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 It also gives information on projects, replaced and withdrawn publications.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.

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.

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).

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).

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

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

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.

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:

$$\omega = 1/(T_a+T_b) \quad (1)$$

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:

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

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

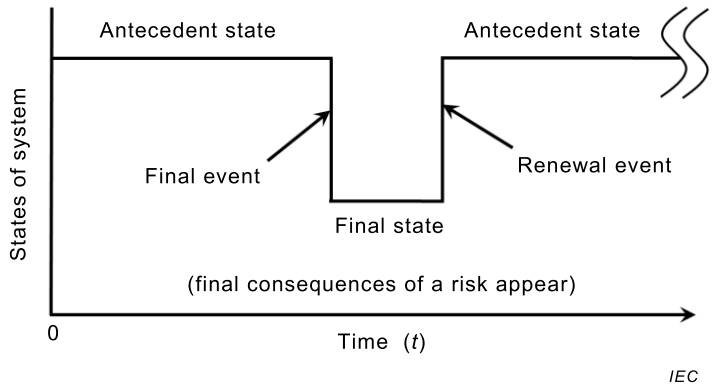


Figure 1 – Antecedent state, final event, final state and renewal event

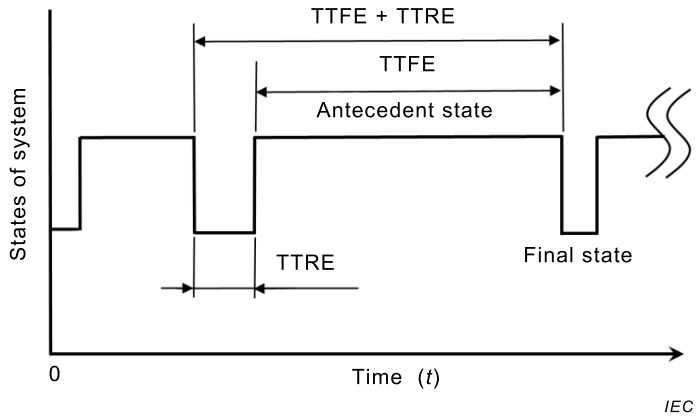


Figure 2 – Time to final event (TTFE) and time to renewal event (TTRE)

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.

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.

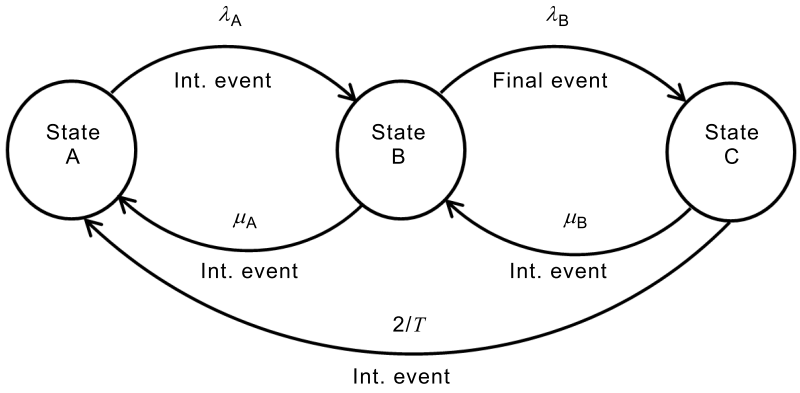
5.3 Final event frequency in a steady state

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

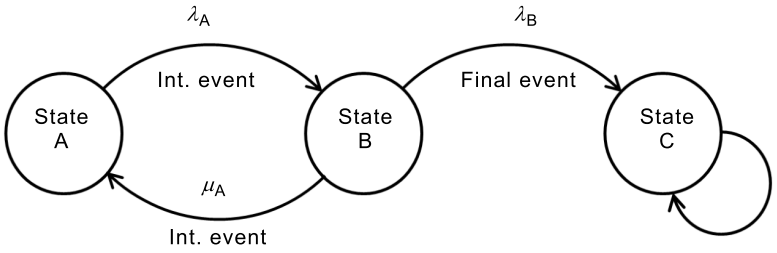
$Pr\{B\}$ is the probability that the system is in system state B in a steady state in Figure 3 a).



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

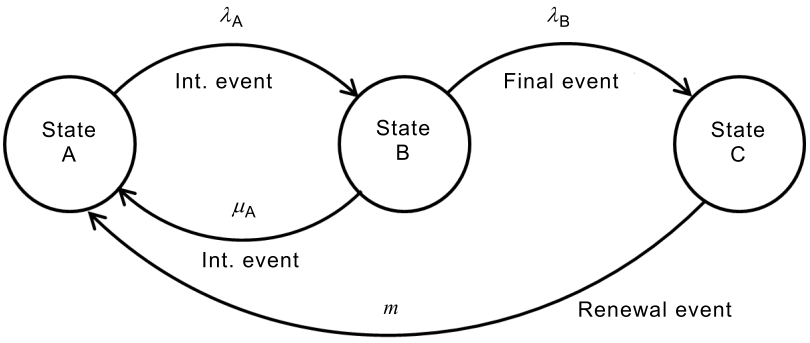
a) Model for a repeatable final event



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,

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]:

$$\omega_{UA} = \lambda_B Pr\{B\} \quad (6)$$

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]:

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

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

$$T_A = 1/\varphi_A \quad (8)$$

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):

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

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

$$T_B = 1/\varphi_B \quad (10)$$

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]:

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

where

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

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.

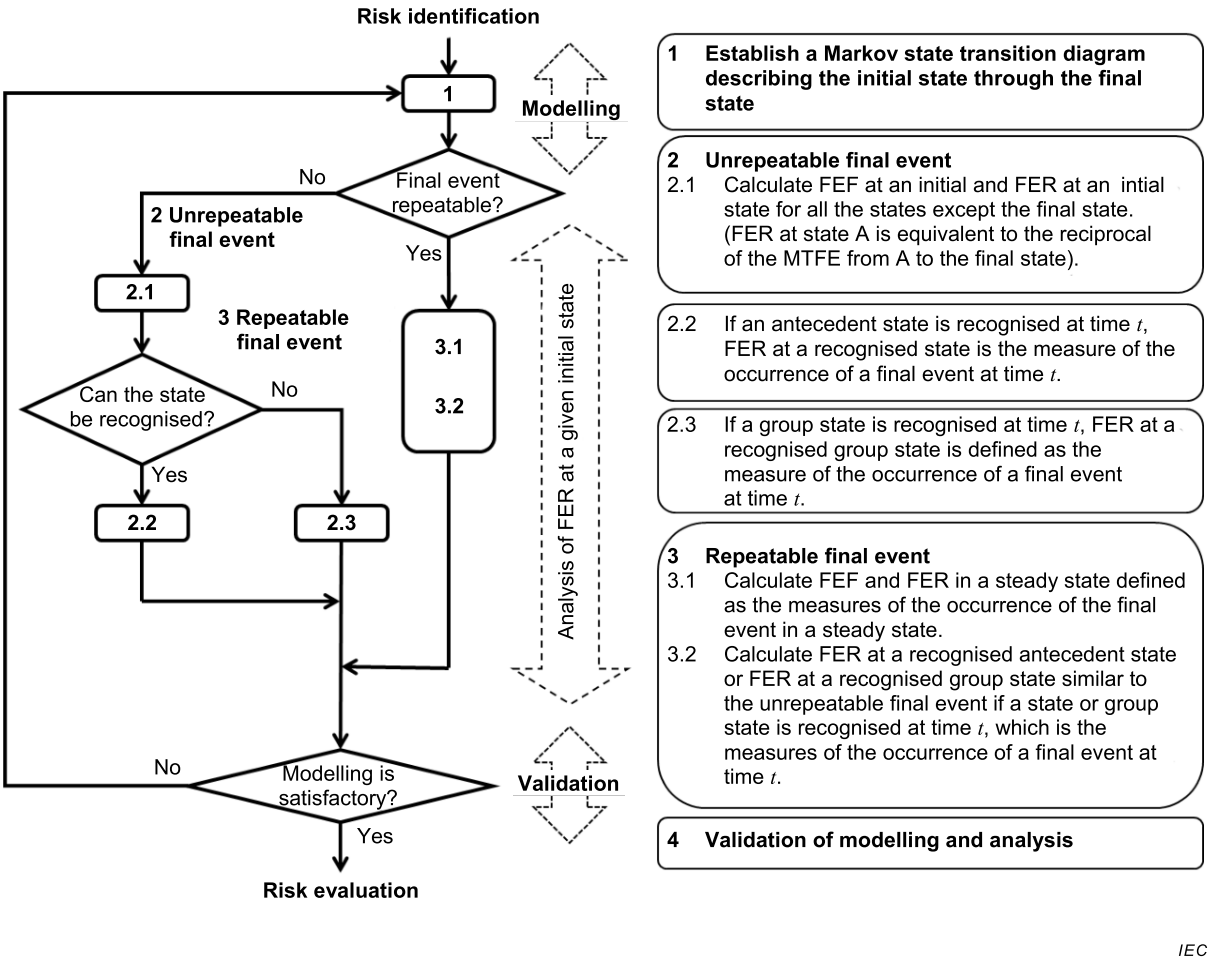


Figure 4 – Procedure for analysis of repeatable/unrepeatable final events

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,

FT and Markov state transition diagram in Table 3. Here, notation "$m \rightarrow n$ (m, n = 1, 2, …)" means the transition from system state m to system state n.

Concrete expressions for those system states and events are for instance illustrated in 7.2. Here final events are events 2→4 and 3→4. Those final events do not change any property of the risk and therefore do not change the occurrences of the paths from the initial to the final state.

A branch of the event tree, which has arrows at both ends, means that the event indicated by the branch can repeat. This branch is categorised as the repeatable branch of Type 1. The PAND gate with a triangle for the FT means that the output event of this PAND gate is repeatable. This is categorised as the PAND gate of Type 1.

