PD IEC/TR 63039:2016

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: PD IEC/TR 63039:2016

National foreword

This Published Document is the UK implementation of IEC/TR 63039:2016.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 92982 3
ICS 03.120.01; 03.120.30

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 July 2016.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD IEC/TR 63039:2016

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

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.

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: PD IEC/TR 63039:2016

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 unrenewable 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

AVA Documents
Document Sharing Hub

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 unrenewable final state 31
Figure 6 – State transition model resulting in an unrenewable 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

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

Figure A.1 – Reliability bock 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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

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.

AVA Documents
Document Sharing Hub

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.

Documents
Document Sharing Hub

Full document details: PD IEC/TR 63039:2016

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.

Documents
Document Sharing Hub

Full document details: PD IEC/TR 63039:2016

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).

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

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).

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

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.

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

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).

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

Note 3 to entry: If a final state is transferred to the initial state and the system is renewed, the final event is the unrepeatable final event because the renewed system state is different from the original system state (namely the renewed system state is not the original system state itself).

3.1.20
renewal event
termination of a final state that results from an unrepeatable final event, causing transition to an initial state or a virtual initial state

Note 1 to entry: The final state resulting from a repeatable final event may cause transition to an int. state(s) (see 3.1.18, Note 3).

3.1.21
event frequency
limit, if it exists, of the quotient of the mean number of occurrences of an event within time interval [t, $t+\Delta t$], to Δt, when Δt tends to zero, given that the system is in a given initial state at time t = 0

Note 1 to entry: Event frequency $\omega(t)$ is expressed in the formula

$$\omega(t) = \lim_{\Delta t \to 0+} E[N(t+\Delta t) - N(t)] / \Delta t$$

where

$N(t)$ is the statistically-expected number of occurrences of an event in the time interval [0, t], where E denotes the expectation.

Note 2 to entry: The unit of measurement of event frequency is the unit of time to the power -1.

3.1.22
average event frequency
event frequency averaged over a period of time H

Note 1 to entry: Average event frequency of $\omega(t)$, $\omega(0,H)$, is defined as

$$\omega(0,H) = (1/H)\int_0^H \omega(t)dt$$

where

$\omega(t)$ is event frequency at time t;

$\int_0^H \omega(t)dt$ is the probability that an unrepeatable event occurs in the time interval [0, H] or is the statistically-expected number of occurrences of a repeatable event in the time interval [0, H].

3.1.23
state transition rate
conditional event intensity
limit, if it exists, of the quotient of the conditional probability that an event, i.e., a state transition from system state X to Y, occurs within time interval [t, $t+\Delta t$], to Δt, when Δt tends to zero, given that the system is in system state X at time t

Note 1 to entry: If the occurrence of an event follows an exponential distribution, i.e., an event occurs at random and independently of time, then the conditional event intensity is constant and the constant conditional event intensity is called a constant event rate or a constant state transition rate in this document (see Clauses 1, 5, 7, 9, A.1 and B.1).

Note 2 to entry: The unit of measurement of event rate and state transition rate is the unit of time to the power -1.

3.1.24
MTFE at a given initial state
mean time to final event at a given initial state
mean time from an initial state or a virtual initial state to the occurrence of the first final event

Note 1 to entry: A given initial state means any antecedent state (see 3.1.8, 3.1.9, 3.1.12 and 3.1.20).

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

Note 2 to entry: The MTFE at a given initial state is similar to mean up time (MUT) rather than mean operating time to failure (MTTF), however antecedent states include not only up, down, operating and non-operating states of items but also demand, non-demand, shutdown states and other environmental conditions outside of the items (see IEC 60050-192: 2015,192-05-11 and IEC 60050-192:2015,192-08-09).

3.1.25
FER at a given initial state
final event rate at a given initial state
limit, if it exists, of the quotient of the conditional probability that a final event occurs within time interval [t, $t+\Delta t$], to Δt, when Δt tends to zero, given that the system, of which state transition rates are constant, and of which final state causes transition only to an initial state or a virtual initial state, is in a steady state and is not in the final state

Note 1 to entry: For the renewable system with constant state transition rates the FER at a given initial state becomes constant and equals the reciprocal of the MTFE at a given initial state [18][19][27][29].

