shelf Items (or COTS) failure.

Note 2 to entry: the symbol for elementary events is given in Table 3, line 5.

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

3.19
event to be developed
primary event to be analysed and developed in more detail to complete the fault tree

Note 1 to entry: This is a reminder for the analyst to identify the primary events needing to be analysed more in depth. They are normally replaced by more detailed sub-fault tree in the final version of the fault tree.

Note 2 to entry: the symbol for events to be developed is given in Table 3, line 6.

3.20
house event
primary event which is expected to occur

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

Note 2 to entry: the symbol for house events is given in Table 3, line 7.

3.21
condition event
conditional event
primary event defining a condition which is needed to validate an IF (see Table 4) logical gate

Note 1 to entry: in the context of a FT, a condition event has the same property as a basic event.

Note 2 to entry: the symbol for condition events is given in Table 3, line 9.

3.22
single failure
single point failure
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)

Note 1 to entry: a single point failure is a minimal cut set of order 1

3.23
common cause events
different primary events in a system or a fault tree that have the same cause for their occurrence

Note 1 to entry: An example of such an event would be shorting of ceramic capacitors due to flexing of the printed circuit board; thus, even though these might be different capacitors having different functions in their design, their shorting would have the same cause – the same input event.

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

3.24
common cause
cause of occurrence of several events

Note 1 to entry: 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.

3.25
repeated event
replicated event
primary event appearing more than once in a FT

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

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Note 2 to entry: The primary events related to repeated events can appear in the direct or complementary form. This is very useful to represent FTs related to a complex system or for representing FTs in the form of failure or success paths (see 8.2).

Note 3 to entry: the symbol for repeated events is given in Table 3 line 10, 11 and 12.

3.26
up state
available state
state of being able to perform as required

Note 1 to entry: The absence of necessary external resources may prevent operation, but do not affect the up state.

Note 2 to entry: "Up" state relates to availability of the item.

Note 3 to entry: An item may be considered to be in an up state for some functions and in a down state for others, concurrently.

Note 4 to entry: The adjectives up and "available" designate an item in an up state.

Note 5 to entry: Within the context of FTs, a complementary primary event (see Table 3) is assimilated to a up state of a component of the system under analysis.

[SOURCE: IEC 60050-192:2015, 192-02-01, modified — Note 5 to entry has been added]

3.27
up time
time interval for which the item is in an up state

[SOURCE: IEC 60050-192:2015, 192-02-02]

3.28
mean up time
MUT
expectation of the up time

[SOURCE: IEC 60050-192:2015, 192-08-09]

3.29
down state
unavailable state
state of being unable to perform as required, due to internal fault, or preventive maintenance

Note 1 to entry: "Down" state relates to unavailability of the item.

Note 2 to entry: The adjectives "down" or "unavailable" designate an item in a down state.

Note 3 to entry: Within the context of FTs, a primary event is assimilated to a down state of a component of the system under analysis.

[SOURCE: IEC 60050-192:2015, 192-02-20, modified — Note 3 to entry: has been added]

3.30
down time
time interval for which the item is in a down state

[SOURCE: IEC 60050-192:2015, 192-02-21, modified — Note 1 to entry has been deleted]

3.31
mean down time
MDT
expectation of the down time

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Note 1 to entry: This note only applies to the French language.

[SOURCE: IEC 60050-192:2015, 192-08-10]

3.32
success path
tie set
in and RBD [3], a set of blocks, with each block in the set being in the up state thus resulting in the RBD to be in the up state

Note 1 to entry: The name tie set is given by analogy with an electrical circuit: the blocks in up state constitute a closed (tied) circuit between the RBD input and the RBD output.

Note 2 to entry: In the context of FT a tie set is a set of primary events in the complementary form (i.e. corresponding to the blocks in up state) such as the modelled system is in up state.

[SOURCE IEC 61078:2016, modified — Note 2 to entry has been added]

3.33
minimal tie set
in and RBD [3], a tie set such as that any failure of one of the blocks in up state also fails the whole RBD

Note 1 to entry: In a minimal tie set, every block in up state, i.e. primary events in complementary form, is necessary to retain the modelled system in up state.

Note 2 to entry: The order of a minimal tie set is given by the number of blocks in the set in up states: order 1 comprises 1 block in up state, order 2 comprises 2 blocks in up state, etc.

[SOURCE IEC 61078:2016, modified]

3.34
failure path
cut set
group of events that, if all occur, would cause occurrence of the top event

Note 1 to entry: The name cut set is given by considering the equivalent RBD and by analogy with an electrical circuit (see [3]).

Note 2 to entry: in the context of fault tree the events are related to faults (i.e., down states), of components of the modelled system.

3.35
minimal failure path
minimal cut set
a minimal failure path such that the occurrence of every event is needed to cause the top event

Note 1 to entry: In a minimal cut set the non-occurrence of any one of the events in the set would prevent the occurrence of the top event. Therefore, minimal cut sets are the smallest sets of events causing the top event.

Note 3 to entry: The order of a minimal cut set is given by the number of primary events in the set: order 1 comprises 1 primary event, order 2 comprises 2 primary events, etc.

3.36
disjoint set of elements
set of Boolean elements whose intersections are empty

EXAMPLE If $(C_i^{\mathrm{d}})_{i=1,n}$ is a set of disjoint cut sets then $C_i^{\mathrm{d}} \cap C_j^{\mathrm{d}} = \Phi \quad \forall i \neq j$ and therefore, the probability $P(C_i^{\mathrm{d}} \cap C_j^{\mathrm{d}}) = 0 \quad \forall i \neq j$.

Note 1 to entry: The term "element" is used here in the general meaning used in the set theory, i.e. a member of a given collection of objects.

AVA Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Note 2 to entry: Disjoint elements are incompatible: when one is true, the other is false and vice versa. This describes mutual exclusiveness and, therefore, complete dependency between the elements.