Table 2 – Symbols newly introduced for event tree and fault tree analyses

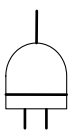
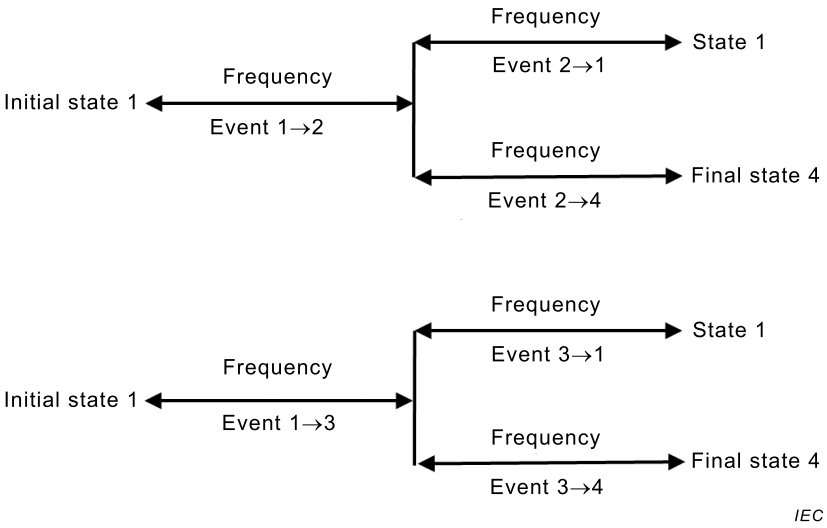
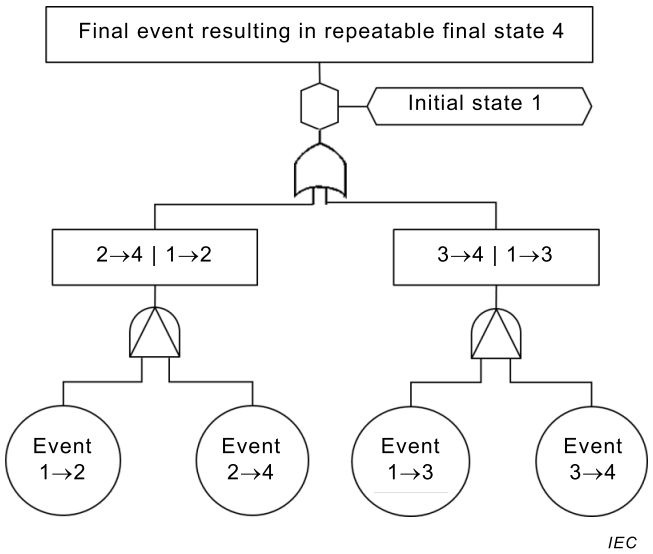
Symbols	Name	Description
◀ ▶	Repeatable branch of Type 1	The event of this branch in an event tree (ET) is repeatable.
▶	Unrepeatable branch of Type 2	The event of this branch in an ET is unrepeatable, and results in a renewable final state if this event is a final event.
▶	Unrepeatable branch of Type 3	The final event of this branch in an ET is unrepeatable and results in an unrenewable final state.
	PAND gate of Type 1	The output event of this PAND gate is repeatable (a combination of an AND gate and inhibit gate can be applied to an unrepeatable int. output event.)
	PAND gate of Type 2	The output event of this PAND gate is unrepeatable and results in a renewable final state.
	PAND gate of Type 3	The output event of this PAND gate is unrepeatable and results in an unrenewable final state.

Table 3 – Symbols and graphical representation for a repeatable (final) event

Techniques	Diagrams
ETA	
FTA	

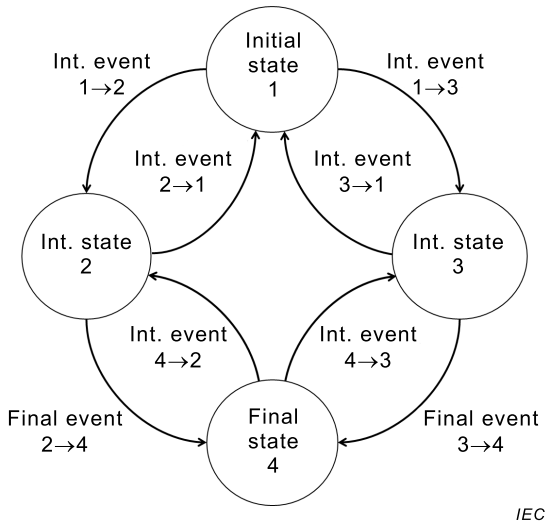
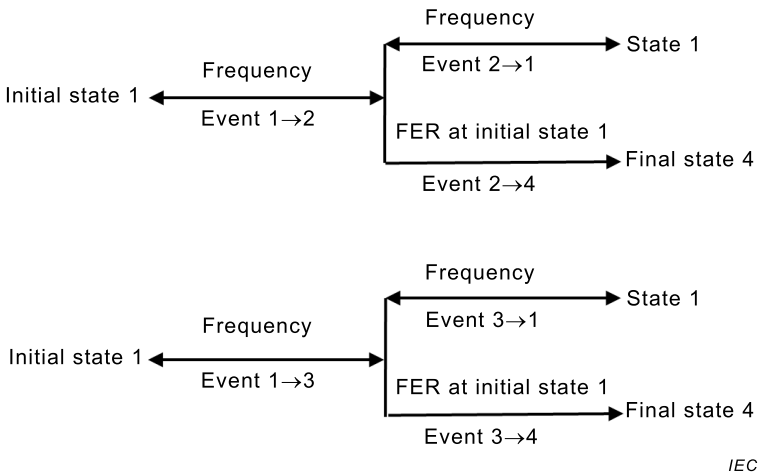
Techniques	Diagrams
Markov state transition	

Table 4 – Symbols and graphical representation for a renewable final state

Techniques	Diagrams
ETA	

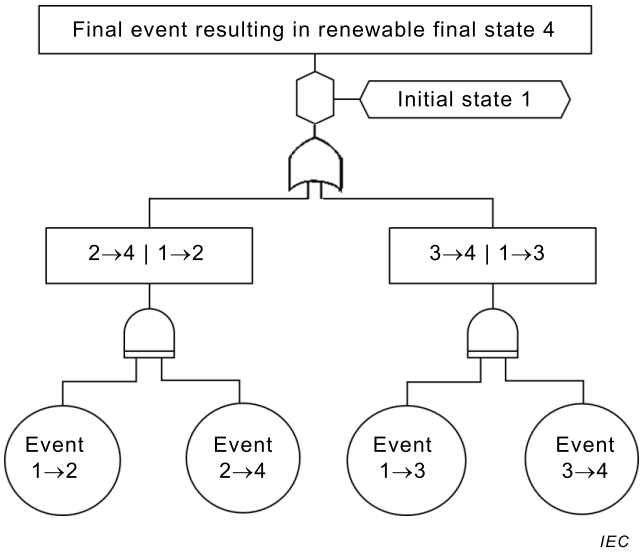
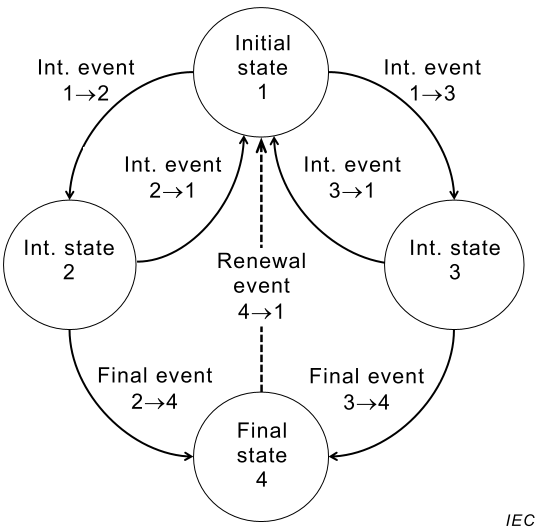
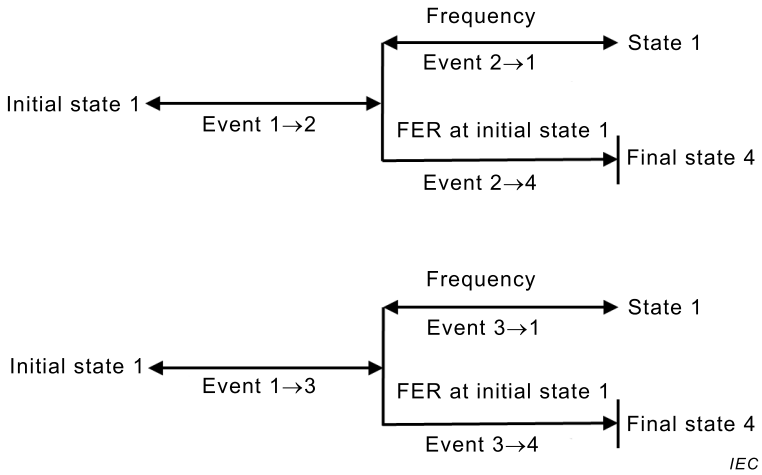
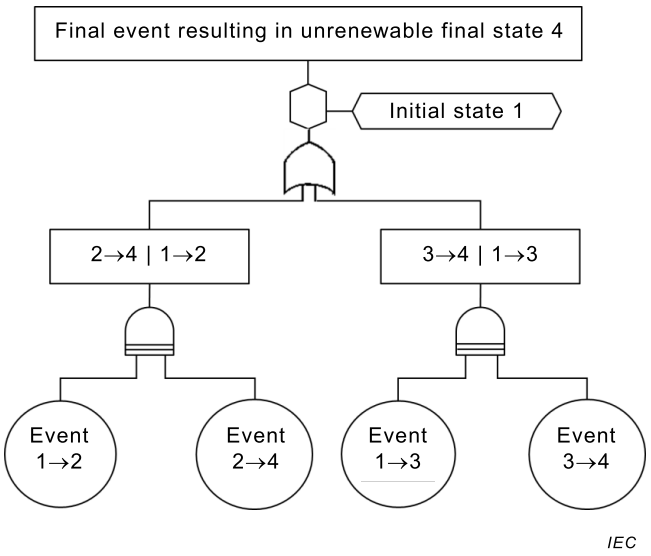
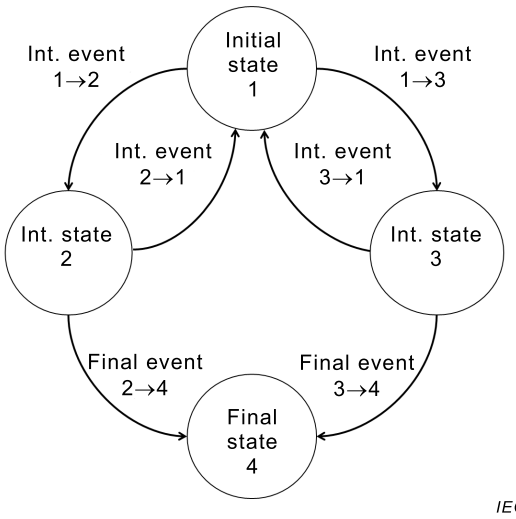
Techniques	Diagrams
FTA	
Markov state transition	

Table 5 – Symbols and graphical representation for an unrenewable final state

Techniques	Diagrams
ETA	
FTA	

Techniques	Diagrams
Markov state transition	

7.1.3 Unrepeatable final event resulting in a renewable final state

In Table 4 the symbols and graphical representations are illustrated for the estimation of FER at initial state 1 for an unrepeatable final event resulting in a renewable final state by use of the ETA, FTA and Markov techniques. A risk is represented similarly to Table 3 by initial state 1, int. states 2 and 3, and final state 4, and events 1→2, 2→1, 2→4, 1→3, 3→1, 3→4 and 4→1 as shown in the event tree, FT and Markov state transition diagram in Table 4.

Here events 2→4 and 3→4 are final events, and event 4→1 is a renewal event. The final event changes the risk, i.e., the ways from the initial state to the final state because the system state(s) of the overall system is(are) permanently changed by the final event and the similar risk cannot be retained as long as the overall system is not restructured.

The branch of the event tree in Table 4, which has an arrow at the right end, means that the event indicated by the branch brings about a renewable final state. This branch is categorised as the unrepeatable branch of Type 2. The PAND gate with a horizontal line in the FT diagram means that the output of the gate results in a renewable final state, and is categorised as the PAND gate of Type 2.

The FER at initial state 1 is calculated by use of those diagrams.