Note 2 to entry: The FER at a given initial state may refer to a harmful or hazardous event rate (HER) in the field of functional safety (see 3.1.17, Note 3, 7.2, 9.3.2, Clauses B.1 and B.4).

Note 3 to entry: Steady state is the state of a system where infinite time has elapsed and the probabilities of all systems states of a state transition diagram that represents (a) risk(s) converged to constant values.

3.1.26
FEF at a given initial state
final event frequency at a given initial state
frequency of the final event, given that the system, of which state transition rates are constant, and of which final state causes transition only to an initial state or a virtual initial state, is in a steady state

Note 1 to entry: See 3.1.17, 3.1.21 and 3.1.25, Note 3.

Note 2 to entry: For the renewable system with constant state transition rates the FEF at a given initial state becomes constant and equals the reciprocal of mean time from the initial state to the occurrence of the first renewal event [18][19][27][29].

Note 3 to entry: FER at a given initial state, φ, is expressed in the formula [18][19][27][29]:

$$\varphi = \omega / \left(1 - P\{X\}\right)$$

where

ω is the FEF at a given initial state;

$P\{X\}$ is the probability that the system is in the final state in a steady state.

3.1.27
MTFE at a recognised state
mean time to final event at a recognised state
MTFE at a given initial state when the given initial state is a recognised state

Note 1 to entry: See 3.1.24.

3.1.28
FER at a recognised state
final event rate at a recognised state
FER at a given initial state when the given initial state is a recognised state

Note 1 to entry: See 3.1.25.

Note 2 to entry: The relationship between the FER at a recognised state and the FEF at a recognised state is identical with that between the FER at a given initial state and the FEF at a given initial state (see 3.1.26, Note 3, 8.2 and 9.3.3).

3.1.29
FER at a recognised group state
final event rate at a recognised group state
weighted average of all the FER at a given initial state in a group state

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

Note 1 to entry: See 8.2, 9.3.4 and 9.4.5.

3.1.30
risk exposure time
T
statistically expected time while a system will be exposed to a specific risk during its life

Note 1 to entry: See 5.2, 7.2.2, 7.2.3, Clauses A.3 and A.4.

Note 2 to entry: Risk exposure time T is often referred to such terms as useful life (see IEC 60050-192:2015, 192-02-27), operational life and mission time. However those terms are not necessarily equivalent to the risk exposure time because a risk can be changed into a number of transformed risks during the useful (or operational) life or the mission time of a system, and a specific risk among those risks could only be of interest to the risk exposure time. In such a case, the risk exposure time will not be equivalent to the time specified by those terms.

3.1.31
APF_{drg}
approximate probability of dangerous failure during a demand state
P_b
approximate probability that a dangerous failure of an item occurs in statistically expected time interval of a demand state [0, τ], given that the demand at the item occurred at time zero

Note 1 to entry: It is a necessary condition for the approximation that the probability of two or more occurrences of the dangerous failure in the time interval [0, τ] is negligible (see 7.2.3, 9.3.1 b), 9.3.2 and Annex B).

Note 2 to entry: This term is applied to the risk analysis in the field of safety only (see Annex B).

3.1.32
PFD_{avg}
average probability of dangerous failure on demand
P_a
mean unavailability of an item to perform a specified safety function when a demand occurs

Note 1 to entry: This term is applied to functional safety only (see IEC 61508-4:2010, 3.6.18).

Note 2 to entry: It is postulated for this term that the state of item is changed from a non-operating state to an operating state by the demand and the item can fail in the non-operating state (see 7.2.3, 9.3.1 b), 9.3.2 and Annex B).

3.1.33
PFH
average frequency of dangerous failure per hour
λ
average frequency of a dangerous failure of an item to perform a specified safety function over a given period of time

Note 1 to entry: This term is applied to functional safety only (see IEC 61508-4:2010, 3.6.19).