[SOURCE IEC 61078:2016]

availability
<item> ability to be in up state

[SOURCE: IEC 60050-192:2015, 192-01-23, modified]

3.37
$A(t)$
instantaneous availability
point availability
<measure> probability of being in up state at a given instant t

[SOURCE: IEC 60050-192:2015, 192-08-01, modified]

3.38
$U(t)$
instantaneous unavailability
point unavailability
<measure> probability of being in down state at a given instant t

[SOURCE: IEC 60050-192:2015, 192-08-04, modified]

3.39
$A^{\mathrm{avg}}(t_1, t_2)$
mean availability
average availability
<measure> average value of the instantaneous availability over a given time interval $[t_1, t_2]$

[SOURCE: IEC 60050-192:2015, 192-08-05, modified — Note 1 to entry has been deleted]

3.40
$U^{\mathrm{avg}}(t_1, t_2)$
mean unavailability
average unavailability
<measure> average value of the instantaneous unavailability over a given time interval (t_1, t_2)

Note 1 to entry: The mean unavailability of a safety instrumented system (see IEC 61508 [14]) is also called "average probability of failure on demand" (Acronym: $\mathrm{PFD}_{\mathrm{avg}}$).

[SOURCE: IEC 60050-192:2015, 192-08-06, modified — Note 1 to entry has been replaced]

3.41
A^{st}
A^{as}
steady state availability
asymptotic availability
limit, if it exists, of the instantaneous availability, when the time tends to infinity

Note 1 to entry: Under certain conditions, the steady state availability may be expressed as the quotient MUT/(MUT+MDT). See IEC 61703.

[SOURCE: IEC 60050-192:2015, 192-08-07, modified — Note 1 to entry modified]

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

3.42
reliability
<item> ability to perform as required, without failure, for a given time interval, under given conditions

[SOURCE: IEC 60050-192:2015, 192-01-24, modified — Notes to entry have been deleted]

3.43
$R(t_1, t_2)$
$R(t)$
reliability
<measure> probability of performing as required for time interval $[t_1, t_2]$, under given conditions

Note 1 to entry: The reliability $R(t)$ is the reliability for the time interval $[0, t]$.

[SOURCE: IEC 60050-192:2015, 192-01-24, modified — Notes to entry have been deleted, Note 1 to entry has been added]

3.44
$F(t_1, t_2)$
$F(t)$
unreliability
<measure> probability of not performing as required for time interval $[t_1, t_2]$, under given conditions

Note 1 to entry: The unreliability $F(t)$ is the unreliability for the time interval $[0, t]$.

Note 2 to entry: The unreliability is the complement to 1 of the reliability: $F(t)$=1-R(t).

3.45
$\lambda(t)$
instantaneous failure rate
failure rate
limit, if it exists, of the quotient of the conditional probability that an item goes from up state to down state within time interval $[t, t + \Delta t]$, and Δt, when Δt tends to zero, given that it has not been in down state within time interval $[0, t]$

Note 1 to entry: The definition has been adapted from IEC 60050-192 to also cover repairable items:

- if the item has no internal built-in redundancy, the failure rate is identical to what it would be if it was not repairable;
- if the item has built-in internal redundancy it can remain in up state when some redundant parts are failed. Therefore, those failures are repairable as long as the whole item has no transition to the down state due to a further part failure.

Note 2 to entry: The terms failure rate (3.45), conditional failure intensity (3.46) and unconditional failure intensity (3.47) seem similar but they differ by the conditional events used in their definitions. Even if these parameters can have close numerical values in particular cases, they behave in different ways and should not be confused with each other.

[SOURCE: IEC 60050-192:2015, 192-05-06, modified — Notes to entry have been replaced by new notes to entry]

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

3.46
$\lambda_v(t)$
instantaneous conditional failure intensity
conditional failure intensity
Vesely failure rate
limit, if it exists, of the quotient of the conditional probability that the failure of an item occurs within time interval $[t, t + \Delta t]$, and Δt, when Δt tends to zero, given that the item was in up state at time t and at time 0

Note 1 to entry: See Note 2 to entry of the failure rate definition (3.45).

3.47
$w(t)$
instantaneous unconditional failure intensity
unconditional failure intensity
failure frequency
limit, if it exists, of the quotient of the conditional probability that the failure of an item occurs within time interval $[t, t + \Delta t]$, and Δt, when Δt tends to zero, given that the item was in up state at time 0

Note 1 to entry: See Note 2 to entry of the failure rate definition (3.45).

Note 2 to entry: This parameter is equivalent to the failure intensity defined in IEC 60050-192:2015, 192-05-08. The name has been modified to distinguish it from the term, conditional failure intensity (3.46).

3.48
$w^{\mathbf{avg}}(0,T)$
average failure frequency
number of failures per unit of time of an item averaged over a given period of time T

Note 1 to entry: If N is the number of failures of the item over [0, T] then the average failure frequency over this period of time is calculated as $w^{avg}(0,T)=N/T$.

Note 2 to entry: If m is the mean elapsed time between failures (METBF see IEC 61703) of an item then the average number of failures occurring over [0, T] is $N \approx T/m$. Therefore $w^{avg}(0,T) = N/T \approx 1/m$.

Note 3 to entry: Mathematically speaking, $w^{avg}(0,T)$ is the average of $w(t)$ over [0, T]. Then $w^{avg}(0,T) = \frac{1}{T}\int_0^T w(\tau)d\tau$.

[SOURCE IEC 61078:2016 – Note 2 to entry modified]

3.49
mean time between failure
mean elapsed time between failures
METBF
expectation of the time which elapses between successive failures

[SOURCE IEC 61703]

3.50
mean operating time to failure
MTTF
expectation of operating time to failure

Note 1 to entry: In the case of non-repairable items with an exponential distribution of times to failure (thus a constant failure rate) the MTTF is numerically equal to the reciprocal of the failure rate. This is also true for repairable items if, after restoration, they can be considered to be “as-good-as-new”.

[SOURCE IEC 60050-192, 192-05-11, modified — Note 2 to entry has been deleted]

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

3.51
systemic dependency
holistic dependency
dependency between the parts of a system which are related to the system considered as a whole

EXAMPLE 1 A single repair team constitutes a systemic dependency between repairable items: when an item fails it can be repaired only if the repair team is not busy due to the repair of another item belonging to the system.

