



**SLOVENSKI STANDARD**  
**oSIST prEN IEC 61025:2023**  
**01-november-2023**

---

**Analiza drevesa okvar (FTA)**

Fault tree analysis (FTA)

Fehlzustandsbaumanalyse

Analyse par arbre de panne (AAP)

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

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

<https://standards.iteh.ai/catalog/standards/sist/30ac9e87-c897-4d24-98df-e966c3220647/osist-pren-iec-61025-2023>

**ICS:**

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

**oSIST prEN IEC 61025:2023**

**en**





## COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER:

**IEC 61025 ED3**

DATE OF CIRCULATION:

**2023-09-08**

CLOSING DATE FOR VOTING:

**2023-12-01**

SUPERSEDES DOCUMENTS:

**56/1916/CD, 56/1922A/CC**

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

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

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

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

TITLE:

**Fault tree analysis (FTA)**

PROPOSED STABILITY DATE: 2024

NOTE FROM TC/SC OFFICERS:

1	<b>CONTENTS</b>		
2			
3	FOREWORD.....		7
4	INTRODUCTION.....		9
5	1 Scope.....		10
6	2 Normative references .....		10
7	3 Terms and definitions .....		11
8	3.1 Definitions directly relating to a fault tree .....		11
9	3.2 Dependability related definitions .....		14
10	4 Symbols and abbreviated terms.....		17
11	5 General aspects of FTA.....		24
12	5.1 Fault tree description and structure.....		24
13	5.2 Objectives and purpose .....		25
14	5.3 Applications .....		26
15	5.4 Limitations .....		26
16	6 Development of an FT .....		27
17	6.1 Steps in performing an FTA .....		27
18	6.2 Defining objectives, scope and context .....		27
19	6.3 Information required for performing FTA .....		28
20	6.4 Understanding how the system works and potential failure modes .....		29
21	6.5 Identifying and specifying the top event .....		29
22	6.6 Developing the FT .....		30
23	6.6.1 Modelling the system.....		30
24	6.6.2 Identification and labelling.....		31
25	6.7 Qualitative and quantitative analysis .....		31
26	6.8 Assessment of results, sensitivity and uncertainty analysis .....		32
27	6.9 Report .....		33
28	7 Mathematical representation of logic gates .....		34
29	7.1 General.....		34
30	7.2 OR Gate .....		34
31	7.3 AND Gate .....		35
32	7.4 Voting gate .....		36
33	7.5 NOT, NOR and NAND gates .....		37
34	7.6 Subtrees and transfer symbols.....		37
35	8 Qualitative analysis .....		38
36	8.1 Identification of minimal cut sets of an FT .....		38
37	8.2 Qualitative analysis with minimal cut sets .....		40
38	8.3 Common cause failure analysis.....		40
39	9 Quantitative analysis .....		41
40	9.1 Constant probabilities .....		41
41	9.1.1 General .....		41
42	9.1.2 Use of cut sets .....		41
43	9.1.3 Probability of the top event using Sylvester-Poincaré formula .....		42
44	9.1.4 Quantitative analysis with disjointed terms.....		43
45	9.1.5 Importance factors.....		43
46	9.2 Analysis of FTs involving events with time-dependent probabilities .....		44