Note 2 to entry: The PFH approximates to the reciprocal of a mean operating time to first failure in the case where the dangerous failure is an unrepeatable final event, whereas it approximates to the reciprocal of a mean operating time between failures in the case where the dangerous failure is a repeatable event. The item is usually assumed to be able to fail in a non-operating state (see IEC 61508-4:2010, 3.6.19, Note 4, as well as IEC 61508-6:2010, B.2.3.2 and B.2.3.3; and 3.1.32, Note 2, 7.2.3, 9.3.1 b), 9.3.2 and Annex B in this document).

3.1.34
channel
Ch
component or group of components that independently implements a function of an item

Note 1 to entry: An independent Ch is a single 1-out-of-1 architecture system for a function(s), i.e., if any component of the Ch is in a fault then the Ch is also in a fault.

3.1.35
basic element
MCS element
element that composes an MCS extracted through FTA or RBD analysis or both

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

Note 1 to entry: An MCS element is always a basic event of an FT, but not vice versa. Therefore, for convenience, the term "basic element" will be used to denote an MCS element.

3.2 Abbreviated terms

APF_{drg}	Approximate probability of dangerous failure during a demand state
CCF	Common cause failures
Ch	Channel
D	Detected
DU	Detected only by demand
E/E/PE	Electrical/electronic/programmable electronic
ETA	Event tree analysis
FEF	Final event frequency
FER	Final event rate
FMEA	Failure modes and effects analysis
FPL	Final protection layer
FT	Fault tree
FTA	Fault tree analysis
HAZOP	Hazard and operability
HER	Harmful (hazardous) event rate
Int.	Intermediate
MCS	Minimal cut set
MTFE	Mean time to final event
MTRE	Mean time to renewal event
MTTF	Mean operating time to failure
MUT	Mean up time
PAND	Priority AND
PFD_{avg}	Average probability of dangerous failure on demand
PFH	Average frequency of dangerous failure per hour
PL	Protection layer
RBD	Reliability block diagram
SIL	Safety integrity level
TTFE	Time to final event
TTRE	Time to renewal event
UD	Undetected

4 Difference between frequency and rate of final event

The term frequency can be used both to refer to the number of times an event occurs over a given sample and to refer to the number of times it occurs in a given time period. In this document the latter meaning is used and therefore defined in 3.1.21.

On the other hand, the term rate generally means the speed at which something moves or happens, and in the field of dependability an event rate such as a failure rate is defined as a limit, if it exists, of the quotient of the conditional probability that the event occurs within time interval $[t, t+\Delta t]$, to Δt, when Δt tends to zero, given that the event has not occurred up until time t.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

The definitions of the event rate and event frequency seem quite different. However, in the field of risk assessment, the event frequency and event rate are often confused as described below. Figure 1 describes changes of states of an overall system, in which occurrences of the final and renewal events follow exponential distributions, i.e., the final event rate (FER) and renewal event rate are constant (see 3.1.17, 3.1.20 and 3.1.23). Two system states, the final and antecedent states, are described in Figure 1 (see 3.1.10 and 3.1.12).

Figure 2 describes a process of occurrences of final and renewal events, in which the TTFE and TTRE are equivalent to the amount of time while the antecedent state continues (i.e., the duration of the antecedent state) and the amount of time while the final state continues (i.e., the duration of the final state), respectively. Here, it is assumed that the stochastic process of the occurrences of final and renewal events can be modelled by use of a Markov transition diagram, and the MTFE and MTRE are T_a (≠0) [h] and T_b (≠0) [h], respectively. Then, in a steady state of the process, the FEF, ω [1/h], is expressed in the following equation:

$$\omega = 1/(T_a+T_b) \tag{1}$$

where

T_a is MTFE [h]

T_b is MTRE [h]