EXAMPLE 2 The reliability $R(t)$ of a system can be expressed as the probability for the system to be in up state at time t, provided it has never been in down state over the interval [0, t]. Therefore only the sequences of events which do not lead to the down state over [0, t] can be retained and the sequences of events which include a sucession "up state" →"down state"→"up state" have to be excluded from the calculations. This implies that, with regards to the calculation of $R(t)$, an item going to the down state is repairable only if the system remains in up state during the repair of the item. Therefore, with regards to the calculation of $R(t)$, the items are repairable or not depending on the states of the other blocks and this constitutes systemic dependencies between all blocks of the RBD modelling the system.

Note 1 to entry: A systemic dependency cannot be described as a local property of the individual items of the system.

[SOURCE IEC 61078:2016]

3.52
binary decision diagram
BDD
compact decision tree based on the Shannon decomposition of a Boolean expression

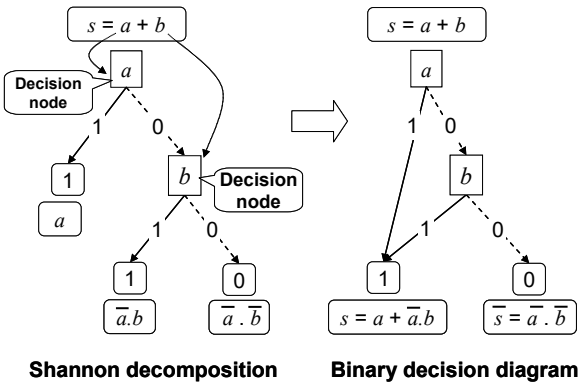


Figure 1 – Shannon decomposition of a simple Boolean expression and resulting BDD

Note 1 to entry: Figure 1 illustrates how the simple Boolean expression $s = a + b$ can be transformed into a decision tree by using the Shannon decomposition and then how the corresponding BDD is obtained by gathering the paths giving the same value (0 or 1) of the Boolean expression.

Note 2 to entry: Mathematically speaking, BDDs are rooted, directed acyclic graphs. This is a data structure expressing Boolean expressions as unions of disjointed terms. This, in turn, leads to exact probabilistic calculations. This is the state of the art with regards to probabilistic calculation on Boolean related models. More details about BDDs can be found in references [7] and [8].

[SOURCE IEC 61078:2016 – Note 2 to entry modified]

4 Symbols and abbreviated terms

Table 1 – Acronyms used in IEC 61025

Abbreviation/Acronym	Meaning
BDD	Binary decision diagram.
CCA	Cause consequence analysis.

AVA Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Abbreviation/Acronym	Meaning
CCF	Common cause failure.
cdf	Cumulative distribution function.
DFT	Dynamic Fault tree.
ETA	Event tree analysis.
FMEA	Failure modes and effects analysis.
FT, FTA	Fault tree, fault tree analysis.
HAZOP	Hazard and operability study.
MDT	Mean down time.
METBF	Mean elapsed time between failures.
MTTF	Mean operating time to failure.
MTTR	Mean time to restoration.
MUT	Mean up time.
PAND	Priority AND gate.
pdf	Probability density function.
PFD_{avg}	Average of the probability of failure on demand (mean unavailability).
PFH	Average failure frequency (Probability of failure per hour).
PN	Petri net.
RBD	Reliability block diagram.
SEQ	Sequential gate.
STA	Success tree analysis.

Table 2 – Symbols used in IEC 61025

Symbol	Meaning
S	Letter "S" reserved for the system modelled by a FT.
$X \in (A, B, C, ..), X \neq S$	Item whose failure mode is used as primary event into a fault tree (see NOTE 1). The letter S is reserved for the system.
$S, \overline{S}$	System S in up state, in down state. $\overline{S}$ is the top event of the fault tree.
$s = \{S, \overline{S}\}$	Boolean variable indicating the state of system S.
$X, \overline{X}$	Item X in up state, item X in down state. $\overline{X}$ is a primary event of the fault tree. See NOTE 1.
$x = \{X, \overline{X}\}$	Boolean variable indicating the state of item X.
$(\Pi_i), (C_i)$	Minimal success paths (minimal tie sets), minimal failure paths (minimal cut sets). See 3.33 and 3.35
$(\Pi_i^{\mathrm{d}}), (C_i^{\mathrm{d}})$	Disjoint success paths (disjoint tie sets), disjoint failure paths (disjoint cut sets).
$P(.)$	Probability function.
$P_S = P(\text{S in "up" state})$	Constant (time independent) probability that the system S is in the up state S, i.e., constant probability that the top event is not achieved.
$P_{\overline{S}} = P(\text{S in "down" state})$	Constant (time independent) probability that the system S is in the down state $\overline{S}$, i.e., constant probability that the top event is achieved.