47	9.2.1	General .....	44
48	9.3	Boolean techniques for quantitative analysis of large models .....	46
49	9.4	Time dependent analysis for systems consisting of non-repaired components .....	47
50	9.4.1	Failure rates .....	47
51	9.4.2	Small sub trees related to non-repaired items .....	47
52	9.4.3	Preventive replacement strategies and MTTF .....	49
53	9.5	Time-dependent analysis for systems that include repaired components .....	49
54	9.5.1	General .....	49
55	9.5.2	Small sub trees related to repaired items .....	50
56	9.5.3	FTs involving failures of periodically tested components .....	51
57	9.5.4	Average and asymptotic unavailability calculations .....	52
58	9.5.5	Frequency calculations and METBF .....	53
59	9.5.6	Unreliability calculations .....	54
60	9.5.7	Composition of two independent items – Practical examples using rates .....	56
61	10	Extension of fault tree technique .....	57
62	10.1	XOR gates and non-coherent fault trees .....	57
63	10.1.1	Example of probabilistic calculation for a non-coherent fault tree .....	58
64	10.2	Dynamic fault trees .....	59
65	10.2.1	General .....	59
66	10.2.2	Local interactions .....	59
67	10.2.3	Systemic dynamic interactions .....	61
68	10.2.4	Graphical representations of dynamic interactions .....	61
69	10.2.5	Probabilistic calculations .....	64
70	Annex A (informative)	Relationship with other dependability and risk assessment techniques .....	66
71			
72	A.1	Reliability block diagrams .....	66
73	A.1.1	Introduction .....	66
74	A.1.2	Series structure .....	66
75	A.1.3	Parallel structure .....	67
76	A.1.4	Mix of series and parallel structures .....	67
77	A.2	Combination of FTA and failure modes and effects analysis (FMEA) .....	68
78	A.3	Combination of FTA and event tree analysis (ETA) or cause-consequence analysis (CCA) .....	68
79			
80	A.4	Combination of FTA and Markov analysis .....	70
81	Annex B (informative)	Automated fault tree construction .....	71
82	Annex C (informative)	Use of Monte Carlo analysis for analysing uncertainty .....	72
83	Annex D (informative)	Procedure for disjointing minimal cut sets .....	75
84	Annex E (informative)	Shannon decomposition and BDDs .....	77
85	E.1	Shannon decomposition .....	77
86	E.2	Binary decision diagram (BDD) .....	79
87	E.2.1	Building of BDDs .....	79
88	E.2.2	Minimal cut sets identification .....	79
89	E.2.3	Probabilistic calculations with BDDs .....	80
90	E.2.4	Conditional probability calculations with BDD .....	81
91	Annex F (informative)	Importance factors .....	83
92	F.1	General .....	83
93	F.2	Vesely-Fussell importance factor .....	83
94	F.3	Birnbaum importance factor or marginal importance factor .....	83

95	F.4	Lambert importance factor or critical importance factor .....	84
96	F.5	Diagnostic importance factor.....	85
97	F.6	Risk achievement worth .....	85
98	F.7	Risk reduction worth .....	85
99	F.8	Differential importance measure .....	85
100	F.9	Remarks about importance factors.....	86
101	Annex G (informative)	FT driven Petri nets .....	87
102	G.1	General.....	87
103	G.2	Example of sub-PN to be used within FT driven PN models .....	87
104	G.3	Evaluation of the DFT state.....	89
105	G.4	Availability, reliability, frequency and MTTF calculations .....	91
106	Annex H (informative)	Numerical examples.....	93
107	H.1	General.....	93
108	H.2	Typical series structures (OR gates) .....	93
109	H.2.1	Non-repaired components.....	93
110	H.2.2	Repaired components.....	94
111	H.3	Typical parallel structure (AND gate) .....	96
112	H.3.1	Non-repaired components.....	96
113	H.3.2	Repaired components.....	97
114	H.4	Series-parallel structures .....	98
115	H.5	Complex structures .....	99
116	H.5.1	Fault tree with a repeated event .....	99
117	H.5.2	Convergence to asymptotic values versus MRT .....	101
118	H.5.3	System with periodically tested components .....	101
119	H.6	Dynamic fault tree example.....	103
120	H.6.1	Comparison between analytical and Monte Carlo simulation results.....	103
121	H.6.2	Dynamic RBD example .....	104
122	Bibliography.....		107
123			
124	Figure 1–	Simple pumping system .....	29
125	Figure 2 –	Fault tree for system illustrated in Figure 1 .....	30
126	Figure 3 –	OR Gate.....	34
127	Figure 4 –	Venn diagram illustrating Union of 3 events .....	35
128	Figure 5 –	AND gate .....	35
129	Figure 6 –	Voting gate .....	36
130	Figure 7	Representation of equation (7) in an equivalent fault tree.....	36
131	Figure 8 –	Use of transfer symbols to split a large FT into smaller trees.....	38
132	Figure 9 –	Fault tree as in Figure 2 showing gate outputs .....	39
133	Figure 10 –	Simplified fault tree for system illustrated in Figure 1 .....	40
134	Figure 11 –	Principle of combining time dependent probabilities .....	44
135	Figure 12 –	Combining time dependent probabilities: example unavailability with	
136		periodically tested components.....	45
137	Figure 13 –	Example showing the relationship between a Markov process and a primary	
138		event for a non-repaired item.....	48
139	Figure 14 –	Example of dependent primary events gathered into a single primary event.....	48
140	Figure 15 –	State transition diagram for a simple repaired item.....	50
141	Figure 16 –	Standby redundancy .....	51

