

This is a preview - click here to buy the full publication



IEC TR 63039

Edition 1.0 2016-07

TECHNICAL REPORT



Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 03.120.01; 03.120.30

ISBN 978-2-8322-3511-9

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references.....	10
3 Terms, definitions and abbreviated terms	10
3.1 Terms and definitions	10
3.2 Abbreviated terms	17
4 Difference between frequency and rate of final event.....	17
5 Final event frequency and final event rate at a given initial state	19
5.1 General.....	19
5.2 Classification of final events	19
5.3 Final event frequency in a steady state	20
5.4 Final event rate at a given initial state and at a recognised state	22
5.5 Relationship between final event rate and frequency at a given initial state	22
6 Procedure for probabilistic risk analysis and flow to reach risk profile	23
7 Techniques for quantitative analysis of the occurrence of a final event.....	24
7.1 Graphical symbols for three types of final events	24
7.1.1 General	24
7.1.2 Repeatable final event	24
7.1.3 Unrepeatable final event resulting in a renewable final state	30
7.1.4 Unrepeatable final event resulting in an unrenovable final state.....	30
7.2 Analytical example of an unrepeatable final event.....	31
7.2.1 General	31
7.2.2 Average final event frequency	32
7.2.3 Final event rate at a given initial state	34
8 Final event rate at a recognised state and recognised group state	40
8.1 General.....	40
8.2 Example of recognised (group) states	40
9 Analysis of multiple protection layers	43
9.1 General.....	43
9.2 Frequency and rate for repeatable events	45
9.2.1 General	45
9.2.2 Independent of event sequence.....	45
9.2.3 Depending on event sequence	47
9.3 Final protection layer arranged in a 1-out-of-1 architecture system	51
9.3.1 General	51
9.3.2 Final event rate at initial state (0, 0) for unrepeatable final event.....	51
9.3.3 Final event rate at recognised state (x, y)	53
9.3.4 Final event rate at a recognised group state	54
9.4 Final protection layer arranged in a 1-out-of-2 architecture system	56
9.4.1 General	56
9.4.2 Independent failure parts of the 1-out-of-2 architecture system	57
9.4.3 Fault tree for independent undetected and detected failures.....	58
9.4.4 Final event rate at a given initial state owing to independent failures.....	58
9.4.5 Recognised states at each part	59

9.4.6	Recognised (group) states and final states for the overall system.....	60
9.5	Common cause failures between protection layers and complexity of a system.....	61
9.6	Summary and remarks	61
Annex A	(informative) Risk owing to fault recognised only by demand	62
A.1	Demand, detection and failure logic.....	62
A.2	Final event rate at a given initial state.....	64
A.3	Comparison between new and conventional analyses	65
A.4	Further development	67
A.5	Summary and remarks	68
Annex B	(informative) Application to functional safety	69
B.1	Risk-based target failure measures in functional safety	69
B.2	Safe/dangerous system states and failures	70
B.3	Complexity of safety-related systems.....	72
B.4	Comparison between conventional and new analyses	73
B.5	Splitting up mode of operation	74
B.6	Tolerable hazardous/harmful event rate and residual risk.....	75
B.7	Procedure for determining the safety integrity level (SIL) of an item	75
B.8	Summary and remarks	76
Bibliography	77
Figure 1	– Antecedent state, final event, final state and renewal event.....	18
Figure 2	– Time to final event (TTFE) and time to renewal event (TTRE).....	19
Figure 3	– State transition models with various final states	21
Figure 4	– Procedure for analysis of repeatable/unrepeatable final events	24
Figure 5	– FT for an unrepeatable final event resulting in an unrenovable final state.....	31
Figure 6	– State transition model resulting in an unrenovable final state	32
Figure 7	– FT for an unrepeatable final event resulting in a renewable final state	35
Figure 8	– State transitions resulting in a renewable final state	35
Figure 9	– FT for unintended inflation of an airbag due to failure of control.....	38
Figure 10	– State transition model of unintended inflation of an airbag	39
Figure 11	– Event tree of a demand source, int. PL and FPL for a risk	44
Figure 12	– Failure of int. PL independent of event sequence	46
Figure 13	– FT for failure of int. PL through sequential failure logic	49
Figure 14	– FT for an unrepeatable final event at initial state (0,0)	53
Figure 15	– State transition model for an unrepeatable final event at initial state (0,0).....	53
Figure 16	– FT for an unrepeatable final event for recognised state (0,1)	54
Figure 17	– State transition model for recognised state (0,1).....	54
Figure 18	– FT for an unrepeatable final event for recognised group state G1	55
Figure 19	– State transition model for recognised group state G1.....	56
Figure 20	– RBD of FPL arranged in a 1-out-of-2 architecture system	57
Figure 21	– RBD of the independent parts of Ch 1 and Ch 2	57
Figure 22	– RBD equivalent to that in Figure 21.....	58
Figure 23	– FT for UD failure of Ch 1, D failure of Ch 2 and demand	58
Figure 24	– State transitions due to UD failure of Ch 1, D failure of Ch 2 and demand	59