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Symbol	Meaning
$P_X = P(\text{X in "up" state})$	Constant (time independent) probability that the item X is in the up state X.
$P_{\overline{X}} = P(\text{X in "down" state})$	Constant (time independent) probability that the item X is in the down state $\overline{X}$, i.e., probability of a fault tree primary event related to the failure of X.
$P_{\overline{S}\|X} = P(\text{S in "down" state} \mid \text{X in "up" state})$	Conditional probability that the system S is in the down state $\overline{S}$ given that block X is in the up state X: conditional probability that the top event is achieved given the item X is not faulty.
$P_{\overline{S}\|\overline{X}} = P(\text{S in "down" state} \mid \text{X in "down" state})$	Conditional probability that the system S is in the down state $\overline{S}$ given that block X is in the up state $\overline{X}$: conditional probability that the top event is achieved given the item X is faulty.
$P_S(t)$	Time dependent probabilities that the system S is in the up state S, i.e., time dependent probability that the top event is not achieved at time t.
$P_{\overline{S}}(t)$	Time dependent probabilities that the system S is in the down state $\overline{S}$, i.e., time dependent probability that the top event is achieved at time t.
$P_X(t)$	Time dependent probability that the item X is in the up state X.
$P_{\overline{X}}(t)$	Time dependent probability that the item X is in the down state $\overline{X}$, i.e., time dependent probability of a fault tree primary event related to the failure of X.
$P\ (OK,t)$	Probability of state OK at time t.
t, t_i	Current instant of time.
T, T_i	Time duration.
$[t_1,t_2]$, $[0,T] \equiv [t_1 = 0,\ t_2 = 0 + T]$	Time interval, $t_1 < t_2$
$A_S(t) = P(\text{S in "up" state at time } t) \equiv P_S(t)$	Availability of the system S at time t, i.e., probability that the top event is not achieved at time t.
$A_S^{avg}(t_1,t_2)$, $A_S^{avg}(0,T)$, $A_S^{avg}(T)$	Average availability of the system S over the time interval $[t_1, t_2]$ or $[0,T]$, i.e., average probability that the top event is not achieved over the time interval $[t_1, t_2]$ or $[0,T]$.
A_S^{avg}, A_S^{st}, A_S^{as}	Average availability of the system S over[0, ∝], steady state availability and asymptotic availability, i.e., average probability over [0, ∝], steady state probability and asymptotic probability that the top event is not achieved.
$A_X(t) = P(\text{X in "up" state at time } t) \equiv P_X(t)$	Availability of the item X at time t, i.e., probability that the item X is in up state at time t.
$A_i(t) = A_{X_i}(t) = P(\text{X}_i \text{ in "up" state at time } t)$	Availability of the item X_i at time t, i.e., probability that the item X_i is in up state at time t.
$A_X^{avg}(t_1,t_2)$, $A_X^{avg}(0,T)$, $A_X^{avg}(T)$	Average availability of the item X over the time interval $[t_1, t_2]$ or $[0,T]$.
A_X^{avg}, A_X^{st}, A_X^{as}	Average availability of the item X over [0, ∝], steady state availability and asymptotic availability.
$U_S(t) = P(\text{S in "down" state at time } t) \equiv P_{\overline{S}}(t)$	Unavailability of the whole system S at time t, i.e., probability that the top event is achieved at time t.
$U_S^{avg}(t_1,t_2), U_S^{avg}(0,T), U_S^{avg}(T)$	Average unavailability of the system S over the time interval $[t_1, t_2]$ or $[0,T]$, i.e., average probability that the top event is achieved over the time interval $[t_1, t_2]$ or $[0,T]$.

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Symbol	Meaning
$U_S^{avg}, U_S^{st}, U_S^{as}$	Average unavailability of the system S over [0, ∝], steady state unavailability and asymptotic unavailability, i.e., average probability over [0, ∝], steady state probability and asymptotic probability that the top event is achieved.
$U_X(t) = P(\text{X in "down" state at time } t) \equiv P_{\overline{X}}(t)$	Unavailability of the item X at time t, i.e., probability that the item X is in down state at time t. This is the probability of the corresponding primary event.
$U_i(t) = U_{X_i}(t)$	Unavailability of the item X_i at time t.
$U_X^{avg}(t_1,t_2), U_X^{avg}(0,T), U_X^{avg}(T)$	Average unavailability of the item X over the time interval [t_1, t_2] or [0,T].
$U_X^{avg}, U_X^{st}, U_X^{as}$	Average unavailability of the item X over [0, ∝], steady state unavailability and asymptotic unavailability.
$R_S(t) = P(\text{S in "up" state all over } [0,t])$	Reliability of the system S over [0, t] , i.e., probability that the top event does not occur over [0, t].
$F_S(t) = 1 - R_S(t)$	Unreliability of the overall system S over [0, t] (failure distribution of the system S), i.e., probability of occurrence of the top event before t.
$F_\Lambda(\lambda) = P(\Lambda \le \lambda)$	Cumulative distribution function (cdf) of the random variable Λ.
$f_S(t)$	Time to failure density functions of system S, i.e., density of the probability of occurrence of the top event.
$R_X(t) = P(\text{X in "up" state all over } [0,t])$	Reliability of the item X over [0, t].
$F_X(t) = 1 - R_X(t)$	Unreliability of the item X over [0, t] (failure distribution of block X).
$f_X(t)$	Time to failure density functions of the item X.
γ	Probability of failure due to a demand.
$\Lambda_S, \Lambda_S(t)$	Constant and time dependent failure rates of the system S, i.e., related to the occurrence of the top event.
$\Lambda_{VS}, \Lambda_{VS}(t)$	Conditional failure intensity (Vesely failure rate) of the overall system, i.e., related to the occurrence of the top event.
Λ, Λ_K	Failure rate as a random variable.
$(\lambda_K^i)_{i=1,N}$	N random values of the random variable Λ_K.
$w_S(t)$,	Unconditional failure intensity (failure frequency) of the system S, at time t, i.e., related to the occurrence of the top event.
$W_S(0,T), W_S(T)$	Expected number of failures of the system S over [0, T], i.e., expected number of occurrences of the top event.
$w_S^{avg}(0,T), w_S^{avg}(T)$	Average unconditional failure intensity (average failure frequency) of the system S over [0, T], i.e., related to the occurrence of the top event.
$\lambda_X, \lambda_X(t)$	Constant and time dependent failure rates of the item X.
$w_X(t)$	Unconditional failure intensity (failure frequencies) of the item X, at time t, i.e., related to the occurrence of the primary event $\overline{X}$.
$W_X(0,T), W_X(T)$	Expected number of failures of the item X over [0, T], i.e., expected number of occurrences of the primary event $\overline{X}$.
$w_X^{avg}(0,T), w_X^{avg}(T)$	Average unconditional failure intensity (average failure frequency) of the item X over [0, T], i.e., related to the occurrence of the primary event $\overline{X}$.
$\mu_X, \mu_X(t)$	Constant or time-dependent repair rates of the item X.

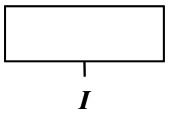
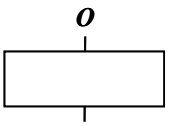
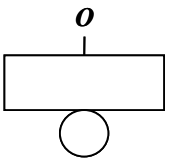
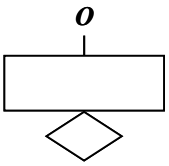
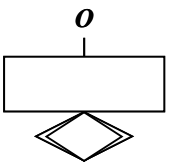
AVA Documents Document Sharing Hub

Full document details: 18/30378905 DC

Symbol	Meaning
$\binom{n}{r}$	Number of ways of selecting r blocks from n blocks without order: $\binom{n}{r} = \frac{n!}{r!(n-r)!}$.
"0", "1"	Symbols used in truth tables, Karnaugh map, Shannon decomposition and binary decision diagrams to denote down (failure) states and up (success) states of blocks or of systems.
$\cap, \bullet, \cdot$	Boolean operators denoting AND logic, e.g. $a \cap b \equiv a \bullet b \equiv a \cdot b$ (intersection).
$\cup, +$	Boolean operators denoting OR logic, e.g. $a \cup b, a + b$ (union).
Φ, Ω	"Impossible" event and "certain" events.
NOTE 1 To simplify the formulae only one failure mode is considered for a given item X. Nevertheless, when an item X has several failure modes the notations $X^{(n)}, \overline{X}^{(n)}$ and $x^{(n)}$ can be used to note that the item X is in "up" or "down" state with regards to a given failure mode n.	