142	Figure 17 –Typical unavailability of a periodically tested component.....	51
143	Figure 18 –Average unavailability over $[0, T]$ .....	52
144	Figure 19 – $US_{avg}(0, t)$ for a system with periodically tested components .....	53
145	Figure 20 –FT and equivalent Markov process for reliability calculations.....	55
146	Figure 21 – Equivalence XOR gate with a combination of AND and OR gates.....	57
147	Figure 22 – Example of a non-coherent Fault tree and of ITE gate.....	58
148	Figure 23 – BDD equivalent to the example of Figure 22.....	59
149	Figure 24 – Symbol for external elements .....	60
150	Figure 25 – Dynamic interaction between CCF and primary events .....	61
151	Figure 26 –Two ways to indicate dynamic interactions between primary events .....	62
152	Figure 27 – Example of functional dependency due to a single repair team.....	62
153	Figure 28 – Implementation of a PAND gate .....	63
154	Figure 29 – Implementation of a SEQ gate.....	63
155	Figure 30 – CCF as a repeated event .....	64
156	Figure 31 – PAND gate modelled with a Markov process .....	65
157	Figure 32 – SEQ gate modelled with a Markov process.....	65
158	Figure A.1 – Series structure: equivalence between RBD and FT.....	66
159	Figure A.2 – Parallel structure: equivalence between RBD and FT.....	67
160	Figure A.3 – Example of mix between series and parallel structures .....	67
161	Figure A.4 – Analysis of a procedure by cause consequence diagram .....	69
162	Figure A.5 – Event tree equivalent to the cause consequence diagram in Figure A.4 .....	69
163	Figure A.6 Global FT related to Figures A.4 and A.5 .....	70
164	Figure C.1 – Example of distribution of a failure rate considered as a random variable .....	72
165	Figure C.2 – Principle of Monte Carlo simulation.....	72
166	Figure C.3 – Example of uncertainty handling by using Monte Carlo simulation .....	73
167	Figure C.4 – Results highlighting the impact of input parameters uncertainties .....	74
168	Figure D.1 – Simple FT for applying disjointing procedure .....	75
169	Figure E.1 – Shannon decomposition of a simple Boolean expression and resulting	
170	BDD.....	77
171	Figure E.2 – Shannon decomposition of a 2/4 logical structure .....	78
172	Figure E.3 – Shannon decomposition (reduced graph).....	78
173	Figure E.4 – Binary decision diagram related to the FT in Figure E.2.....	79
174	Figure E.5 – Minimal cut set identification.....	80
175	Figure E.6 – Probabilistic calculations from a BDD .....	81
176	Figure E.7 – Calculation of conditional probabilities using BDDs.....	82
177	Figure G.1 – Example of a sub-PN modelling a primary event.....	87
178	Figure G.2 – Example of a sub-PN modelling common cause failures .....	88
179	Figure G.3 – Example of DFT based on FT driven PN.....	89
180	Figure G.4 – Logical calculation of classical FT structures .....	89
181	Figure G.5 – Example of logical calculation for an 2/3 gate.....	90
182	Figure G.6 – Example of sub-PN modelling a PAND gate with 2 inputs .....	90
183	Figure G.7 – Example of the inhibition of a primary event .....	91
184	Figure G.8 – Sub-PN for availability, reliability and frequency calculations.....	92