7.1.4 Unrepeatable final event resulting in an unrenewable final state

In Table 5 the symbols and graphical representations are illustrated for analysis of an unrepeatable final event resulting in an unrenewable final state by use of the event tree, FT and Markov state transition diagram. A risk is represented similarly to Table 3 by initial state 1, int. states 2 and 3, and final state 4, as well as events 1→2, 2→1, 2→4, 1→3, 3→1 and 3→4 as shown in Table 5. The final events are 2→4 and 3→4. The final events change the overall system so significantly that it will never be renewed any more.

The branch of the event tree in Table 5, which has both an arrow and a vertical line at the right end, means that the event of this branch results in an unrenewable final state, and is categorised as the unrepeatable branch of Type 3. The PAND gate with dual horizontal lines in the FT in Table 5 means that the output of the PAND gate results in an unrenewable final state, and is categorised as the PAND gate of Type 3.

Here, FER at initial state 1 is identical with the FER at initial state 1 obtained in 7.1.3 for the renewable system with the renewable final state (see 5.5).

7.2 Analytical example of an unrepeatable final event

7.2.1 General

Suppose a risk is represented by initial state A, int. states B and D, and final state C, as well as two paths through the initial state to the final state, A→B→C and A→D→C. Here, it is assumed that the final event is unrepeatable and only path A→B→C brings about the final state in which the final consequences of the risk appear (see 3.1.10, Note 1). In Figure 5 the causation of the unrepeatable final event is described. In the figure system state D is omitted because the final event through path A→D→C does not bring about any final state in which the final consequences of the risk appear. The causation of the final event is also modelled by use of the Markov state transition diagram described as in Figure 6.

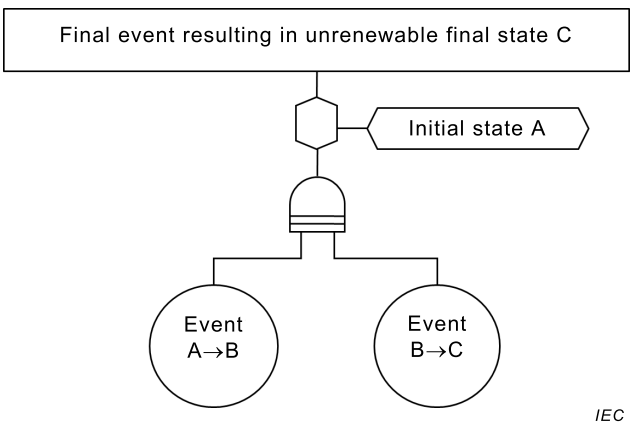
Two risks owing to the failure of an airbag control system for automobiles are identified at least [31]: 1) the airbag control system inflates its airbag unintentionally when the automobile is normally running, and, 2) the airbag control system fails to inflate the airbag when a collision occurs. Here, the airbag control system is typically composed of electrotechnical items such as sensors, controllers and actuators. The former risk, i.e., the risk of the unintentional inflation, can be cited as an actual example of the state transition model shown in Figure 6. In this case the risk is represented by the following system states of A to D in Figures 5 and 6.

A automobile is stationary and the airbag control system is UP;

B automobile is running and the airbag control system is UP;

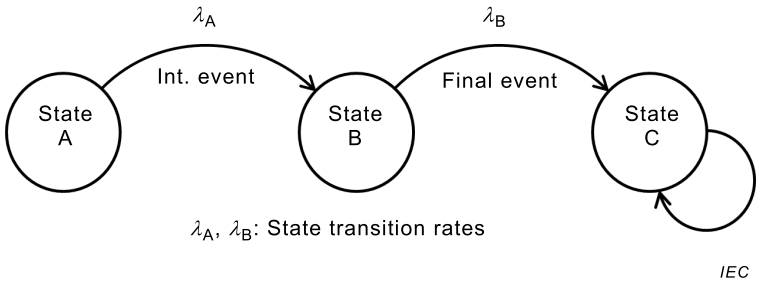
C automobile is running and the airbag has been inflated unintentionally;

D automobile is stationary and the airbag has been inflated unintentionally.



NOTE System state D is omitted from the figure.

Figure 5 – FT for an unrepeatable final event resulting in an unrenewable final state



System state A: Initial state (antecedent state)

System state B: Int. state (antecedent state)

System state C: Final state

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

If the airbag control system inflates its airbag unintentionally in system state B, a state transition B to C is caused and this could bring about a traffic accident to an overall system that includes a driver and traffic circumstances. The causation of state transition from A to C corresponds with the path A→B→C in the model.

Whereas if the unintended inflation of the airbag occurs in system state A, a state transition A to D is caused. However similar traffic accidents will not occur even if a state transition D to C occurs, because the airbag cannot be inflated while the automobile is running, i.e., a wrecker is pulling the damaged automobile to an auto repair shop. This event sequence is represented by the path A→D→C as mentioned above. Thus, the final event that can cause a traffic accident is the unintended inflation of the airbag when the automobile is running, i.e., state transition from B to C only. This final event is also called a critical event [7].

Here, the start of a running state of the automobile is the demand to activate the function of the airbag control system to prevent unintended inflation from occurring because the unintended inflation can result in a traffic accident. Thus the system state B is regarded as the demand state for the function of the airbag control system to prevent the airbag from inflating unintentionally and dangerously.

In Figure 6, if it can be assumed that the demand and failure of the airbag control system occur at random and independently of time, then the constant event rates, λ_A [1/h] and λ_B [1/h], are assigned to the demand rate and the failure rate for the function of the airbag control system, respectively (see 9.3.1 b)).

7.2.2 Average final event frequency

Suppose that an overall system in which a risk is represented by Figure 5 and Figure 6 is in initial state A at time 0, and probabilities that the overall system will be in system state A and B at time t, given that neither state transition B to A nor D to A occurs during [0, t], are $P_{A,A}(t)$ and $P_{A,B}(t)$, respectively, then those probabilities are expressed in the following equations:

$$P_{A,A}(t) = \{\exp(-\lambda_A t)\}\exp(-\lambda_B t) \quad (12)$$

$$P_{A,B}(t) = \{1-\exp(-\lambda_A t)\}\exp(-\lambda_B t) \quad (13)$$

where

t is the time;

λ_A is the demand rate, i.e., constant state transition rate from A to B (and D to C) [1/h];

λ_B is the failure rate, i.e., constant state transition rate from B to C (and A to D) [1/h].

The frequency of the final event that results in the final consequences of the risk, $\omega_A(t)$ [1/h], is expressed in the following equation, given that the system is in initial state A at time 0 and neither state transition B to A nor D to A occurs during [0, t]:

$$\omega_A(t) = \omega_{ABC}(t)$$

$$= \lambda_B P_{A,B}(t) = \lambda_B\{1-\exp(-\lambda_A t)\}\exp(-\lambda_B t) \quad (14)$$

where

$\omega_{ABC}(t)$ is the frequency of the final event caused by path A→B→C [1/h].

It is noted that the frequency of the final event caused by path A→D→C, $\omega_{ADC}(t)$, does not contribute to $\omega_A(t)$, because this final event does not bring about any final state in which the final consequences of the risk appear, namely, $\omega_A(t) = \omega_{ABC}(t)+\omega_{ADC}(t) = \omega_{ABC}(t)$ holds.

The average FEF derived from Equation (14), $\omega_A(0,T)$ [1/h], is expressed as (see 3.1.22 and 3.1.30):

$$\omega_A(0,T) = \omega_{ABC}(0,T) = (1/T)[1-\exp(-\lambda_B T)-\{\lambda_B/(\lambda_A+\lambda_B)\}[1-\exp\{-(\lambda_A+\lambda_B)T\}]]$$

$$= (1/T)[\{\lambda_A/(\lambda_A+\lambda_B)\}-\exp(-\lambda_B T)+\{\lambda_B/(\lambda_A+\lambda_B)\}\exp\{-(\lambda_A+\lambda_B)T\}] \quad (15)$$

where

$\omega_{ABC}(0,T)$ is the average frequency of the final event caused by path A→B→C [1/h];

T is the risk exposure time [h] (see 3.1.30).

The following a) to e) can be said on the FEF, i.e., $\omega_A(t) = \omega_{ABC}(t)$, and the average FEF, i.e., $\omega_A(0,T) = \omega_{ABC}(0,T)$, from Equations (14) and (15).

a) If $\lambda_A t << 1$ and $\lambda_B t << 1$, then $\omega_A(t) \approx \lambda_A \lambda_B t$.

If $1 << \lambda_A t$ and $\lambda_B t << 1$, then $\omega_A(t) \approx \lambda_B$.

If $0 < t < (1/\lambda_A)\ln\{(\lambda_A+\lambda_B)/\lambda_B\}$, then $\omega_A(t)$ tends to its maximum value of $\lambda_B[1-\exp[-\ln\{(\lambda_A+\lambda_B)/\lambda_B\}]]\exp[-(\lambda_B/\lambda_A)\ln\{(\lambda_A+\lambda_B)/\lambda_B\}]$.

If $(1/\lambda_A)\ln\{(\lambda_A+\lambda_B)/\lambda_B\} < t$, then $\omega_A(t)$ tends to 0.

b) If $\lambda_A T << 1$ and $\lambda_B T << 1$, then $\omega_A(0,T) \approx \lambda_A \lambda_B T/2$.

c) If $1 << \lambda_A T$ and $\lambda_B T << 1$, then $\omega_A(0,T) \approx \lambda_B$.

IEC 61508 (all parts) is, for instance, a risk-based functional safety standard series and specifies safety integrity, i.e., an average failure frequency (PFH) of a safety-related item as the target failure measure of the item to control and/or reduce a risk(s) in a high demand mode of or continuous mode operation, based on this approximate formula of average FEF, $\omega_A(0,T) \approx \lambda_B$ (see 3.1.33 and Clause B.1). Here λ_B is the dangerous failure rate of the safety-related item that is the target failure measure for the safety integrity of the item (see Clause B.2). It is noted the demand completion rate is not supposed in IEC 61508 (all parts).

d) If $0 < T < T^*$, then $\omega_A(0,T)$ tends to its maximum value of $(1/T^*)[\{\lambda_A/(\lambda_A+\lambda_B)\}-\exp(-\lambda_B T^*)-\{\lambda_B/(\lambda_A+\lambda_B)\}\exp\{-(\lambda_A+\lambda_B)T^*]$, where T^* is the value that satisfies Equation (16):

$$\exp(-\lambda_B T^*)-\{\lambda_B/(\lambda_A+\lambda_B)\}\exp\{-(\lambda_A+\lambda_B)T^*\}+\lambda_B T^*[\exp(-\lambda_B T^*)-\exp\{-(\lambda_A+\lambda_B)T^*\}] = \lambda_B/(\lambda_A+\lambda_B). \quad (16)$$

e) If $T^* < T$, then $\omega_A(0,T)$ tends to 0.

7.2.3 Final event rate at a given initial state

If an overall system is exposed to the risk as represented by Figure 5 and Figure 6 for risk exposure time T, the FER at initial state A, i.e., the reciprocal of the mean time from initial state A to final state C (i.e., the reciprocal of the mean time from t = 0 to occurrence of the unrepeatable final event), should be estimated.