826

827 **Table 3 – Graphical representation of Fault trees: events**

Graphical representation	Meaning
I ***O***	**1. Input (*I*) and output (*O*)** Such indications are used for convenience. They are not mandatory, but can be useful to show how the output at a given level becomes an input for the level just above.
	**2. Top event**, unwanted event, root of the tree. It is equal to the input ***I*** and have no output
	**3. Intermediate event**. The output ***O*** is equal to the input ***I***.
Primary events	
	**4. Basic event.** The output ***O*** is true when the event has happened. It generally models a component fault which cannot be analysed more in depth.
	**5. Elementary event.** The output ***O*** is true when the event has happened. It generally models a component fault which could be analysed in more details but for which it is not useful with regards to the performed study.
	**6. Event to be developed.** The output ***O*** is true when the event has happened. It generally models a component fault which must be developed in more detail before completing the study.

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

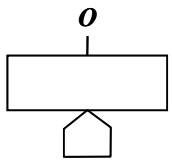
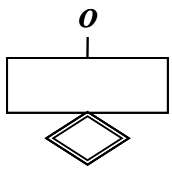
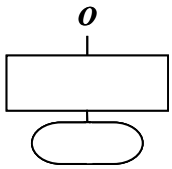
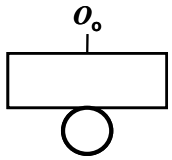
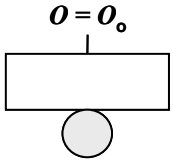
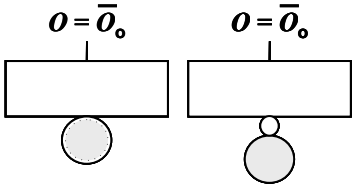
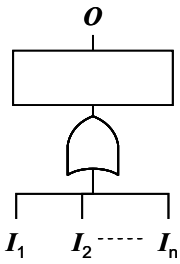
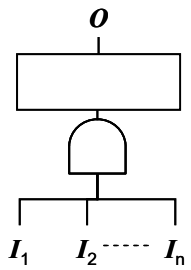
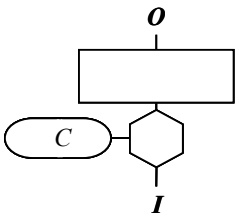
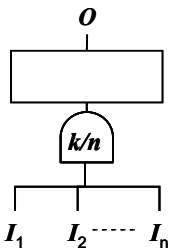
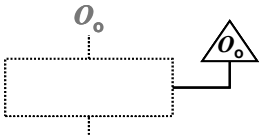
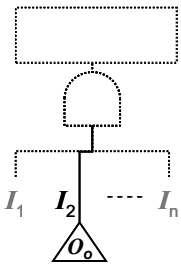
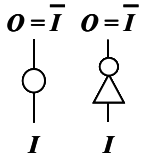
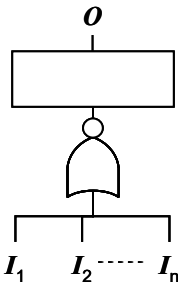
Graphical representation	Meaning
	**7. House event.** Event which has occurred or will occur with certainty. The output O is true.
	**8. Dormant failure.** Such failure is not revealed when it happens but could, perhaps, be detected by additional tests, inspection or analysis. The output O is true when the event has happened.
	**9. Condition.** Event that is a condition of occurrence of another event. The output O is true when the event has happened. Conditions are used with IF and ITE logic gates.
Repeated events	
	**10. Repeated event.** Original event which is used in several places of a FT. The output O_o is true when the event has happened.
	**11. Direct repeated event.** Identical copy of a repeated event. The output O is true when the original event has happened: $O = O_o$.
	**12. Complementary repeated event.** Inverted copy of a repeated event. The output O is true when the original event has not happened: $O = \overline{O}_o$.

Table 4 – Graphical representation of Fault trees: logic gates

Graphical representation	Meaning
Static logic gates	
	**1. OR gate**. The output is true when one of input is true: $O = I_1 + I_2 + ... + I_n$ where "+" is the logical operator "OR".

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Graphical representation	Meaning
	**2. AND gate**. The output is true when all of inputs are true: $O = I_1 \cdot I_2 \cdot .... \cdot I_n$ where "·" is the logical operator "AND"
	**3. IF gate**. The output is true when the condition C and the input I are true. It is equivalent to an AND gate: $O = C \cdot I$ It is also called inhibition gate.
	**4. Majority vote *k/n* gate**. The output O is true when k of the inputs (I_1, I_2, ..., I_n) about n are true. Note: It is important to make the difference between the "success" majority vote logics implemented in RBDs and the "failure" majority vote logics implemented in fault trees. Generally the context (RBD or fault tree) is sufficient to show the difference. The relationship is the following: $(k/n)_{Fail.} \equiv ([n-k+1]/n)_{Suc.}$
	**5. Transfer gate OUT**. The output O_o is used in one or several places of the FT.
	**6. Transfer gate IN**. The output O_o of the transfer gate OUT is used as input of a logical gate. Transfer gate is useful to: – split large FTs into several smaller parts (sub-trees); – transfer the output at one place in a FT to another place in the FT.
Gates using the NOT operator	
	**7. NOT gate.** The output is the complementary of the input. $O = \bar{I}$
	**8. NOR gate.** The output is true when the output of the OR gate is false: $O = \overline{I_1 + I_2 + ... + I_n} = \bar{I}_1 \cdot \bar{I}_2 \cdot .... \cdot \bar{I}_n$