185	Figure H.1 – Unavailability/unreliability of a typical non-repaired series structure.....	93
186	Figure H.2 – Failure rate and failure frequency/failure density related to Figure H.1.....	94
187	Figure H.3 – Equivalence of a non-repaired series structure to a single component .....	94
188	Figure H.4 – Unavailability/unreliability of a typical repaired series structure.....	95
189	Figure H.5 – Failure rate and failure frequency related to Figure H.4 .....	95
190	Figure H.6 – Unavailability/unreliability of a typical non-repaired parallel structure.....	96
191	Figure H.7 – Failure rate and failure frequency related to Figure H.6 .....	97
192	Figure H.8 – Unavailability/unreliability of a typical repaired parallel structure .....	97
193	Figure H.9 – Vesely failure rate and failure frequency related to Figure H.8 .....	98
194	Figure H.10 – Example of mixed series and parallel structures .....	99
195	Figure H.11 – Vesely failure rate and failure frequency related to Figure H.10 .....	99
196	Figure H.12 – FT with a repeated event .....	100
197	Figure H.14 – Failure rate and failure frequency related to Figure H.12. ....	100
198	Figure H.15 – Impact of the MRT on the convergence quickness .....	101
199	Figure H.16 – Typical safety instrumented system .....	102
200	Figure H.17 – Unavailabilities related to primary events of the SIS (Figure H.16).....	102
201	Figure H.18 – SIS unavailability and reliability .....	103
202	Figure H.19 – Vesely failure rate and failure frequency of the SIS (Figure H.16).....	103
203	Figure H.20 – Parallel-series system.....	103
204	Figure H.21 – Analytical versus Monte Carlo simulation results according to the	
205	number of simulations .....	104
206	Figure H.22 – Parallel-series system with common cause failures and single	
207	maintenance team .....	104
208	Figure H.23 – Impact of CCFs and limited number of repair teams – .....	104
209	Figure H.24 – Markov graphs modelling the impact of the number of repair teams – .....	105
210	Figure H.25 – Approximation for two redundant components.....	106
211		
212	Table 1 – Acronyms used in this document .....	17
213	Table 2 – Symbols used in this document .....	18
214	Table 3 – Graphical representation of fault tree: events .....	21
215	Table 4 – Graphical representation of fault tree: gates .....	22
216	Table 5 – Graphical representation of FTs: dynamic gates and functional dependencies.....	23
217	Table 6 – Ranking of cut sets.....	42
218	Table 7 – Approximate formulae for system reliability measures .....	54
219	Table H.1 – Reliability parameters of the SIS in Figure H.16.....	102
220	Table H.2 – Impact of functional dependencies .....	105
221		
222		



223

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

224

225

226

## FAULT TREE ANALYSIS

227

228

229

## FOREWORD

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

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

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

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

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

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

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

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

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

262 International Standard IEC61025 has been prepared by Technical committee TC 56:  
 263 Dependability.

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

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

268 a) The structure of the document has been modified with general applications of fault trees  
 269 discussed in the earlier clauses and applications specific to dependability in the later  
 270 clauses.

271 b) The mathematical content relating to dependability has been written to align with IEC 61078  
 272 (Reliability block diagrams) and to provide more information about availability, reliability and  
 273 failure frequency calculations.

274 c) Clauses have been introduced to describe non-coherent fault trees and dynamic fault trees.

275 d) Additional annexes have been added as follows: Annex A (Relationship with other  
 276 dependability and risk assessment techniques), Annex B (Automated fault tree  
 277 construction), Annex C (Use of Monte Carlo analysis for analysing uncertainty), Annex E

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

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

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

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

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

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

- 287 • reconfirmed,
- 288 • withdrawn,
- 289 • replaced by a revised edition, or
- 290 • amended.

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

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

[oSIST prEN IEC 61025:2023](https://standards.iteh.ai/catalog/standards/sist/30ac9e87-c897-4d24-98df-e966c3220647/osist-pren-iec-61025-2023)

<https://standards.iteh.ai/catalog/standards/sist/30ac9e87-c897-4d24-98df-e966c3220647/osist-pren-iec-61025-2023>

295

## INTRODUCTION

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

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

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

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

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

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

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

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

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

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

---

<sup>1</sup> Numbers in square brackets refer to the Bibliography

## FAULT TREE ANALYSIS

332  
333

### 1 Scope

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

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

353 In annexes, the document also describes:

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

### 2 Normative references

362 The following documents are referred to in the text in such a way that some or all of their content  
363 constitutes requirements of this document. For dated references, only the edition cited applies.  
364 For undated references, the latest edition of the referenced document (including any  
365 amendments) applies.

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

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

370

371 **3 Terms and definitions**

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

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

- 375 • IEC Electropedia: available at <http://www.electropedia.org/>
- 376 • ISO Online browsing platform: available at <http://www.iso.org/obp>

377 **3.1 Definitions directly relating to a fault tree**

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

379 **3.1.1**380 **Boolean related model**381 mathematical model where the state of a system is represented by a logical function of Boolean  
382 variables representing the states of its components383 Note 1 to entry: A Boolean variable only has two values and a logical function of several Boolean variables also  
384 has only two values. Those two values can be for example, {0, 1}, {up, down}, {true, false}, {working, failed}, etc. The  
385 underlying mathematics behind the logical functions is Boolean algebra.