Causation of a final event in an overall system with renewal is modelled in Figure 7 and Figure 8 in which system states A, B, C and D, which is omitted, have the same features as those in Figure 6, respectively. If the average duration of the demand state is τ hours and the completion can be modelled to occur at constant completion rate, $1/\tau$ [1/h], then the FEF at initial state A and FER at initial state A can be formulated by use of those models described in Figure 7 and Figure 8.

Suppose that the probabilities that the overall system will be in system state A, B and C in a steady state are $P_{A,A}$, $P_{A,B}$ and $P_{A,C}$, respectively. Then, $P_{A,A}$, $P_{A,B}$ and $P_{A,C}$ are expressed in the following equations for constant renewal event rate m [1/h] (see 9.3.1 b)):

$$P_{A,A} = (\lambda_A+1/\tau)(\lambda_B+1/\tau)/\{(\lambda_A+1/\tau)(\lambda_B+1/\tau)+\lambda_A(\lambda_A+1/\tau)(1+\lambda_B/m)+\lambda_B(\lambda_B+1/\tau)(1+\lambda_A/m)\} \quad (17)$$

$$P_{A,B} = \{\lambda_A/(\lambda_B+1/\tau)\}P_{A,A} \quad (18)$$

$$P_{A,C} = [\{\lambda_A/(\lambda_B+1/\tau)\}(\lambda_B/m)+\{\lambda_B/(\lambda_A+1/\tau)\}(\lambda_A/m)]P_{A,A} \quad (19)$$

The FEF at initial state A in which the final consequences of the risk appear, ω_A, of which reciprocal is the mean time from initial state A to the first renewal event described as in Figure 8, is easily formulated, given that risk exposure time is T (see 3.1.30 and 5.3):

$$\omega_A = \omega_{ABC}$$

$$= \lambda_B P_{A,B} = \lambda_B\{\lambda_A/(\lambda_B+1/\tau)\}(\lambda_A+1/\tau)(\lambda_B+1/\tau)/\{(\lambda_A+1/\tau)(\lambda_B+1/\tau)+\lambda_A(\lambda_A+1/\tau)(1+\lambda_B/m)$$

$$+\lambda_B(\lambda_B+1/\tau)(1+\lambda_A/m)\} \quad (20)$$

where

ω_{ABC} is FEF at initial state A, where the final event occurs on path A→B→C [1/h].

Similarly, it is noted that FEF at initial state A that results from the final event caused by path A→D→C, ω_{ADC} [1/h], does not contribute to ω_A, namely, $\omega_A = \omega_{ABC}+\omega_{ADC} = \omega_{ABC}$ holds.

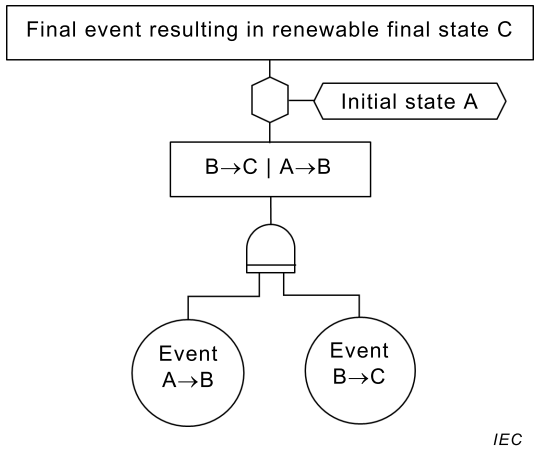


Figure 7 – FT for an unrepeatable final event resulting in a renewable final state

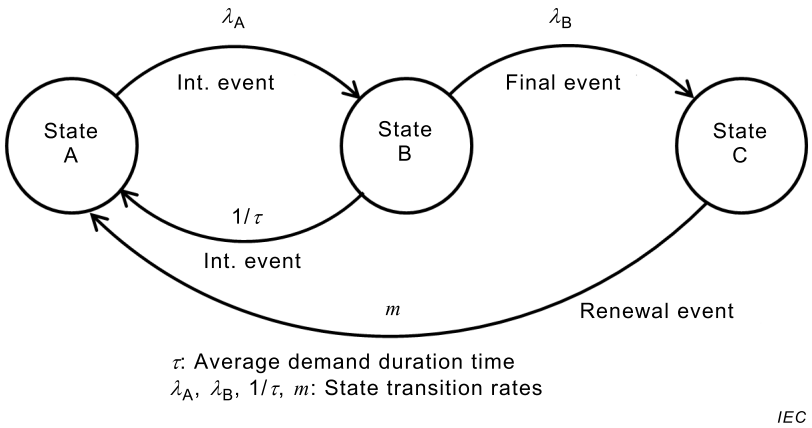


Figure 8 – State transitions resulting in a renewable final state

FER at initial state A, φ_A, of which reciprocal is the mean time from initial state A to final state C in Figure 7 and Figure 8, as well as the mean time from A to C in Figure 5 and Figure 6, is easily formulated from Equation (20), given that risk exposure time is T:

$$\varphi_A = \varphi_{ABC}$$

$$= \omega_{ABC}/\{1-P_{A,C}\}$$

$$= \lambda_A\lambda_B/[(\lambda_B+1/\tau)\{1+\lambda_A/(\lambda_B+1/\tau)+\lambda_B/(\lambda_A+1/\tau)\}] \quad (21)$$

where

φ_{ABC} is FER at initial state A, where the final event occurs on path A→B→C [1/h].

Similarly, it is noted that FER at initial state A that results from the final event caused by path A→D→C, φ_{ADC}, does not contribute to φ_A, i.e., $\varphi_A = \varphi_{ABC}+\varphi_{ADC} = \varphi_{ABC}$ holds.

The following a) to c) can be said from Equation (21).

a) If $\lambda_A\tau<<1$ and $\lambda_B\tau<<1$, then $\varphi_A = \varphi_{ABC}\approx\lambda_A\lambda_B\tau$. This approximate formula is identical with that of average FEF, given that $\tau = T/2$ holds (see 7.2.2 b), 9.3.2 and Annex B).

   In the context of the airbag control system, it is clear for path A→B→C that the probability $\varphi_A/\lambda_B = \varphi_{ABC}/\lambda_B\approx\lambda_A\tau$ is the approximate average probability that the overall system is in

the demand state for the airbag control system when a failure of the airbag control system occurs. On the other hand, it is also clear for path A→B→C that the ratio, $\varphi_A/\lambda_A = \varphi_{ABC}/\lambda_A \approx \lambda_B\tau$, is the approximate probability that a failure of the airbag control system occurs within the mean time interval of the demand state [0, τ], given that a demand occurred at time 0. Namely, $\varphi_{ABC}/\lambda_A \approx \lambda_B\tau$ is equal to APF_{drg}, i.e., $\varphi_{ABC}/\lambda_A \approx \lambda_B\tau \approx P_b$.

However, it is believed in IEC 61508 (all parts) that only path A→D→C can bring about a final event that results in the appearance of the final consequences of risk by the failure of the item in the low demand mode of operation. Namely $\varphi_{ABC} \equiv 0$ is assumed. The FER (or HER in IEC 61508 (all parts)), φ, is the target measure of occurrence of the final event for the item in the low demand mode operation, and is defined only by the approximate formula, $\varphi \approx \lambda_B\lambda_A\tau \approx \varphi_{ADC}$, i.e., $\varphi \approx \lambda_A\lambda_B\tau \approx \lambda_A P_a$, where λ_A and λ_B are the demand rate of the item and the (dangerous) failure rate of the item, respectively (see 9.3.2 and Annex B).

If the final event is brought about only by the demand that occurs in a fault of an item, i.e., the final event occurs only on path A→D→C, then the probability, $\varphi_A/\lambda_A = \varphi_{ADC}/\lambda_A \approx \lambda_B\tau = \lambda_B T/2$, is the approximated average probability that the item is in a fault at time t ($0<t\leq T$), given that the item is in an up state at time zero and $\lambda_B T/2 << 1$ holds.

This approximated average probability, $\lambda_B\tau = \lambda_B T/2 (= P_a)$, is defined as “average probability of failure on demand (PFD_{avg})” in IEC 61508. Currently only PFD_{avg} is the target failure measure of SIL for the item in the low demand mode of operation as mentioned above. Thus, IEC 61508 (all parts) cannot cover such specific items as the airbag control systems illustrated above if those systems work in the low demand mode of operation (see 9.3.2 and Annex B).

b) If $1 << \lambda_A\tau$ and $\lambda_B\tau << 1$, then $\varphi_A = \varphi_{ABC} \approx \lambda_B$ holds. This approximation is identical with that of the average FEF (see 7.2.2 c), 9.3.2 and Annex B).

c) If $1 << \lambda_A\tau$ and $1 << \lambda_B\tau$, then $\varphi_A (= \varphi_{ABC})$ tends to $\lambda_A/(1+\lambda_A/\lambda_B+\lambda_B/\lambda_A)$. This characteristic is quite different from that of the average FEF (see 7.2.2 d) and e), and Annex B).

In case of the airbag control system cited above, system state B in Figure 5 to Figure 8, in which the automobile is running, is the demand state for the function of the airbag control system to prevent the airbag from inflating unintentionally. Thus, those int. events from system state A to B and B to A in Figure 8 are a demand and a completion, respectively. Suppose that the occurrences of int. events follow exponential distributions, and the average duration of the demand state is τ hours, then a completion can be modelled to occur at the constant rate of $1/\tau$ [1/h]. This constant rate is defined as the completion rate of the demand state. Namely $2/T = 1/\tau$ holds in this case, and therefore it can be known that 2τ hours should be allocated to risk exposure time T for the airbag control system above. Here it is noted again that the completion rate is not considered in IEC 61508 (all parts).

If the airbag control system is analysed in accordance with IEC 61508 (all parts), two extreme target measures for an item to control and/or reduce a risk are to be considered as described above. For instance, approximate HERs are $\varphi \approx \lambda_B\lambda_A T/2 \approx \varphi_{ADC}$ and $\varphi \approx \omega_A(0,T) \approx \lambda_B$ for the 1-out-of-1 architecture items in the low demand mode of operation and in the high demand mode of/continuous operation, respectively. Thus the target measure PFD_{avg} for the former is equal to $\varphi/\lambda_A \approx \lambda_B T/2 (= P_a)$, and the target measure for the latter PFH is equal to $\omega_A(0,T) \approx \lambda_B$ (see 3.1.32, 3.1.33, and Clause B.1), respectively.

However, the approximate HER, $\varphi \approx \lambda_B\lambda_A\tau \approx \varphi_{ADC}$, and therefore PFD_{avg} (that is equal to $P_a = \varphi/\lambda_A \approx \lambda_B\tau$) cannot be derived in the context of the risk of unintended inflation of an air bag owing to the failure of the airbag control system, because actually the path A→D→C will not bring about any final state in which the final consequences of the risk appear.

