IEC TR 63039

Edition 1.0 2016-07

TECHNICAL REPORT

colour inside

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

IEC TR 63039:2016-07(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

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

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

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

Edition 1.0 2016-07

TECHNICAL REPORT

colour inside

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

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 modifed 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*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-192 and IEC 61703, as well as the following apply.

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

3.1.1
risk
effect of uncertainty on objectives

Note 1 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence (see ISO Guide 73:2009, 1.1, Note 4).

Note 2 to entry: Safety-related risk is defined as the combination of the probability of harm and the severity of that harm (see 3.9 in ISO/IEC Guide 51:2014).

Note 3 to entry: Residual risk is the risk remaining after risk treatment. The risk treatment includes the process to modify any risk by protection layers in this document (see 3.8.1.6 in ISO Guide 73:2009, 7.2.1, 9.1 and Clause B.6).

[SOURCE: ISO Guide 73:2009, 1.1, modified — the notes from the original definition have been replaced by new notes.]

3.1.2
state

3.1.2.1
state
<mathematical expression> particular condition which an item keeps in a specific time interval

Note 1 to entry: A fault is for example a state while a failure is an event. A state transition diagram describes system states and state transitions (see 192-03-01 in IEC 60050-192:2015, and 3.1.4, 3.1.5 and 3.1.7).

3.1.2.2
state
<risk identification, analysis and controls> property of a system being of certain duration

Note 1 to entry: States are classified into activated and inert states according to their degree of disorder (or order). The activated state is in the lower degree of disorder (i.e., the higher degree of order) and the inert state is in the higher degree of disorder. The measure of disorder of a system state is entropy that is also a measure of the "multiplicity" associated with the system state (see 3.1.2.2, Note 4, 3.1.3, Note 2, and Clause B.2).

Note 2 to entry: If items interact with each other, an activated action can occur in their activated state, however in their inert state the activated action cannot occur and an inert action is generated instead of the activated action.

Note 3 to entry: Activated actions are categorized into, for example, types of: a) energy transmission, b) information propagation, c) agent transfer, d) supply obstruction, and e) the rest [16].

Note 4 to entry: Function is an ability of an item to generate activated action(s) or inert action(s) or both as required (see 3.1.3, 3.1.13, 3.1.32, 3.1.33, 3.1.34, 7.2, 9.1, Clauses B.1, B.4, B.5 and B.6) [16].

3.1.3
demand state
state in which a function is demanded from a system

Note 1 to entry: Under a demand state an item is required to be operating to demonstrate its specific function(s), i.e., to generate activated action(s) or inert action(s) or both as required (see 3.1.2.2, Note 4).

Note 2 to entry: A non-demand state is the state where a function is not demanded from a system, i.e., the item is required to be in a non-operating state for a specific function(s) (see 192-02-06 in IEC 60050-192:2015).

Note 3 to entry: A state, for instance, in which a driver of automobile is activating the computer-regulated brake control system to stop the automobile is a demand state for this function of the system, and the state in which the driver is not activating this control system is a non-demand state for this function of the control system. The state in which the driver is not activating this control system is the demand state for the additional function of this control system to prevent unnecessary activation of the brake control function to stop an automobile from occurring, and the state where the driver is activating the control system is the non-demand state for the additional function (see 9.3.1 b) and Clause B.2).

Note 4 to entry: A demand is defined as the start of a demand state, and a completion is defined as the termination of the demand state. A demand and completion are events (see 3.1.4).

Note 5 to entry: Continuous mode of operation for a function is a mode of operation where a demand state for the function lasts for use. The demand mode of operation of a function is that where those demand and non-demand states, i.e., demands and completions appear alternately for use (see 7.2, 9.3, Clauses A.1, B.1, B.4, B.5 and B.7).

Note 6 to entry: Demand and operating states are not equivalent because of the possibility of two failure modes: an item is operating under a non-demand state, and another item is not operating under a demand state (see 3.1.3, Notes 1 and 2, and 9.3).

3.1.4
event
transition
change from one state to another state

Note 1 to entry: An event is the termination of a state or the start of a next state.

Note 2 to entry: In the context of risk analysis, a risk is often represented not only by verbal expressions but also in terms of states and their transitions by use of a fault tree (FT), a state transition diagram, etc.

Note 3 to entry: Events are classified into intermediate and final events from the perspective of state transition diagrams for representation of risks (see 3.1.16 and 3.1.17).

[SOURCE: IEC 61165:2006, 3.9, modified — the notes from the original definition have been replaced by new notes.]

3.1.5
system
set of interrelated or interacting elements

Note 1 to entry: The structure of a system may be hierarchical. An overall system is composed of several subsystems.

Note 2 to entry: For convenience the term “system state” will be used to denote a state of a system (see 3.1.7).