386 [SOURCE: IEC 61078:2016]

387 **3.1.2**388 **fault tree**

389 FT

390 a directed acyclic graph (i.e. a graph without loops) representing the logical links between a top  
391 event and the primary events that caused it392 Note 1 to entry: The primary events could be component hardware failures, human errors, software failures or any  
393 other pertinent events that could contribute to the occurrence of the undesired event (top event).394 Note 2 to entry: According to IEC 60050-192 [192-04-01] a fault is the state of being unable to perform as required  
395 and a failure is the loss of the ability to perform as required (i.e. an event) However, in an FT, the term event is used  
396 to refer to either a state or an event.397 **3.1.3**398 **static fault tree**399 fault tree where it is reasonable to assume that the primary events are independent and their  
400 probabilities are constant401 **3.1.4**402 **sub fault tree**

403 fault tree related to an intermediate event within a fault tree

404 Note 1 to entry: Sub fault trees are used to split large fault trees into several parts, e.g. for readability,  
405 understandability or to fit on a page.406 **3.1.5**407 **dynamic fault tree**

408 DFT

409 fault tree implementing temporal interactions and where the assumption of independency  
410 between the primary events is not reasonably fulfilled411 Note 1 to entry: The primary events of a DFT can have interactions with elements external to the FT itself (e.g.  
412 weather, night and day, repair team availability, spare parts provisioning, etc.).

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

414 **3.1.6**  
 415 **non coherent fault tree**  
 416 fault tree where a failure path can become a success path by adding another fault or a success  
 417 path can become a failure path by removing a fault

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

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

422 **3.1.7**  
 423 **gate**  
 424 logic gate  
 425 symbol used to represent the logical relationship that must exist among its input events for its  
 426 output event to occur

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

429 **3.1.8**  
 430 **transfer symbol**  
 431 transfer gate  
 432 an IN-OUT symbol used to indicate that a fault tree has been split into smaller sub-fault trees

433 **3.1.9**  
 434 **top event**  
 435 root  
 436 top outcome  
 437 final event  
 438 event of interest for which the FTA is performed

iTeh STANDARD PREVIEW  
 (standards.iteh.ai)

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

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

442 **3.1.10**  
 443 **primary event**  
 444 leaf  
 445 an event in the FT which the FT analyst has chosen for some reason not to develop any further

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

448 **3.1.11**  
 449 **complementary primary event**  
 450 primary event repeated in the FT in its negated form

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

453 **3.1.12**  
 454 **basic event**  
 455 primary event at the lowest level of resolution defined for the purpose of analysis

456 **3.1.13**  
 457 **intermediate event**  
 458 event that is neither a top event nor a primary event

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

460 **3.1.14**  
461 **undeveloped event**  
462 a primary event in the FT that the FT analyst has chosen not to develop further because its  
463 development is inconsequential or the information required to develop the event further is not  
464 available

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

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

467 **3.1.15**  
468 **event to be developed**  
469 a primary event in the FT which the FT analyst has chosen not to develop further at the time of  
470 FT development but wants to indicate that it will be developed later for the completion of the  
471 FTA.

472 **3.1.16 Note 1 to entry:**  
473 **house event**  
474 primary event which is expected to occur

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

476 **3.1.17**  
477 **condition event**  
478 conditional event  
479 primary event defining a condition which is referred to in an IF gate

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

481 **3.1.18**  
482 **repeated event**  
483 replicated event  
484 primary event appearing more than once in a fault tree

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

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

488 **3.1.19**  
489 **common cause events**  
490 different events in a fault tree that have the same cause for their occurrence

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

493 Note 2 to entry: In the context of fault tree, common cause events are generally common cause failures (see IEC  
494 60050-192, definition [192-03-18]).

495 **3.1.20**  
496 **common cause**  
497 a single cause that results in the occurrence of several events

498 **3.1.21**  
499 **cut set**  
500 group of primary events that, if all occur, would result in the occurrence of the top event

501 **3.1.22**  
502 **minimal cut set**  
503 a group of primary events such that the occurrence of every primary event is necessary and  
504 sufficient to cause the top event