The final event rate (FER), φ [1/h], and renewal event rate, m [1/h], are also expressed by:

$$\varphi = 1/T_a \quad \text{(i.e., } T_a = 1/\varphi\text{)}; \tag{2}$$

$$m = 1/T_b \quad \text{(i.e., } T_b = 1/m\text{)} \tag{3}$$

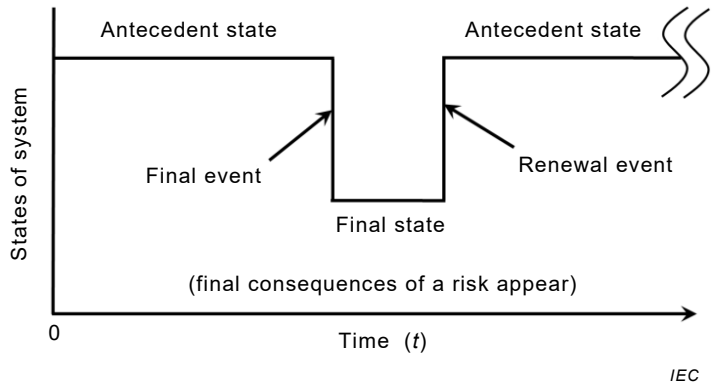


Figure 1 – Antecedent state, final event, final state and renewal event

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

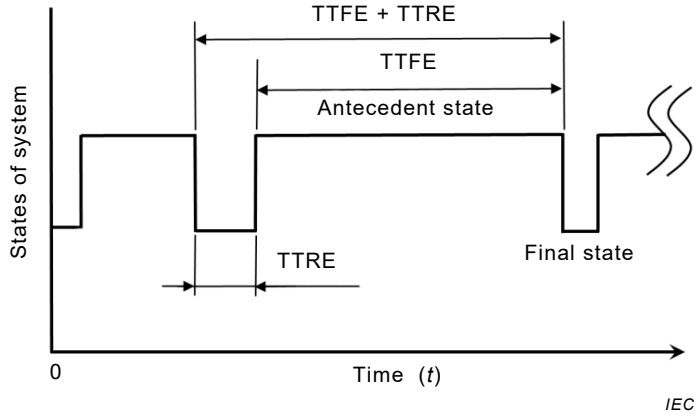


Figure 2 – Time to final event (TTFE) and time to renewal event (TTRE)

The FEF can be expressed by use of φ and m from Equations (1), (2) and (3):

$$\omega = \varphi m/(\varphi+m) = \varphi/\{(T_b/T_a)+1\} \quad (4)$$

If T_a is much greater than T_b, namely if φ is much less than m, then ω is nearly equal to φ. However the FEF is not necessarily equal to the FER, and the following discussion is possible.

a) In the field of risk assessment of nuclear power plants, for example, the tolerable risk of severe accidents like meltdown is defined by use of the event frequency per year-plant. Here, the final event is a meltdown.

b) If a tolerable frequency of the final event is 10^{-4} [1/year-plant], then typically two cases can be assumed. One is $1/\varphi$ = 50 years and $1/m$ = 9 950 years, and therefore $1/\omega$ = 10 000 years. Another case is $1/\varphi$ = 9 950 years and $1/m$ = 50 years, and $1/\omega$ = 10 000 years.

c) Although the event frequencies of those two cases are equal, the probabilities that the event will occur in its operating life or risk exposure time of 50 years are different. Namely, those probabilities may be 60 % or more for the first case, and be 0,5 % or lower for the second case. This means the level of risk of the first case is much higher than that of the second case.

Thus, it is desirable to utilize not the event frequency but the event rate for the target measure of occurrence of a rare final event.

5 Final event frequency and final event rate at a given initial state

5.1 General

Clause 5 clarifies the FEF at a given initial state and FER at a given initial state, and defines how to adapt those to the target measures of the occurrence of a final event.

5.2 Classification of final events

Figure 3 a), Figure 3 b) and Figure 3 c) are the state transition diagrams that represent risks, where system states A, B and C are an initial state, int. state and final state, respectively (see 3.1.4, Note 2).

If Figure 3 refers to risks associated with some human activity, for example, symbol B indicates the system state in which a human is at work, A is the system state in which he stops working and takes a rest, and C is the system state in which some slight incident or some disaster has befallen him.