AVA Documents
Document Sharing Hub
Full document details: 18/30378905 DC

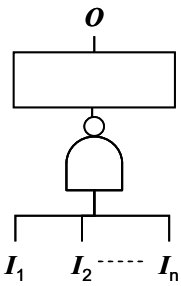
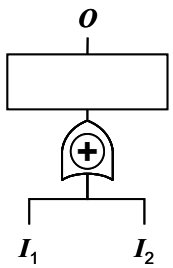
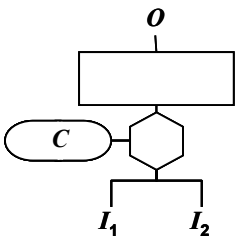
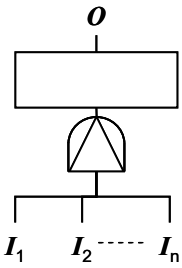
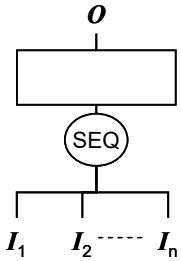
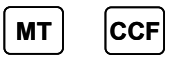
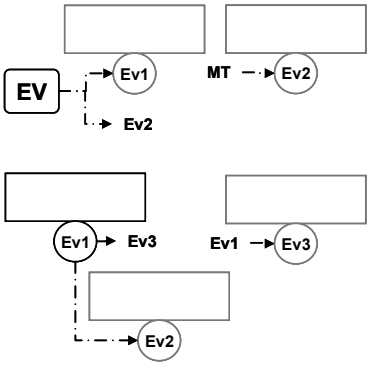
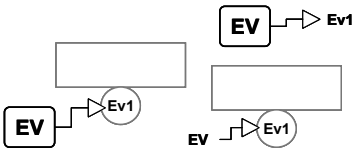
Graphical representation	Meaning
	**10. NAND gate**. The output is true when the output of the AND gate is false: $O = \overline{I_1 \cdot I_2 \cdot .... \cdot I_n} = \bar{I}_1 + \bar{I}_2 + ... + \bar{I}_n$
	**11. XOR gate**. The output is true if event I_1 is true, or event I_2 is true but not both: $O = I_1 \cdot \bar{I}_2 + \bar{I}_1 \cdot I_2$
	**12. ITE** (IF, THEN ELSE) **gate**. It is an extension of the classical IF gate. If the condition is true then the output O equal I_1 else it equals I_2: $O = I_1 \cdot C + I_2 \cdot \overline{C}$

Table 5 – Graphical representation of FTs: dynamic gates and functional dependencies

Graphical representation	Meaning
	**1. PAND gate**. The output O goes to true when the inputs go to true in the order I_1, then I_2, then I_3, ... then I_n. The inputs I_1, I_2, I_3, ... I_n behave independently from each other.
	**2. SEQ gate**. Like for the PAND gate the output O goes to true when the inputs go to true in the order I_1, then I_2, then I_3, ... then I_n. However, the inputs do not behave independently from each others: I_n cannot go to true if I_{n-1} is not already true, I_{n-1} cannot go to true if I_{n-2} is not already true, etc., I_2 cannot go to true if I_1 is not already true.
	**3. External event.** This is used for dynamic FTs to model external element interacting with one or several parts of the FT. For example common cause failures (CCF) or number of maintenance teams (MT).

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

Graphical representation	Meaning
	**4. Functional dependency.** Functional dependencies: the state of Ev1 and Ev2 depend on the event EV. This event may be external or internal to the FT. This symbol reminds that a dependency exists but the type of dependency may be diverse and has to be described somewhere else
	**5. Complete functional dependency.** Complete functional dependency: when the event Ev occurs, then Ev1 becomes true. This event may be external or internal to the FT. It plays the role of trigger.

5 General considerations

5.1 Fault tree within the dependability framework

Several analytical methods of dependability analysis are available, of which fault tree analysis (FTA) is one. Fault trees can be split into two categories:

- Basic fault trees which implements only static logical gates (see Table 4).
- Extended fault trees which implements also dynamic gates (see Table 5).

The advantages and disadvantages of each method and their respective products, required data, complexity of analysis and other factors identified in this standard should be examined by the analyst before selecting the FTA for undertaking a dependability study.

The first criterion to select FTA is its top-down (i.e. effect to cause) approach for building the model. It is a unique feature in the dependability field which is very powerful to analyse systems in depth and step by step. From this point of view, FTA is more effective than RBDs [3] , Markov [5] or Petri net approaches [6].

NOTE 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. Success tree analysis (STA) can be performed in the same way as fault tree analysis.

The second criterion is its 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". Even when the FT is large, this form can be clearly understood, qualitatively 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 dependability characteristics of the system, 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).

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

The third criterion is that basic FT, embeds the logical function linking the top event to the primary events. When the primary events behave independently from each other, Boolean calculations can be used to identify the combinations of events (cut sets) leading to the top event. This allows to refine the qualitative analysis and in conjunction with probabilities or descriptive likelihood of occurrence (e.g., “highly probable”, “very probable” “medium probability”, “remote probability”, etc.) semi-quantitative FTAs (see 9.2) may be undertaken to investigate causes of potential unfavourable outcomes.

The fourth criterion is that, when probability parameters are available for the primary events, calculations of dependability measures (probability of failure, unavailability, failure frequency or, with approximation, unreliability) can be performed by using FTs, see Clauses 9, 10 and 11). Such quantitative FTA is very useful in reliability analysis of a product or a system in its development.

For basic FTs, the first limitation is due to the Boolean underlying properties (i.e., the use of random variables with only two states and the static representation). The second limitation is linked with the combinatorial explosion of the minimal cut sets which can occur with large systems with complex logic but, nowadays, this is not really a problem when binary decision diagrams (BDD) are implemented. The third limitation comes from to the calculation of the unreliability $F_S(t)$ of the modelled system when it comprises repaired components, but approximations are generally available.

Extended FTs overcome to some extent the limitations of basic fault trees and they can be used for qualitative analysis of systems with complex interactions between sub-systems including software/hardware interactions. But, for quantitative analysis, other modelling techniques such as Markov [5], Monte Carlo simulation based, for example, on dynamic FTs or Petri net techniques [6], may be more suitable.

From the probabilistic calculations point of view, the mathematical background, the advantages and the limitations of FTA are the same as these of RBDs [3].