The FER at a given initial state presents a resolution to cope with the PFD_{avg} issue in the functional safety by introducing a new target measure for the item to reduce and/or control a risk in the low demand mode of operation. This new target measure is the risk-reduction ratio, φ_A/λ_A, where φ_A is the FER at a given initial state and λ_A is the demand rate. In general, it can be said that the formula of the risk-reduction ratio (e.g., $\varphi_A/\lambda_A = (\varphi_{ABC}+\varphi_{ADC})/\lambda_A$) is nearly equal to the sum of APF_{drg} and PFD_{avg} in the low demand mode of operation. Thus, if $\varphi_{ADC} = 0$ holds, the risk-reduction ratio, $\varphi_A/\lambda_A = \varphi_{ABC}/\lambda_A$, is nearly equal to APF_{drg}. Whereas if $\varphi_{ABC} = 0$ holds, then the risk-reduction ratio is nearly equal to PFD_{avg}. Thus, the risk-

reduction ratio of φ_A/λ_A can cover the PFD_{avg} and APF_{drg} for both paths A→B→C and A→D→C (see 9.3.2, Clauses B.4, B.5, B.6 and B.7). Numerical analyses are illustrated with the following examples.

1) Suppose a driver drives his private car, where state transition rates are, λ_A = 0,1 [1/h] (i.e., the driver begins to drive his car each 10 hours on average), $1/\tau$ = 2,0 [1/h] (i.e., the car is running for 30 minutes on average) and $\lambda_B = 1{,}0 \times 10^{-5}$ [1/h]. Then the low demand mode of operation will be preferred for analysis of the risk control and the reduction performed by this airbag control system, because the demand frequency, $1/(1/\lambda_A+\tau)\approx 0{,}1$ [1/h], is lower compared to the reciprocal of the risk exposure time $1/T = 1/(2\tau) = 1{,}0$ [1/h]. Thus the approximate formula gives the estimation, $\varphi_A = \varphi_{ABC} \approx \lambda_A\lambda_B\tau = 5{,}0 \times 10^{-7}$ [1/h]. Exact estimations $\varphi_A = \varphi_{ABC} = 4{,}8 \times 10^{-7}$ [1/h] and $\omega_A(0,2\tau) = \omega_{ABC}(0,2\tau) = 4{,}7 \times 10^{-7}$ [1/h] are calculated from Equations (21) and (15), respectively. The approximate formula provides a good approximation.
2) Another example is of a taxi being driven at more frequent intervals, λ_A = 2,0 [1/h] (i.e., the driver begins to drive each 30 minutes on average), $1/\tau$ = 2,0 [1/h] (i.e., same as in 1)) and $\lambda_B = 1{,}0 \times 10^{-6}$ [1/h]. The demand frequency, $1/(1/\lambda_A+\tau) = 1{,}0$ [1/h], seems to be on a dividing line between two modes of operation in comparison with $1/T$ = 1,0 [1/h]. Approximate formulas are $\varphi_A = \varphi_{ABC} \approx \lambda_A\lambda_B\tau = 1{,}0 \times 10^{-6}$ [1/h] (low demand mode of operation) and $\omega_A(0,2\tau) = \omega_{ABC}(0,2\tau) \approx \lambda_B = 1{,}0 \times 10^{-6}$ [1/h] (high demand mode of operation), while the exact estimations are $\varphi_{ABC} = 5{,}0 \times 10^{-7}$ [1/h] and $\omega_A(0,2\tau) = 5{,}7 \times 10^{-7}$ [1/h] from Equations (21) and (15), respectively. In this case, the approximate formulas $\varphi_A \approx \varphi_{ABC} \approx \lambda_A\lambda_B\tau$ and $\omega_A(0,2\tau) \approx \omega_{ABC}(0,2\tau) \approx \lambda_B$ provide the approximations about two times greater than the exact estimations (see Clause B.4).

It is noted that the airbag control system assumed above is a 1-out-of-1 architecture system. However real airbag control systems may have a feature of redundancy and be structured in a more complicated way. Malfunctioning parts of the system will be detected automatically and the system may cause transition to a safe shutdown state in order to be repaired. In addition, the causation process of harm brought about by unintended inflation of an airbag might be considered for real risk analysis. The FTs and state transition models described in Figure 5 to Figure 8 should be modified and/or remodelled more realistically for such analyses.

Figure 9 and Figure 10 describe a practical example of the hazard, i.e., the causation process of unintended inflation of an airbag due to malfunctioning of an airbag control system [31]. Here, the airbag control system is supposed to be a 1-out-of-2 architecture system, i.e., this system is composed of two independent Chs, Ch 1 and Ch 2. Not only detected (D) failures but also undetected (UD) failures occur in each Ch, and both Chs have equivalent D failure rates, λ_D, and equivalent UD failure rates, λ_{UD}, respectively (see 9.3.1 b)). The safe system state is invariable against this unintended inflation hazard (or risk) that is reciprocal to that caused by the failure of the airbag control system to inflate the airbag when a collision occurs (see Clause B.2).

If a D fault of any Ch is detected by the self-diagnosis function of the system, the sensor and control part causes the airbag control system to a safe shutdown state and alarms the driver immediately, in which case any unintended inflation cannot occur. However, if both Chs fall into the UD faults when the automobile is running, then the sensor and control part fails to prevent an unintended inflation of the airbag and a traffic accident can occur.

The CCF between both Chs are not represented in Figure 9 and Figure 10 because those failures can be analysed separately from the independent failures for simplicity of analysis. Risk exposure time is here assumed to be a proof test interval if the proof test exists, or a lifetime of the airbag control system if it does not exist. The probabilities of system states A to G in Figure 10, P_A to P_G, are easily calculated, given that the system is in a steady state. FER at initial state A, φ_A, is also obtained easily from the formula $\varphi_A = \lambda_{UD}P_C/(1-P_G)$ [31].

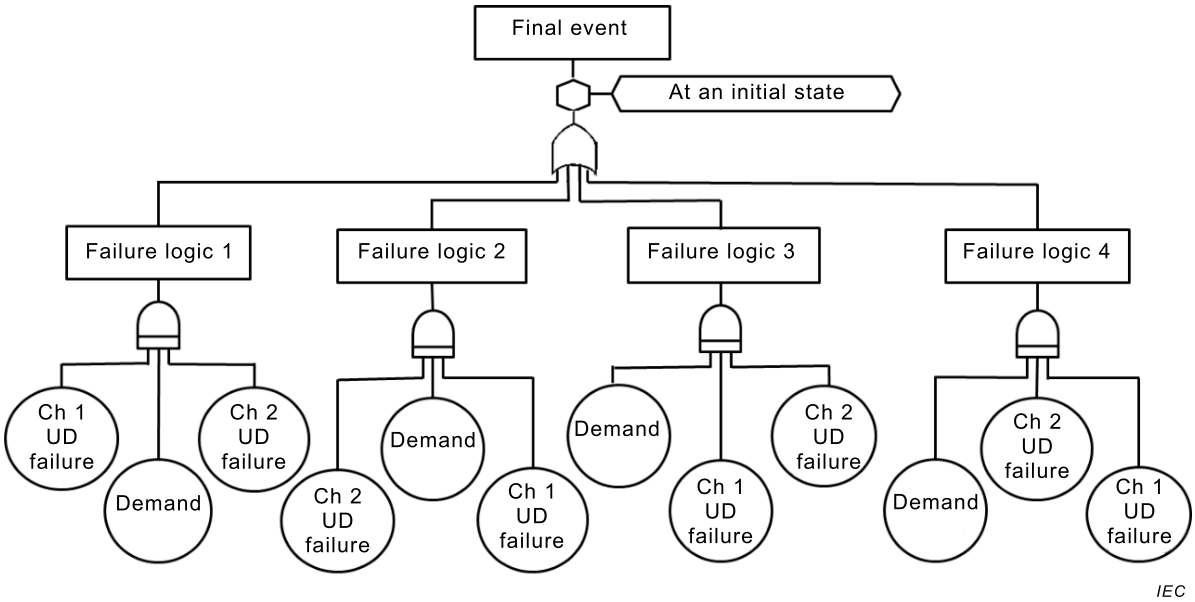
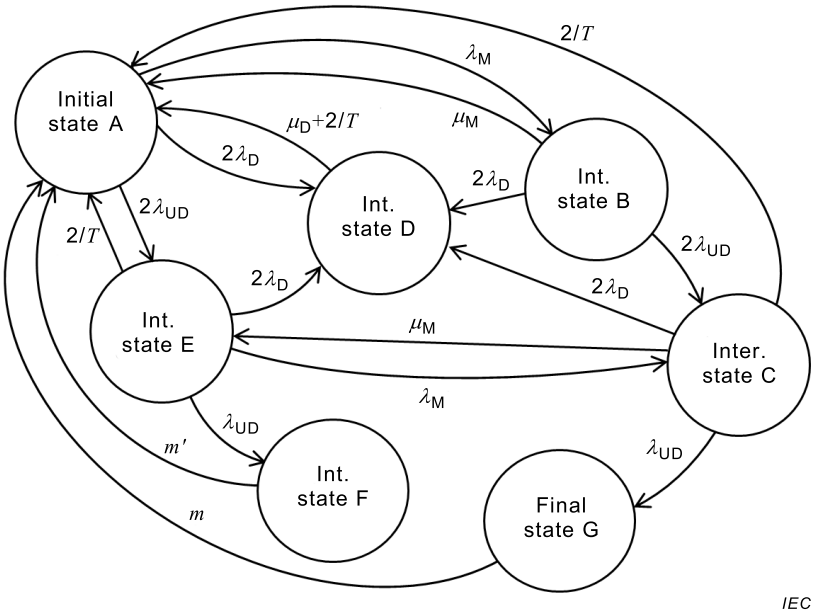


Figure 9 – FT for unintended inflation of an airbag due to failure of control



System states

A : Both Chs are up when the automobile halts;

B : Both Chs are up when the automobile is running;

C : One Ch is in a UD fault when the automobile is running;

D : Airbag control system is in shutdown owing to detection of a D fault;

E : One Ch is in a UD fault when the automobile halts;

F : Unintended inflation of airbag when the automobile halts;

G : Unintended inflation of airbag when the automobile is running.

State transition rates

λ_{UD} : UD failure rate of the Ch of airbag control system;

λ_D : D failure rate of the Ch of airbag control system;

μ_D : repair rate of the shutdown state;

λ_M : demand rate;

μ_M : completion rate;

m' : repair rate of the unintended inflation when the automobile halts;

m : renewal rate;

T : risk exposure time (but $1/T << \mu_M$ and $1/T << m'$).

Figure 10 – State transition model of unintended inflation of an airbag

Thus, the analytical technique of FER at a given initial state X, φ_X, covers a wide range of issues in risk analysis involving those that cannot be handled by use of conventional techniques. The new target measures of the occurrence of an unrepeatable final event, i.e., the FEF at a given initial state, ω_A, and FER at a given initial state, φ_A, are quite different from any one of the conventional dependability target measures such as a failure rate, failure frequency, reliability, unreliability, availability and unavailability of items because not only the up and down states of the items but also the demand and non-demand states, shutdown states, final consequences of a risk, other environmental conditions as well as risk exposure time that have not been applied to conventional dependability analyses are generally involved in the formulation of ω_A and φ_A.