[SOURCE: ISO 9000:2015, 3.5.1, modified — notes have been added.]

3.1.6
element
component or set of components, which acts as a single entity

3.1.7
system state
particular combination of the states of elements that compose a system

Note 1 to entry: The system state often consists of up, down, operating and non-operating states of items, demand and non-demand states, and other environmental conditions outside of the items (see 3.1.5, Note 2).

3.1.8
initial state
system state in which a system originates the first state transition in a state transition diagram that represents (a) risk(s)

Note 1 to entry: If a risk is identified, it can be represented not only verbally but also by use of such diagrams as an event tree, FT, etc. for qualitative or probabilistic risk analyses (see for example Figure 3, Figure 9 and Figure 10).

Note 2 to entry: If system state X is, for instance, an initial state, this is also expressed as initial state X.

3.1.9
virtual initial state
system state to which a virtual state transition from a final state is assumed to calculate MTFE at a recognised state and FER at a recognised state

Note 1 to entry: See 3.1.10, 3.1.24, 3.1.25, 3.1.27 and 3.1.28.

Note 2 to entry: See for example Figure 17.

Note 3 to entry: If system state X is, for instance, a virtual initial state, this is expressed as virtual initial state X.

3.1.10
final state
system state in which the final consequences of a risk may appear

Note 1 to entry: The final consequence does not always appear in the final state because it may depend on the sequence of appearances of int. states (see 3.1.11, 7.2, 9.2 and 9.3).

Note 2 to entry: A system enters the final state by a final event (see 3.1.17).

3.1.11
int. state
intermediate state
system state in a state transition diagram that represents (a) risk(s), which is not the initial or final states

3.1.12
antecedent state
initial state, or, if it exists, any int. state in a state transition diagram that represents (a) risk(s)

Note 1 to entry: See 3.1.8 and 3.1.11.

Note 2 to entry: An antecedent state can be designated by use of a set of states such as up, down, operating, non-operating, demand, non-demand, shutdown states, and other environmental conditions (see for example Figure 3).

3.1.13
recognised state
antecedent state that is detected and/or recognised at a specific time

Note 1 to entry: Antecedent states are often (but not always) recognised by use of such means as self-diagnosis functions of products, periodical tests of components, human recognition of circumstances, human recognition of operation, etc., at a specific time.

Note 2 to entry: If an antecedent state of a system is a recognised state, then it can be recognised that the system state is or is not in this antecedent state at a specific time, and vice versa.

Note 3 to entry: A final state is assumed to be recognised at any time in this document (see 9.3 and 9.4).

Note 4 to entry: Because there may be antecedent state(s) outside of monitoring and recognition, the antecedent states are not always recognised and therefore classified into the recognised and not recognised states (see 3.1.15, Note 1).

3.1.14
group state
set of two or more antecedent states that cannot be recognised as single antecedent states

Note 1 to entry: See 3.1.13, Note 4.

3.1.15
recognised group state
group state that is recognised at a specific time

Note 1 to entry: Suppose, for example, that antecedent states are system states A, B and C, and the recognised state is system state C only, then the group state that is composed of A and B is the recognised group state, because it can be recognised that the system is in this group state if it is recognised that the system is in neither the system state C nor the final state at a specific time, and vice versa (see, 3.1.13, Notes 3 and 4).

3.1.16
int. event
intermediate event
state transition which is not the final or the renewable events

Note 1 to entry: See 3.1.4, 3.1.17 and 3.1.20.

Note 2 to entry: A state transition between antecedent states is an int. event, but not vice versa (see 3.1.18).

3.1.17
final event
start of the final state, i.e., a state transition from any antecedent state (or critical state) to the final state

Note 1 to entry: See 3.1.10 and 3.1.12.

Note 2 to entry: A final event is also called a critical event, but not vice versa [7].

Note 3 to entry: This term may refer to a hazardous or harmful event in the field of (functional) safety [10].

3.1.18
repeatable final event
final event that can repeat

Note 1 to entry: See for example Figure 3.

Note 2 to entry: It is necessary for a repeatable final event that this final event does not affect the way of appearance and disappearance of (an) int. state(s), because if a final event changes the way(s) of appearance and disappearance of the int. state(s), the original system state(s) and the associated risk that results from the original system state(s) will not remain any longer after the final event.

Note 3 to entry: The final state that results from a repeatable final event may cause transition to int. state(s) and the final event may repeat (see 3.1.16, Note 2).

3.1.19
unrepeatable final event
final event that cannot repeat

Note 1 to entry: See for example Figure 3.

Note 2 to entry: If a final event changes the way(s) of appearance and disappearance of (an) intermediate state(s) permanently then the final event cannot repeat, because the original system state(s) and the risk resulting from the original system state(s) do not remain any longer after the final event (see 3.1.18, Note 2).