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 dependability 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 and when a system is repairable, for identifying possible system availability improvements;
– analysis and comparison of various design alternatives to improve system dependability;
– 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);
– search for an event or combinations of events (minimal cut sets) which are the most likely to cause the top event to occur;
– calculation of the probability of failure of a non-repaired system or the unavailability, failure frequency, Vesely failure rate and unreliability (with approximation) of a repaired system represented by a fault tree, from its components probability of failure, or unavailabilities and failure frequencies;
– assessment of the impact of the occurrence of a primary event on the probability of the top event (importance factor, see Annex D);

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

NOTE For basic fault trees the assumption to make probabilistic calculations with fault trees is that all the primary events behave independently from each others. This means, in particular, that eventual repairs are independent of each other.

5.3 Applications

FTA is particularly suited to the analysis of systems comprising several 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, safety systems, chemical, oil and gas systems and other industrial processes, railway systems, home entertainment systems, medical systems, computer systems, etc. FT analysis is also of particular value when applied to systems comprising various component types (mechanical, electronic and software components), which cannot be easily modelled with other techniques.

NOTE When the subsystems are independent and the outcome of a combination of events does not depend on the order of appearance, then basic fault trees can be used. Otherwise extended fault trees are more suitable.

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 dependability measures, identify the major contributors to these measures 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. 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. Then, early efforts would 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.

6 Fault tree analysis development

6.1 Simple example to help the clause understanding

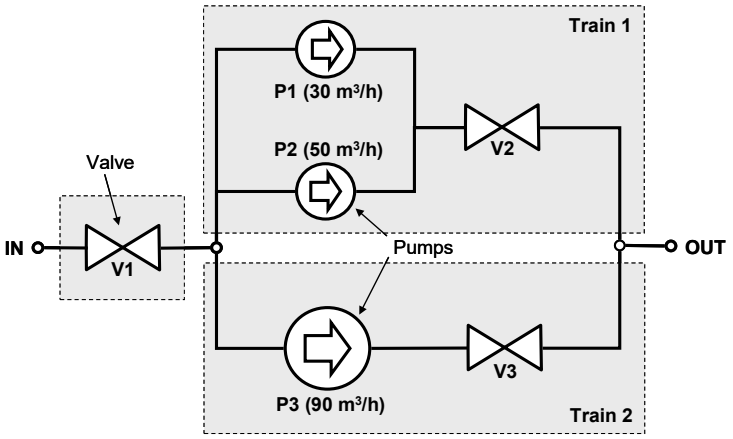


Figure 2 – Simple pumping system

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

The simple pumping system presented in Figure 2 aims to be used to clarify the meaning of the clauses developed hereafter in the standard. It is made of two pumping trains in series with a valve V1. The train 1 comprises two small pumps (flow rate capacities of 30 and 50m^3/h) and a valve V2 in series; the train 2 comprises one big pump (flow rate capacity of 90m^3/h) and a valve V3 in series. The purpose is of this system is to provide a flow rate of at least 80m^3/h.

6.2 Steps of a FTA

In order to use the fault tree technique effectively as a method for system analysis, it should be in agreement with the general dependability analysis procedure. This consists of at least the following steps:

a) definition of the scope of the analysis;

b) functioning analysis (i.e. familiarization with the design, functions and operation of the system) ;

c) dysfunctioning analysis:

- risk identification (i.e. identification and definition of relevant top events);
- system modelling (i.e. choosing FTA)
- gathering operational and dependability data
- qualitative analysis (i.e. analysis of the FT logic)
- quantitative analysis (i.e. performing probabilistic calculations)

d) assessment of dependability improvements and decisions about trade-offs

e) reporting on results of the analysis, conclusions.

There are often multiple objectives in the analysis which can be related, for example, to safety or dependability (production systems). Therefore, when performing FTA the step a) should be cautiously performed as all the remainder of the analysis depends on its relevance. Information needed to undertake this step is described in 6.3. The scope of analysis defines the events or the failure modes that will be included in the fault tree. It 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. At this step, the level of detail of the analysis and the boundaries (i.e., what is included and what is excluded from that system – internal connections, mechanical enclosures, etc. – should be specified.

For the example in Figure 2 the scope of the study can be related to the ability of the pumping system to achieve, at least, a flow rate of 80m^3/h from the input to the output of the system by taking into account the possible failures of the valves and pumps.

The step b) is very important as, before trying to analyse how a system can fail it is of utmost importance to have previously understood how it works. This is why a detailed knowledge about the design features and operation of the system is required. 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 system functionality and, thus, the analytical results would become meaningless. 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.

For the example in Figure 2 the functioning analysis consist in identifying which components have to be in up state for the system achieving a flow rate of at least 80m^3/h. This can be done if the train 1 is running or the train 2 is running when valve V1 is open.

Detailed FMEA [9] or HAZOP [11] are useful at step b) to understand how each component participate to the system functioning. They are also useful to understand the impacts of the components failure modes and help to undertake the risk identification which is the first stage of step c) which is focused on the system failure. The risk identification leads to highlight

AVA Documents
Document Sharing Hub
Full document details: 18/30378905 DC

detrimental events needing further analysis: they are the potential top events of fault trees if the analysts choose FTA to model and analyse them.

For the example in Figure 2 the impact of each component failure mode can be easily identified by using FMEA: the spurious closure of V1 drop the flow to zero, the trip of P3 drops the flow rate of train 2 to zero, the failure of P1 drop the flow rate of train 1 to 50m^3/h, etc. At this stage it is important to consider the impact of power supply and command-control because this can be a source of common cause failures between components. For example, in case of electrical power supply failure the three pumps are likely to stop at the same time.

When FTA is selected and a given top event identified the aim is to model the system architecture and functionality, searching in a top-down manner for the potential failure modes and their causes that might produce the defined top event. The analyst building a FT has to be trained in FTA and other relevant reliability modelling techniques able to evaluate influences of potential failure modes and logically identify possible causes of abnormal product performance.