In general, for example, if the risk exposure time T is not too long and state transition rates are not too high, namely, if $\lambda_A T << 1$ and $\lambda_B T << 1$, or, $1 << \lambda_A T$ and $\lambda_B T << 1$ hold in the example

shown in Figure 6, the average FEF may be nearly equal to the FER at a given initial state. However, they are not identical, and if risk exposure time T becomes too long the former tends to 0. This is the reason why the average FEF is seldom suitable for the target measure of the occurrence of unrepeatable final events (see Clauses 4 and B.4).

Thus, the risk of the unintentional inflation of the airbag when the automobile is normally running and the risk of the misfire of the airbag when a collision occurs (of which analysis is omitted in this document) due to the failure of the control system can be analysed separately in order to create a risk profile for the next stage of risk assessment [31].

8 Final event rate at a recognised state and recognised group state

8.1 General

Antecedent states should be monitored continuously in an overall system in order to conform to ISO 31000 [3]. If an antecedent state or a group of antecedent states is recognised and designated at any given time, FER at a recognised state or FER at a recognised group state should be analysed based on this risk-monitoring information (see 3.1.28 and 3.1.29). For example, if system state 3 in the state transition diagram in Table 6 or group state G that is composed of system states 1 and 2 in the state transition diagram in Table 7 is monitored and recognised at any given time, the following descriptions for the estimation of FER at recognised state 3 and FER at group state G are possible.

If the antecedent state 3 is monitored and recognised at time t, then FER at recognised state 3 is analysed for an unrepeatable final event by use of Table 6. The FER at recognised state 3 is defined as the target measure of the occurrence of the final event at time t. Table 6 illustrates the symbols and graphical representation for the analysis of FER at recognised state 3 for an unrepeatable final event by use of the ETA, FTA and Markov techniques. Here the antecedent state 3 is a virtual initial state to which the final state 4 reverts to be renewed. The FER at recognised state 3 is estimated by use of those diagrams (see 9.3.3).

Table 7 illustrates the symbols and graphical representation for the analysis of FER at recognised group state G for an unrepeatable final event by use of the ETA, FTA and Markov techniques. If the group state G is monitored and recognised at time t, FER at recognised group state G is defined as the target measure of the occurrence of the final event at time t. The FER at recognised group state G is estimated by use of those diagrams (see 9.3.4).

8.2 Example of recognised (group) states

In Figure 10, for instance, the initial state A is a recognised state at time t = 0 and just after a proof test, given that the proof test is performed perfectly. If CCF are disregarded, the system state D and F will be recognised states at any time, system state G is the final state, system state A and E compose recognised group state G1, and the system state B and C compose group state G2 at any time except the moment just after the proof test (see 9.4.6).

Table 6 – Symbols and graphical representation for the FER at recognised state 3

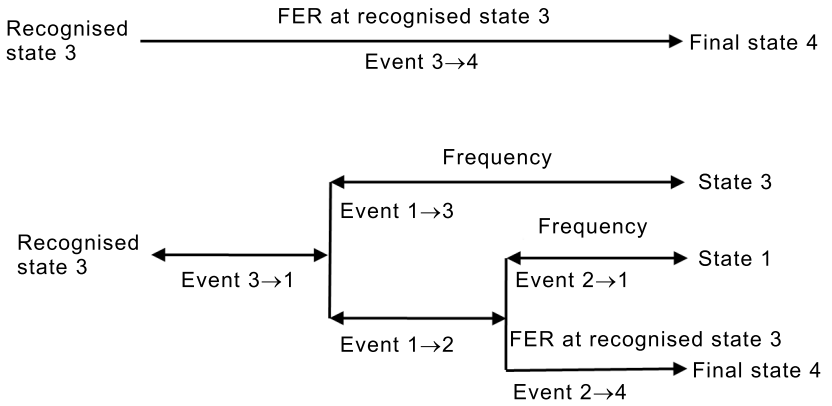
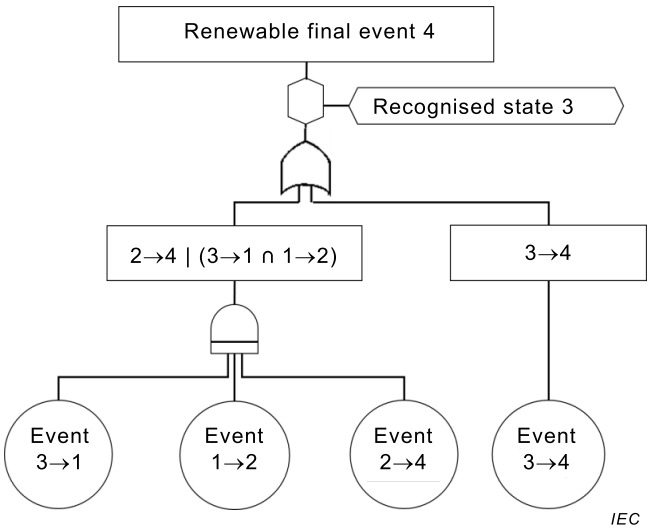
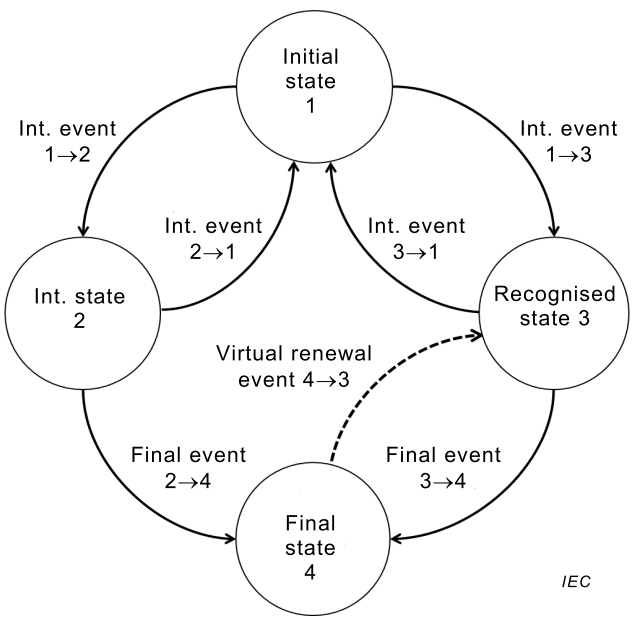
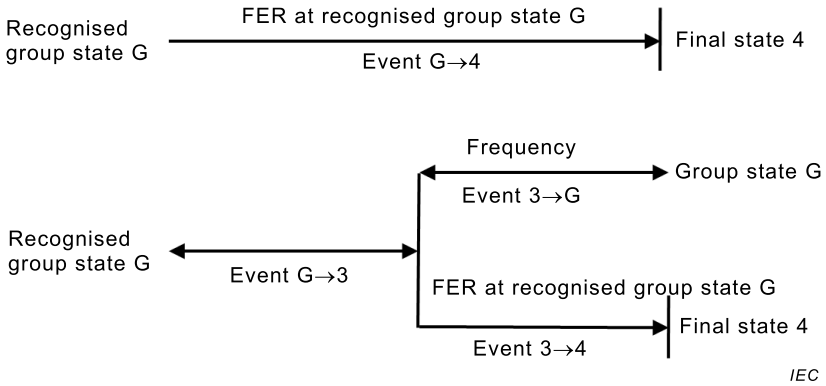
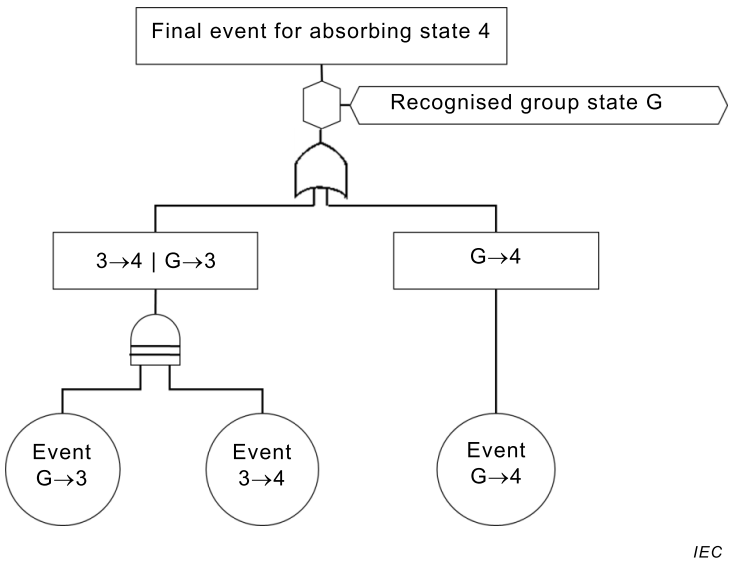
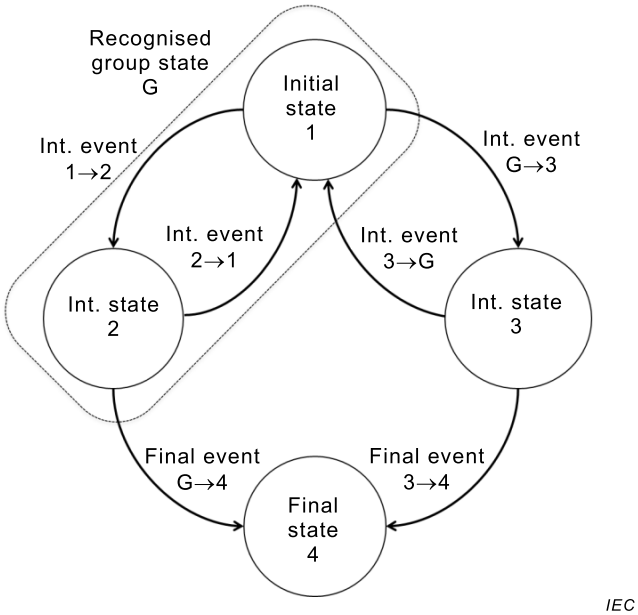
Techniques	Diagrams
ETA	
FTA	
Markov state transition	

Table 7 – Symbols and graphical representation for FER at recognised group state G

Techniques	Diagrams
ETA	
FTA	

Techniques	Diagrams
Markov state transition	

9 Analysis of multiple protection layers

9.1 General

Multiple protection layers (PLs) are hierarchical mechanisms that activate their proactive functions to prevent a final event that can result in a final state of a risk from occurring. If one of the multiple PLs fails to activate its own proactive function, this failure will result in the demand that activates the proactive function(s) of the next PL (see Figure 11). Here the PL that may activate the next PL is categorised as the int. PL, and the PL of which failure brings the overall system to this final state is categorised as the final PL (FPL) for the risk of concern.

Figure 11 shows an event tree for an overall system with a demand source, int. PL and FPL to control and/or reduce (a) risk(s). For instance, a self-driving car being in operation, its cruise control and pre-crash control systems are referred to the demand source, int. PL and FPL against a crash risk, respectively (see Clause B.2) [30][32]. Those systems control and reduce the crash risk, and make the FER at an initial state φ meet a tolerable level (see 3.1.1, Note 3).

If an FPL fails under a demand state (i.e., an FPL fails in its operating state) or if a demand occurs when the FPL is in a fault (i.e., the FPL is demanded in a fault), a final event will usually be brought about. Even if the final event is unrepeatable, the failures of int. PL(s) may be repeatable. This means that the demand at the PLs can be repeatable. For such repeatable events as failures and demands, PAND gate of Type 1 is useful for the FTA of int. PL(s) (see 9.2).