Figure A.1 – Reliability block diagram with independent and common cause failures	62
Figure A.2 – Fault tree of unrepeatable final event due to DU failures	63
Figure A.3 – State transition model for unrepeatable final event caused by DU failures	64
Figure A.4 – Comparison between analyses of $r(\lambda_M)$ and ϖ	67
Figure B.1 – Comparison between conventional and new analyses	74
Table 1 – Events and associated risks.....	9
Table 2 – Symbols newly introduced for event tree and fault tree analyses.....	25
Table 3 – Symbols and graphical representation for a repeatable (final) event.....	26
Table 4 – Symbols and graphical representation for a renewable final state	27
Table 5 – Symbols and graphical representation for an unrenewable final state.....	29
Table 6 – Symbols and graphical representation for the FER at recognised state 3	41
Table 7 – Symbols and graphical representation for FER at recognised group state G.....	42
Table B.1 – Relationship between failure modes, hazards, and safe/dangerous failures	72
Table B.2 – Safety integrity levels (SILs) in IEC 61508 (all parts).....	76

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PROBABILISTIC RISK ANALYSIS OF TECHNOLOGICAL SYSTEMS – ESTIMATION OF FINAL EVENT RATE AT A GIVEN INITIAL STATE

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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a Technical Report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 63039, which is a Technical Report, has been prepared by IEC technical committee 56: Dependability.

The text of this Technical Report is based on the following documents:

Enquiry draft	Report on voting
56/1655/DTR	56/1684/RVC

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

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

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

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

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This document defines the basic properties of events from the perspective of probabilistic risk analysis and use of dependability-related techniques for the analysis of occurrence of the final event that results in a final state in which the final consequences of a risk may appear (see 3.1.1, 3.1.10 and 3.1.17).

Techniques that are applied to risk analysis such as checklists, what-if/analysis, hazard and operability (HAZOP) studies, event tree analysis (ETA), fault tree analysis (FTA), were originated in the field of system safety and have been highly developed by bringing those fields of dependability and system safety into connection for many years [11][14][17][34][35][36]¹. The analytical techniques described in IEC 61025, IEC 61165 and IEC 62502 are well defined and systematised for dependability analysis. However it should be considered that there are significant differences between the dependability and probabilistic risk analyses.

Firstly, states of an item such as the up, down, operating and non-operating states as well as those events of failure and restoration are usually brought into focus in the dependability analysis [5][7]. The probabilistic risk analysis is often concerned with not only those aspects of the states and events related to the down and up but also states of demand and non-demand, and initial, intermediate and final states, as well as such additional events as demand, completion, final and renewal events (see 3.1.3, 3.1.8, 3.1.10, 3.1.11, 3.1.17 and 3.1.20).

Secondly, types of the final event should be considered for the probabilistic risk analysis because systemic dependencies between items are often dominant over the occurrence of the final event. Namely, the final events are categorised into the repeatable and unrepeatable from the perspective of probabilistic risk analysis (see 3.1.18 and 3.1.19). In addition the sequence of occurrences of events should be taken into account because the event sequence often dominates the occurrence of the final event (see 7.2, 9.2, 9.3 and 9.4).

The quantitative measures targeted by the dependability analysis are mainly the failure rate, failure frequency, repair rate, reliability, availability and maintainability, etc. of an item. Not only those target measures but also additional measures such as rates and frequency of those events of demand, completion and renewal, as well as risk exposure time should be explicitly and comprehensively analysed for the probabilistic risk analysis (see 3.1.30).