For the example in Figure 2 the top event can defined as "*flow rate dropping below 80m^3/h*"

The top event can be described as a fault in itself or as an event. It is the same for the FT primary events but this does not really matter as faults or events are handled as random variables with two values "true" and "false" in order to be used as inputs of logical gates (e.g., OR gate, AND gate). For example, according IEC 60050-192, the event "C failure" leads to the state "C faulty". Therefore if "C failure" is "true", that means that "C faulty" is also "true", and vice versa, if "C failure" is "false", that means that "C faulty" is "false". Therefore qualitative analysis can be performed within the Boolean or logical framework.

If a quantitative analysis is planned, it is necessary to gather the dependability data allowing to perform the numerical assessment of primary events probabilities (e.g., failure rates, probabilities of failure frequencies, etc.). The selection of the data to be used and numerical evaluation of the dependability measures are outside the scope of this standard. This should be based on data collection from field feedback established, e.g., on ISO 14224 [12] or IEC 60300-3-2 [13] standards.

For the example in Figure 2 this implies to assess the probability parameters (probabilities of failure, failure rates, repair rates, etc.) related to the valves and pumps failure modes which impede the performances of the pumping system: breakdown, spurious closure, plugging, leakage etc.

Performing a FTA is generally a recurrent task. When results are obtained they should be reviewed by the engineering team participating in the system design, by operators from the field or by experts for correctness and completeness. Improvements and trade-offs leading to design changes are often identified at this stage, step d). The corrective actions agreed upon must be documented to keep trace of what has been done, and followed up.

After some such round trips the results of the FTA converge and final conclusions can be drawn and reported, step e). These conclusions are related to, for example, the top contributors to the top event or the most probable scenarios causing the top event (weak points), the unavailability, failure frequency or the unreliability (with approximation) of the system under study. When used for safety instrumented system (see IEC 61508 [14]), PFDavg (average unavailability) and PFH (average failure frequency) can also be obtained.

NOTE 1 It is important to note that fault tree events are not confined solely to software or hardware failures, but can include other factors, e.g. human factors or actions and processes that are relevant to the top event.

NOTE 2 "Analysis concurrent with design" allows for early systems design change.

NOTE 3 Fault trees can be large, in which case FTA software may be needed to handle them. Software packages are 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

AVA Documents
Document Sharing Hub
Full document details: 18/30378905 DC

sufficiently different to suit the needs of a specific use. However before using a FTA software package, the analyst should make sure that he has understood how it works, especially for running the probabilistic calculations.

6.3 Required information to undertake a FTA

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 including process flow diagrams and piping & instrumentation design drawings, specifications, operating manuals, which give details of the equipment design, operation philosophy and maintenance policy. 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, spare parts policy and personnel involved. Specific information on environment, prescribed functions during each operational phase (installation, starting, normal operation, dismantlement), about procedures and intervention means in case of accident can also be required.

6.4 Identification and labelling in a fault tree

Each event in the fault tree shall be uniquely identified. Events should be labelled so that cross-reference from the fault tree to the corresponding design documentation can easily be made.

The top event of the fault tree is the undesirable outcome, which is the primary reason for undertaking the fault tree analysis. It should be noted that only a single top event may be associated with a given fault tree.

If several events in a fault tree all refer to different failure modes of the same item, then such events shall be labelled so as to enable them to be distinguished. At the same time it should be clear that they are a group of events related to the same item. Most of the software packages for the FTA will not allow the analyst to label two input events with the same name, thus forcing the analyst to consciously assign the same name to the repeated events and to common cause events.

If a particular event such as inability of a particular valve to close, occurs in several places in a tree, or if it occurs in several trees, all such occurrences shall bear the same label (using software, the same input event will be appended with its specific name to different places in the fault tree). However, events which are similar but which involve different items shall not bear the same identification.

A typical event code should contain information relating to the subsystem identification, for identification of a component and its failure mode (second bullet below).

Some examples from electronic circuit analysis are as follows:

Documents
Document Sharing Hub
Full document details: 18/30378905 DC

– "Short_C132", meaning that the fault condition of capacitor C132 is short-circuit;

– "Short_A_C135", where the letter A applies to all components of the analog subsystem in cases where there is repetition of the reference designators in other subsystems (e.g. a C135 exists in the processor subsystem);

– "Open_R34", meaning that the fault condition of the resistor R34 is open-circuit;

– "Low_Output_U2", meaning that the fault condition of the integrated circuit is low output.

A supplementary set of more specialized labels or names of events may be developed when required. However, it is important for the analyst to define and report those labels and names being used and ensure uniform and consistent use throughout a given fault tree analysis. This is particularly true if computer-aided techniques are to be used.

Consistency in labelling is even more important when a fault tree analysis software allows import of values for probability of occurrence of basic or primary events which are calculated in a spreadsheet based on bill of materials, components, components failure modes and their use profile. This may be the case when analysis is undertaken on a complex system. In this case, the labels – names for the basic and primary events – must be identical in both files (the spreadsheet and the fault tree analysis) so that the name matching allows import of probability of occurrence values to the corresponding events.

6.5 Report

The report of the fault tree analysis should include as a minimum the basic items listed below. Additional and supplementary information may be provided to increase clarity, especially in cases of complex systems analyses. A prescribed format is not proposed by this standard.

Basic items in the report should be as follows:

– objective and scope;

– system description: design description, system operation, detailed system boundaries definitions;

– assumptions: system design assumptions;

– operation, maintenance, test and inspection assumptions, reliability and availability modelling assumptions;

– analysing person/team with background and relevant expertise stated in the heading or in a separate section of the report: top event definition and criteria;

– references for basic events, undeveloped events and events analysed elsewhere, e.g. in different projects and justification for use of their probabilities (e.g., same stresses, same use profile, etc.);

– fault tree analysis:

  - data, symbols used
  - qualitative analysis based on minimal cut sets, where appropriate; common cause failures analysis, where appropriate,
  - semi-quantitative analysis based on minimal cut sets, where appropriate
  - quantitative analysis: unavailability, average unavailability (PFDavg), failure frequency, average failure frequency (PFH), Vesely failure rate and unreliability, where appropriate;

– synthesis of results, conclusions and recommendations.

Supplementary data items which may be included consist of

– system block or circuit diagrams;

– summary of reliability and maintainability data and sources used such as databases, information from the component manufacturers, filed information, etc.;

Documents
Document Sharing Hub

Full document details: 18/30378905 DC