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

If a final event occurs, there are two possible successive situations.

a) This final event has no effect on the way of occurrence of the int. event(s), the final state can cause transition to the int. state(s) and the final event can repeat (see Figure 3 a)). This final event is hereafter referred to as a repeatable final event (see 3.1.18).

b) That final event does not repeat because it changes permanently the way in which the int. states appear and disappear, and therefore the risk identical with that of the original system state is no longer retained (see Figure 3 b) and Figure 3 c)). This final event is hereafter referred to as an unrepeatable final event (see 3.1.19).

Figure 3 a) shows a state transition model of the system in which the transition is caused from final state C to int. state B, and the final event can repeat. In this model the constant event rates, λ_A, μ_A, λ_B, μ_B and $2/T$, are the state transition rates, given $1/T<<\lambda_A$, $1/T<<\mu_A$ and $\lambda_B<<1/T$ hold (see 3.1.23). T is the mean time while the system will be exposed to the risk (see 3.1.30).

Suppose some human activity contains a risk.

1) $1/\lambda_A$ is equal to the mean time while a worker stops working and takes a rest, and $1/\mu_A$ is equal to the mean time while he is at work;

2) $1/\lambda_B$ is equal to the mean time to occurrence of a mistake, given that he is at work, and $1/\mu_B$ is equal to the mean time while he stops working to correct his mistake;

3) T is the period of employment of the worker (however the transitions due to the period of employment, i.e., the risk exposure time, may be negligible if inequalities, $1/T<<\lambda_A$, $1/T<<\mu_A$ and $1/T<<\mu_B$, hold.)

In Figure 3 b) the final state is unrenewable, i.e., the final event does not repeat. In Figure 3 b) the constant event rates, λ_A, μ_A and λ_B, are the same as those in Figure 3 a) except the event rate μ_B (= 0). In this case, the final state means, for example, that a human is disabled.

In Figure 3 c), a transition is caused from the final state C to the initial state A, and constant event rate, m, is a constant renewal event rate (see 3.1.20 and 3.1.23). Here the final state also means, for example, that a human is disabled.

5.3 Final event frequency in a steady state

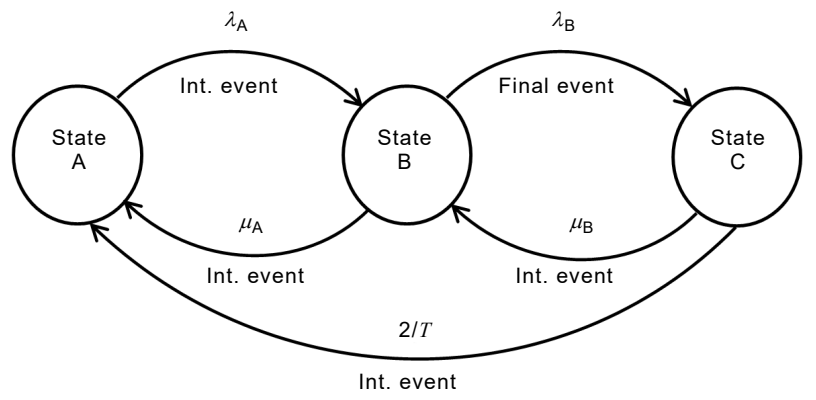
In Figure 3 a), FEF in a steady state, ω_R, is expressed in the following formula, given that the system is in a steady state [18]:

$$\omega_R = \lambda_B \, Pr\{B\} \tag{5}$$

where

$Pr\{B\}$ is the probability that the system is in system state B in a steady state in Figure 3 a).

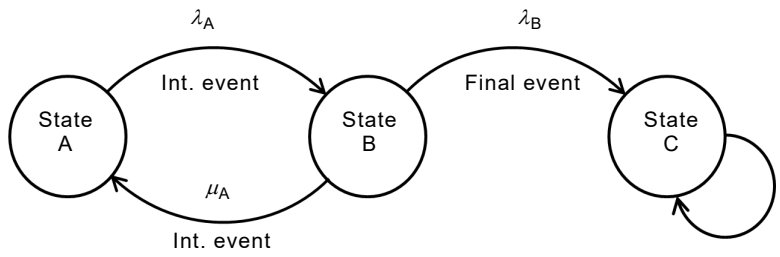
Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016