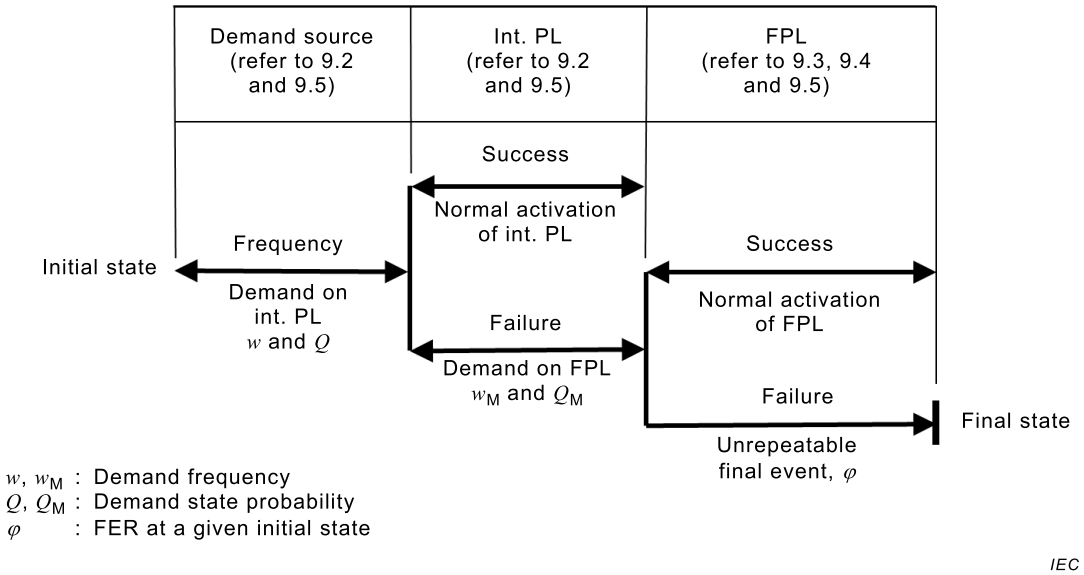


Figure 11 – Event tree of a demand source, int. PL and FPL for a risk

If a risk analysis is performed by using the RBD and FTA techniques complementarily for an int. PL(s), numerous MCSs may be extracted (see Clause 6). Here the MCS is a set that consists of mutually independent basic elements of 1, 2, …, and n (see 3.1.35). The basic elements will be such events as “failure of item”, “failure of Ch”, “demand at item”, “demand at Ch”, etc. Thus the basic element, for example “failure of Ch”, can involve a significant number of failures caused by the hundreds or more components of which the Ch is composed. It is noted that the treatment of several Chs that compose a PL may often mean the treatment of thousands or more components. Such a PL is called a large-scale PL. Risk analysis of an overall system that is composed of a large-scale PL(s) and therefore may involve multiple risks is often called risk analysis of a complex system (see Table 1, Clause 6, 9.5, Clauses A.5, B.2 and B.3).

Risks owing failures of PLs are analysed quantitatively in Clause 9. Firstly, how the failure of int. PL becomes the demand at the next PL is illustrated for complex systems with sequential failure logics in 9.2. Then analyses of FPL are illustrated in 9.3 and 9.4.

Notations

(0,0) FPL is UP under a non-demand state;

(1,0) FPL is in a UD fault under a non-demand state;

(0,1) FPL is UP under a demand state, i.e., FPL is normally operating;

(1,1) final state, i.e., the state in which the final consequences of a risk may appear;

λ_i constant event rate of basic element E_i (i = 1, 2,…, n: $E_i \in \{1, 2, \ldots, n\}$) that comprises an MCS, but $\lambda_i > 0$ (rates are, for instance, failure rate, demand rate, etc.) [1/h];

μ_i constant repair rate of the state resulting from E_i (i = 1, 2, …, n) that comprises an MCS, but $\mu_{ki} > 0$ (rates are, for instance, repair rate, completion rate, etc.) [1/h];

λ_{ki} constant event rate of basic element E_{ki} (i = 1, 2, …, n; $E_{ki} \in \{1, 2, \ldots, n\}$) that comprises MCS K_k (k = 1, 2, …, m), but $\lambda_{ki} > 0$ [1/h];

μ_{ki} constant repair rate of the state resulting from the E_{ki}, but $\mu_{ki} > 0$ [1/h];

λ_{kSi} constant event rate of basic element E_{kSi} (i = 1, 2, …, n; $E_{kSi} \in \{1, 2, \ldots, n\}$) that comprises basic element sequence S (= 1, 2, …, h) of the MCS K_k (k = 1, 2, …, m), but $\lambda_{kSi} > 0$ [1/h];

μ_{kSi} constant repair rate of the state resulting from the E_{kSi}, but $\mu_{kSi} > 0$ [1/h];

λ_{UD} constant UD failure rate of FPL [1/h];

μ_{UD} reciprocal of the mean time to restoration of UD fault of FPL due to the proof test [1/h];

λ_{D} constant D failure rate of FPL [1/h];

μ_{D} constant D repair rate of FPL [1/h];

λ_{M} constant demand rate at FPL [1/h];

μ_{M} constant completion rate at FPL (i.e., reciprocal of the mean time to completion) [1/h];

m constant renewal event rate [1/h];

T risk exposure time at FPL [h];

$P_{x,y}(X,Y)$ probability that a system is in system state (X,Y) in a steady state, given that it is in system state (x, y) at time 0 and its final state causes transition only to (x, y);

$P_{Gi(X,Y)}(t)$ probability that a system is in system state (X,Y) at time t, given that the system entered the recognised group state Gi (i = 1, 2,…, n) at time 0 and has not left this group until time t;

$\omega_{x,y}$ FEF at initial (or recognised) state (x, y) [1/h];

$\varphi_{x,y}$ FER at initial (or recognised) state (x, y) [1/h];

$T_{x,y}$ MTFE at initial (or recognised) state (x, y) [h];

$\varphi_{Gi}(t)$ FER at group state Gi (dynamic estimation) [1/h];

$T_{Gi}(t)$ MTFE at group state Gi (dynamic estimation) [h];

$\varphi_{Gi(x, y)}$ (x, y) centred FER at group state Gi [1/h];

$T_{Gi(x, y)}$ (x, y) centred MTFE at group state Gi [h];

$\{\varphi_{x,y}, T_{x,y}\}_{Gi}$ set of FER at recognised group state Gi (i = 1, 2,…, n) ($\varphi_{x,y}$ and $T_{x,y}$ are for all (x,y) included in the recognised group state Gi).

9.2 Frequency and rate for repeatable events

9.2.1 General

Int. PLs will be arranged in arbitrary architecture systems. It is supposed the MCSs of K_1, K_2, …, and K_m are extracted for arbitrary number m through the FTA of an int. PL, and K_k (k = 1, 2, …, m) consists of the arbitrary number of basic elements of 1, 2, …, and n. In general, basic elements are often, but not always, repeatable, however, it is assumed in 9.2 that all basic elements of MCS K_k are repeatable, i.e., $\mu_{ki}>0$ (i = 1, 2, …, n) holds for all k (see 9.1). Thus, quantitative analyses of a PAND gate of Type 1 are illustrated for both of the non-sequential and sequential failure logics in 9.2.2 and 9.2.3, respectively [12][14][15].

For all basic elements that are unrepeatable, i.e., μ_i = 0 (i = 1, 2, …, n), Fussell et al. have quantified the sequential failure logic of a PAND gate for such basic elements [13]. However, if repeatable and unrepeatable basic elements coexist in an MCS, then the FEF at a given initial state and FER at a given initial state will be applied to the quantitative analysis of such PAND gate failure logics as shown in 9.3 and 9.4 [18][27][29].

9.2.2 Independent of event sequence

If repeatable failures of an int. PL occur independently of the sequence of the occurrences of basic elements, 1, 2, …, n, that comprise MCS K_k, then the failure logic leading to the top event can be described, for instance, as in Figure 12 with PAND gates of Type 1. The input events into a PAND gate of Type 1 for MCS K_k are basic elements of 1, 2, …, and n. The output event of the PAND gate is the top event “failure of the int. PL (due to MCS K_k)”.

The top event becomes true if all the input events of $E_{ki\neq j}$ (i = 1, 2, …, n; but $i\neq j$) become true earlier than the input event E_{kj} and the true conditions are not restored until the input event E_{kj} finally becomes true, given that all the input events are not true at time zero. This failure logic leading to the top event is described in Figure 12, where

$E_{ki\neq j}$ all basic elements i (i = 1, 2, …, and n; but $i\neq j$) of MCS K_k (k = 1, 2, …, m) become true;

E_{kj} basic element j (j = 1, 2, …, or n; but $j\neq i$) of MCS K_k (k = 1, 2, …, m) becomes true.

The top event described in Figure 12 results in a demand at the next PL or FPL (see Figure 11). Thus the probability of the next PL or FPL being under a demand state, Q^*_k, and demand frequency at the next PL or FPL, w^*_k, owing to MCS K_k in a steady state are defined:

Q^*_k probability that the next PL or FPL is under a demand state that results from a demand occurring according to the failure logic of an int. PL of concern as shown in Figure 12, in a steady state;

w^*_k frequency of the demand that occurs according to the failure logic of an int. PL of concern as shown in Figure 12, in a steady state.

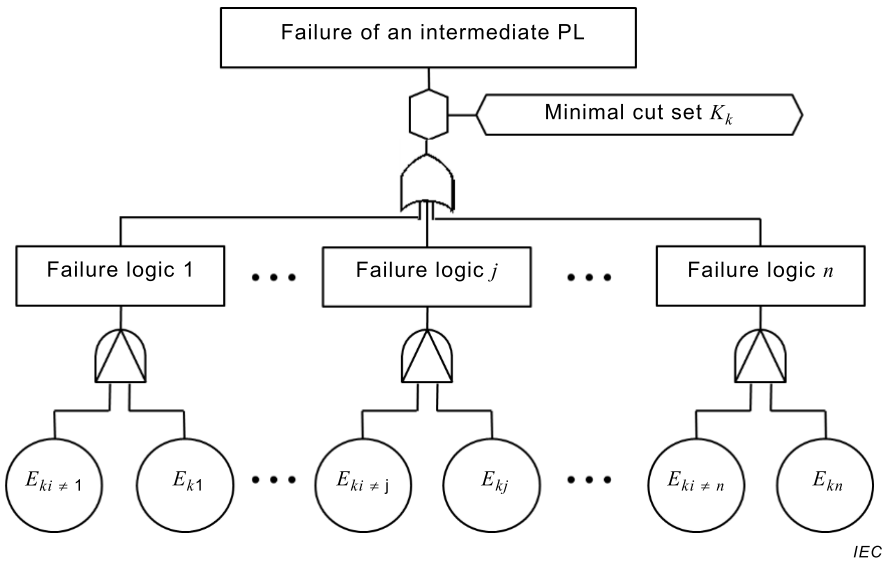


Figure 12 – Failure of int. PL independent of event sequence

Q^*_k and w^*_k are represented in the following formulas [12][14]:

$$Q^*_k = \prod_{i=1}^{n} \{\lambda_{ki}/(\lambda_{ki}+\mu_{ki})\} \tag{22}$$

$$w^*_k = \sum_{j=1}^{n} [\prod_{i=1,i\neq j}^{n} \{\lambda_{ki}/(\lambda_{ki}+\mu_{ki})\}]\ \lambda_{kjk}\mu_{kj}/(\lambda_{kj}+\mu_{kj}) \tag{23}$$

Therefore, the upper limit of the demand state probability Q^*_{UL} and the upper limit of the demand frequency w^*_{UL} are defined, given that $Q^*_k << 1$ (k = 1, 2, …, m) holds [12][14]:

Q^*_{UL} upper limit of the approximate probability that the next PL or FPL is under a demand state according to all the failure logics of MCSs K_k (k = 1, 2, …, m) of an int. PL of concern shown in Figure 12 in a steady state;

w^*_{UL} upper limit of the approximate frequency of the demand at the next PL or FPL according to all the failure logics of MCSs K_k (k = 1, 2, …, m) of an int. PL of concern described in Figure 12 in a steady state.