When risk analysis is performed quantitatively, the event rate and frequency are generally used for the target measures of occurrence of final event (see for instance Annex B). In this document, the target measures of occurrence of final event are defined by such measures as a final event frequency (FEF), average FEF, final event rate (FER) at a given initial state, and FEF at a given initial state (see 3.1.21, 3.1.22, 3.1.25 and 3.1.26).

Such measures as FEF at a given initial state are newly introduced target measures for the probabilistic risk analysis, which are quite different from those target measures of conventional dependability analyses mentioned above, because such variables as demand and completion rates and frequencies, as well as risk exposure time that have not been applied to the conventional dependability analyses are explicitly introduced into the new target measures. Therefore, those new measures should be defined and those conventional techniques modified appropriately for the application to the probabilistic risk analysis.

In addition it is inevitable for the risk analysis of complex systems that such analytic techniques as the HAZOP, FMEA, RBD, FTA and Markov techniques should be applied complementarily. This document illustrates how to orchestrate those modified techniques to extract the maximum synergistic efficacy for the probabilistic risk analysis.

¹ Numbers in square brackets refer to the Bibliography.

Thus, this document aims at defining the target measures of occurrence of a final event by the FER at a given initial state, FER at a recognised state and FER at a recognised group state for the probabilistic risk analysis, and advises how to apply the modified techniques complementarily to the analysis of those target measures by referring to the topics focusing on risk analyses of nuclear power plants, airbag control, automated brake and steering control systems for self-driving cars, system with fault recognised only by demand, as well as the application of this document to functional safety.

It is generally believed that probabilistic risk analyses are more complicated than those of dependability. However, this document will provide a much simpler and realistic approach for probabilistic risk analyses compared to the conventional approaches, and will make it easier to cope with the risks of complex systems (see Table 1, Clause 6, 9.1, 9.2, 9.5, Clauses A.5 and B.3).

PROBABILISTIC RISK ANALYSIS OF TECHNOLOGICAL SYSTEMS – ESTIMATION OF FINAL EVENT RATE AT A GIVEN INITIAL STATE

1 Scope

This document provides guidance on probabilistic risk analysis (hereafter referred to as risk analysis) for the systems composed of electrotechnical items and is applicable (but not limited) to all electrotechnical industries where risk analyses are performed.

This document deals with the following topics from the perspective of risk analysis:

- defining the essential terms and concepts;
- specifying the types of events;
- classifying the occurrences of events;
- describing the usage of modified symbols and methods of graphical representation for ETA, FTA and Markov techniques for applying those modified techniques complementarily to the complex systems;
- suggesting ways to handle the event frequency/rate of complex systems;
- suggesting ways to estimate the event frequency/rate based on risk monitoring;
- providing illustrative and practical examples.

The relationship between the events covered by this document and associated risks are described in Table 1. Risk is defined as the effect of uncertainty on objectives (see 3.1.1). The uncertainty is here assumed to be composed of two elements: the epistemic and aleatory. The epistemic is categorised into the known and unknown, and the effect of the aleatory is classified into the controlled and the uncontrolled, respectively. Therefore, the risk associated with the known event of which impact is controlled is the controlled risk, and the risk associated with the known event of which impact is not controlled is the uncontrolled risk. Favourable meta-risk is of an unknown event of which impact can be casually controlled even if this unknown event appears, and unfavourable meta-risk is of an unknown event of which impact cannot be controlled.

For example, the risks resulting from random hardware failures of electrotechnical items will be categorised into the controlled or uncontrolled risks, while the risks owing to software bugs could be classified into the favourable or unfavourable meta-risks. This document covers the controlled and uncontrolled risks resulting from the events that can be assumed to occur randomly and independently of time (see Clause 6, 9.1, 9.2, 9.5 and Clause B.3).

Table 1 – Events and associated risks

		Epistemic	
		Known	Unknown
Aleatory	Controlled	Controlled Event risk	Controlled Meta-risk
	Uncontrolled	Uncontrolled Event risk	Uncontrolled Meta-risk

2 Normative references

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

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

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