T: Risk-exposure time
λ_A, μ_A, λ_B, μ_B: State transition rates (but $1/T << \lambda_A$, $1/T << \mu_A$ and $\lambda_B << 1/T$)

IEC

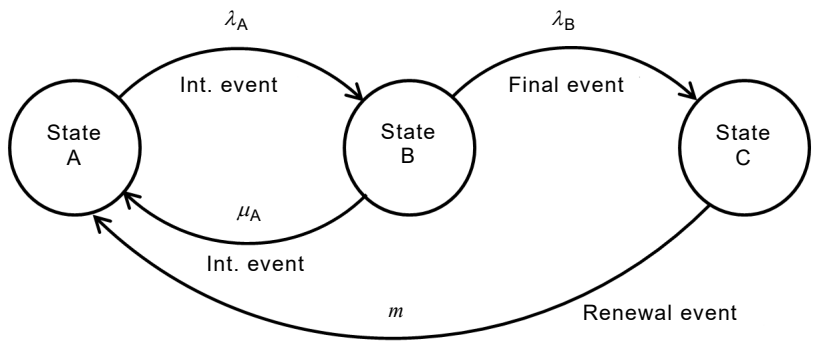
a) Model for a repeatable final event



λ_A, μ_A, λ_B: State transition rates

IEC

b) Model for an unrepeatable final event



λ_A, μ_A, λ_B, m: State transition rates

IEC

c) Model for a final state with renewal

System state A: Initial state (antecedent state)

System state B: Int. state (antecedent state)

System state C: Final state

Figure 3 – State transition models with various final states

In Figure 3 c), (unreal) FEF at initial state A, ω_{UA}, is given formally, assuming that the renewed system is identical to the original system (note that the renewed system is, however,

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

not the original system itself). The FEF at initial state A is then expressed in the following formula, given that the system is in a steady state [18]:

$$\omega_{UA} = \lambda_B Pr\{B\} \tag{6}$$

where

$Pr\{B\}$ is the probability that the system is in system state B in a steady state in Figure 3 c).

5.4 Final event rate at a given initial state and at a recognised state

In Figure 3 c), FER at initial state A, φ_A, is expressed by the following formula, given that the system is in a steady state and $Pr\{C\}$ is the probability that the system is in system state C at that time [18][27][29]:

$$\varphi_A = \omega_{UA}/(1-Pr\{C\}) \tag{7}$$

MTFE at initial state A, T_A, is (see 3.1.24) [18][27][29]:

$$T_A = 1/\varphi_A \tag{8}$$

In Figure 3 c), FER at recognised state B, φ_B, is expressed in the following formula by assuming a virtual state transition (i.e., virtual renewal event) from final state C to int. state B (i.e., recognised state B), and by putting FEF at recognised state B in ω_{UB} (see 3.1.26):

$$\varphi_B = \omega_{UB}/(1-Pr\{C\}) \tag{9}$$

MTFE at recognised state B, T_B, is given as (see 3.1.27):

$$T_B = 1/\varphi_B \tag{10}$$

5.5 Relationship between final event rate and frequency at a given initial state

If the sojourn time at state C of Figure 3 c) is infinite, i.e., $m \to 0$ (or m asymptotically approaches to 0), the renewable system becomes equivalent to the unrenewable system in Figure 3 b). The FER at a given initial state and FER at a recognised state do not contain the renewal event rate m and therefore they do not depend on the value of m. This means that the MTFE at a given initial state and MTFE at a recognised state in Figure 3 b) are equivalent to those in Figure 3 c) [18][27][29].

Thus, in the context of FER at a given initial state and FER at a recognised state, the system with an unrenewable final state is equivalent to the renewable system, given that the state transitions are exactly the same between those systems except the renewable feature.

For any renewable system with renewal event rate, m, let φ be FER at a given initial state (or a recognised state) and ω be FEF at a given initial state (or a recognised state) in a steady state of the system; thus the following generic relationship is useful [18][27][29]:

$$\varphi = \lim_{m \to \infty} \omega = \omega / \left(1 - P\{X\}\right) \tag{11}$$

where

$P\{X\}$ is the probability that the system is in final state X in a steady state.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

6 Procedure for probabilistic risk analysis and flow to reach risk profile

Checklists, what-if/analysis, HAZOP studies [11], FMEA [9], etc., are generally performed to identify risks that will be involved in a targeted system at first [4]. The targeted system may include industrial items each of which is often composed of thousands or more components and therefore the system could consist of thousands or more up or down states of the components. The risks of complex systems with such complex system states are analysed qualitatively and quantitatively by use of such techniques as FMEA, RBD [8], FTA and ETA, and the main mechanisms that are dominant over the causation of a final event will be found (see 9.1, 9.5 and Clause B.2). Those main mechanisms are often expressed for example by use of MCSs extracted through FTA.

The MCSs dominant over the occurrence of the final event are usually composed of several MCS elements, i.e., several basic elements (see 3.1.35). Namely the effect of the MCSs composed of a larger number of basic elements is often negligible compared to that of the MCSs composed of fewer basic elements from the quantitative point of view. For example, CCFs are often (but not always) dominant over the causation of final events from this point of view (see Annex A). The quantitative risk analysis will be performed rigorously and precisely to the MCSs with fewer basic elements by use of, for instance, state transition diagrams while each basic element such as a condition of a channel (Ch) may consist of up and down conditions of hundreds or more components (see 3.1.34 and 3.1.35). Thus the FER at a given initial state can be estimated for large-scale complex systems based on this MCS screening.

The procedure of risk analysis of technological systems involving estimation of FER at a given initial state for complex systems is (see Table 1, 9.1, 9.5, Clauses A.5 and B.3):

– identifying risks at first and analysing qualitatively the risks to find, for example, the MCSs composed of fewer basic elements that will be dominant over the causation of the final event, by use of such techniques as checklists, what-if/analysis, HAZOP studies, FMEA, RBD, ETA and FTA (details are out of the scope of this document);
– establishing analytical models for quantification, with due regard to the causation of the basic elements that are dominant over the occurrence of the final event from the quantitative point of view, by use of such techniques as ETA, FTA and Markov techniques;
– estimating FEF, FER, FEF at a given initial state, FER at a given initial state, FER at a recognised state and FER at a recognised group state for all system states of a state transition model, i.e., an analytical model that is composed of a set of basic elements;
– validating the modelling and analysis from the perspective of the types, measures, comprehensiveness and sequential causation of the events, the approximation, the event rate/frequency data sources, etc., (details are out of the scope of this document);
– repeating the analytical process if the analysis is not satisfactory;
– documentation (details are out of the scope of this document);
– handing over the results of the analyses to the risk-evaluation process.

The procedure for the analysis of the occurrence of final event is summarized in Figure 4.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016

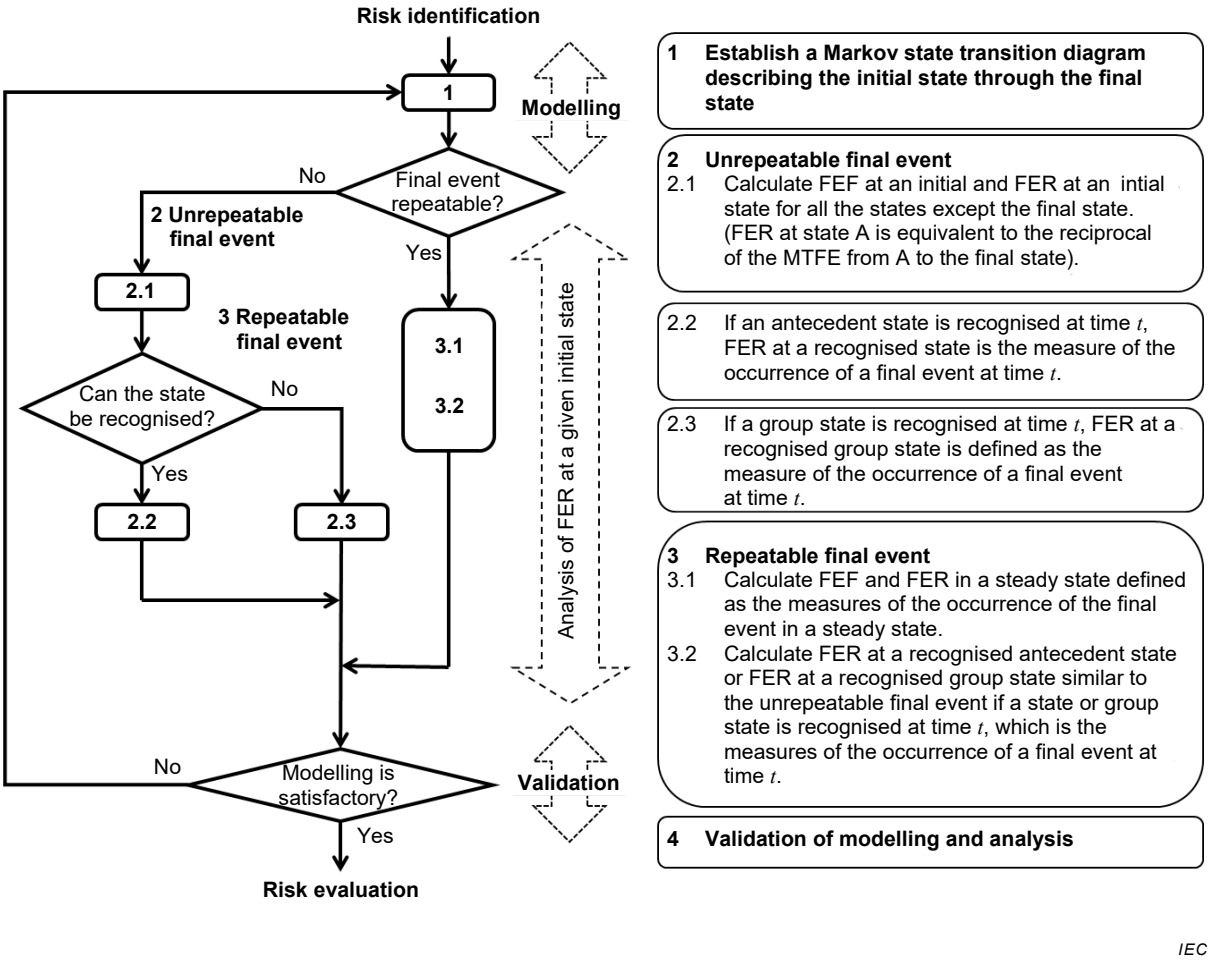


Figure 4 – Procedure for analysis of repeatable/unrepeatable final events

7 Techniques for quantitative analysis of the occurrence of a final event

7.1 Graphical symbols for three types of final events

7.1.1 General

It is important for the risk analysis of complex systems that such analytic techniques as the HAZOP, FMEA, RBD, FTA and Markov techniques should be applied complementarily. The causation of a final event is quantitatively analysed by using typically ETA, FTA and Markov techniques. However, conventional ETA and FTA techniques do not include symbols to classify (final) events as repeatable, renewable as well as unrepeatable types, which are necessary to extract the maximum synergy efficacy for the complementary use of those techniques. Thus this document newly introduces the symbols for ETA, FTA and Markov techniques as described in Table 2 to 5, illustrates the manner in which those symbols are to be used, and demonstrates the effectiveness of modified techniques on risk analysis in 7.2.

Basic symbols for ETA and FTA are shown in Table 2 to classify (final) events to Type 1 (repeatable), Type 2 (unrepeatable and renewable) and Type 3 (unrepeatable and unrenewable).

7.1.2 Repeatable final event

Table 3The symbols and graphical representations are illustrated in Table 3 for the estimation of the FEF of repeatable int. and final events by complementary use of ETA, FTA and Markov techniques. A risk is represented by initial state 1, int. states 2 and 3, and final state 4, as well as events 1→2, 2→1, 2→4, 4→2, 1→3, 3→1, 3→4 and 4→3 as shown in the event tree,

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 63039:2016