Q^*_{UL} and w^*_{UL} are expressed in the following formulas:

$$Q^*_{UL} = \sum_{k=1}^{m} \prod_{i=1}^{n} \{\lambda_{ki}/(\lambda_{ki}+\mu_{ki})\} \quad (24)$$

$$w^*_{UL} = \sum_{k=1}^{m} [\sum_{j=1}^{n} \{ \prod_{i=1, i\neq j}^{n} (\lambda_{ki}/(\lambda_{ki}+\mu_{ki}))\}\lambda_{kj}\mu_{kj}/(\lambda_{kj}+\mu_{kj})] \quad (25)$$

If the postulate above, i.e., $Q^*_k << 1$ for all k (k = 1, 2, …, m), does not hold, two options a) and b) below are suggested.

a) The demand state probability and the demand frequency should be formulated according to the accurate procedure for quantifying minimal cut sets, however, this is beyond the scope of this document (see for instance [14]).

b) The assumption that the top event “failure of the int. PL” is repeatable could be inappropriate. For example, if the demand at the int. PL of concern is continuous, then $Q^*_k << 1$ may not hold. In such a case, option a) could lead to an unfavourable result, and therefore the FEF at a given initial state and FER at a given initial state should be applied to the estimation of the demand state probability and demand frequency at the next PL.

Because failure of an int. PL activates (a) proactive function(s) of the next PL or FPL (see Figure 11), the following relationships between w^*_{UL}, Q^*_{UL}, demand frequency at the next PL or FPL, w_M, and demand state probability at the next PL or FPL, Q_M, hold in a steady state:

$w_M = \lambda_M\mu_M/(\lambda_M+\mu_M) \approx w^*_{UL}$;

$Q_M = \lambda_M/(\lambda_M+\mu_M) \approx Q^*_{UL}$.

Thus the following approximate equations are useful:

$\lambda_M \approx w^*_{UL}/(1-Q^*_{UL})$;

$\mu_M \approx w^*_{UL}/Q^*_{UL}$.

9.2.3 Depending on event sequence

9.2.3.1 General

If the failure of an int. PL is repeatable and depends on the sequence of occurrences of basic elements, i.e., the basic element sequence S (= 1, 2, …, h), then the failure logic in basic element sequence S (= 1, 2, …, h) resulting in the top event can be described with a PAND gate of Type 1. This failure logic is shown in Figure 13, where the output event of the PAND gate of Type 1 “failure of an int. PL (owing to the failure logic in basic element sequence S (= 1, 2, …, h) of MCS K_k)” becomes true if all input events E_{kSi} (i = 1, 2, …, n; $E_{kSi} \in$ {1, 2, …, n}) of MCS K_k (k = 1, 2, …, m) become true in the sequence S, i.e., in the order from the left to the right in the figure, and if the true states are not restored until input event E_{kSn} finally becomes true, given that all the basic elements are not true at time zero. Input event E_{kSi} in Figure 13 is defined:

E_{kSi} basic element of i^{th} order (i = 1, 2, …, n) in sequence S (S = 1, 2, …, h) of MCS K_k (k = 1, 2, …, m) becomes true.

9.2.3.2 Formulas in a steady state

Demand state probability, Q_{kS}, and demand frequency, w_{kS}, in a steady state are defined:

Q_{kS} probability that the next PL or FPL is under a demand state that results from a demand occurring according to the failure logic of an int. PL of concern in sequence S (S = 1, 2, …, h) as shown in Figure 13, in a steady state;

w_{kS} frequency of the demand that occurs according to the failure logic of an int. PL of concern in sequence S (S = 1, 2, …, h) as described in Figure 13, in a steady state.

Q_{kS} and w_{kS} are expressed in the following formulas [15]:

$$Q_{kS} = \prod_{i=1}^{n} \{\lambda_{kSi}\mu_{kSi}/(\lambda_{kSi}+\mu_{kSi})\}/\{\prod_{i=1}^{n} (\sum_{j=1}^{i} \mu_{kSj})\} \quad (26)$$

$$w_{kS} = \prod_{i=1}^{n} \{\lambda_{kSi}\mu_{kSi}/(\lambda_{kSi}+\mu_{kSi})\}/\{\prod_{i=1}^{n-1} (\sum_{j=1}^{i} \mu_{kSj})\} \quad (27)$$

Demand state probability, Q_k, and demand frequency, w_k, in any basic element sequences of S (S = 1, 2, …, and h) of MCS K_k in a steady state are formulated as [15]:

$$Q_k = \sum_{S=1}^{h} [\prod_{i=1}^{n} \{\lambda_{kSi}\mu_{kSi}/(\lambda_{kSi}+\mu_{kSi})\}/\{\prod_{i=1}^{n} (\sum_{j=1}^{i} \mu_{kSj})\}] \quad (28)$$

$$w_k = \sum_{S=1}^{h} [\prod_{i=1}^{n} \{\lambda_{kSi}\mu_{kSi}/(\lambda_{kSi}+\mu_{kSi})\}/\{\prod_{i=1}^{n-1} (\sum_{j=1}^{i} \mu_{kSj})\}] \quad (29)$$

Similarly, the upper limits of the demand state probability, Q_{UL}, and the demand frequency, w_{UL}, owing to all the MCSs of K_k (k = 1, 2, …, and m) are expressed in the following formulas, given that Q_k<<1 (k = 1, 2, …, m) holds [15]:

$$Q_{UL} = \sum_{k=1}^{m} [\sum_{S=1}^{h} [\prod_{i=1}^{n} \{\lambda_{kSi}\mu_{kSi}/(\lambda_{kSi}+\mu_{kSi})\}/\{\prod_{i=1}^{n} (\sum_{j=1}^{i} \mu_{kSj})\}]] \quad (30)$$

$$w_{UL} = \sum_{k=1}^{m} [\sum_{S=1}^{h} [\prod_{i=1}^{n} \{\lambda_{kSi}\mu_{kSi}/(\lambda_{kSi}+\mu_{kSi})\}/\{\prod_{i=1}^{n-1} (\sum_{j=1}^{i} \mu_{kSj})\}]] \quad (31)$$

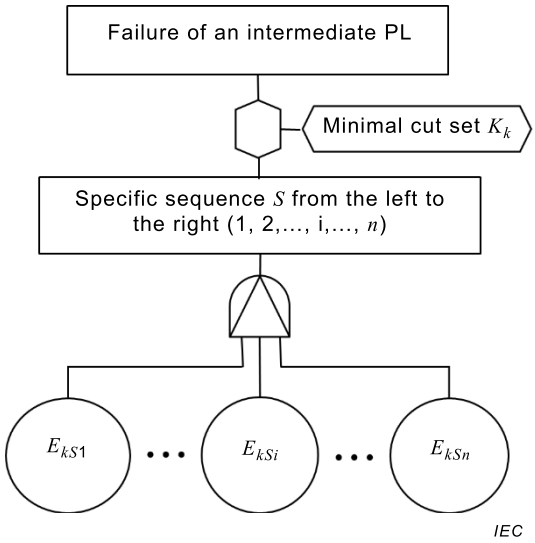


Figure 13 – FT for failure of int. PL through sequential failure logic

Similarly if the failure of the int. PL of concern activates the proactive function(s) of the next PL or FPL, the following relationships between w_M, Q_M, w_{UL} and Q_{UL} are useful:

$\lambda_M \approx w_{UL}/(1-Q_{UL})$;

$\mu_M \approx w_{UL}/Q_{UL}$.

9.2.3.3 Approximate formulas in the dynamic state given that $\lambda_{kSi}/\mu_{kSi}<<1$

If $\lambda_{kSi}/\mu_{kSi}<<1$ holds for any k, S and i, approximate demand state probability, $Q_{akS}(t)$, and approximate demand frequency, $w_{akS}(t)$, at time t are defined, given that all the basic elements were not true at time 0:

$Q_{akS}(t)$ approximate probability that the next PL or FPL is under a demand state at time t that results from a demand occurring according to the failure logic of an int. PL of concern in sequence S (S = 1, 2, …, h) as described in Figure 13;

$w_{akS}(t)$ approximate frequency of the demand at time t that occurs according to the failure logic of an int. PL of concern in sequence S (S = 1, 2, …, h) as described in Figure 13.

$Q_{akS}(t)$ is formulated as [15]:

$$Q_{akS}(t) = \left(\prod_{i=1}^{n} \lambda_{kSi}\right) \sum_{r=0}^{n} \left[\exp(-a_r t)/\left\{\prod_{j=0, j\neq r}^{n} (a_j - a_r)\right\}\right] \quad (32)$$

where

$a_u \equiv \sum_{i=1}^{u} \mu_{kSi}$ (u = 1, 2, …, n), and $a_0 \equiv 0$.

Similarly, $w_{akS}(t)$ is as follows [15]:

$$w_{akS}(t) = \left(\prod_{i=1}^{n} \lambda_{kSi}\right) \sum_{r=0}^{n-1} \left[\exp(-a_r t)/\left\{\prod_{j=0, j\neq r}^{n-1} (a_j - a_r)\right\}\right] \quad (33)$$

Similarly, the approximate demand state probability, $Q_{ak}(t)$, and approximate demand frequency, $w_{ak}(t)$, in any basic element sequence of S (S = 1, 2, …, and h) of MCS K_k (k = 1, 2, …, m) are formulated as:

$$Q_{ak}(t) = \sum_{S=1}^{h} [(\prod_{i=1}^{n} \lambda_{kSi}) \sum_{r=0}^{n} [\exp(-a_r t)/\{ \prod_{j=0, j\neq r}^{n} (a_j - a_r)\}]] \quad (34)$$

$$w_{ak}(t) = \sum_{S=1}^{h} [(\prod_{i=1}^{n} \lambda_{kSi}) \sum_{r=0}^{n-1} [\exp(-a_r t)/\{ \prod_{j=0, j\neq r}^{n-1} (a_j - a_r)\}]] \quad (35)$$

The approximate upper limits of the demand state probability, $Q_{aUL}(t)$, and approximate demand frequency, $w_{aUL}(t)$, owing to all the MCSs of K_k (k = 1, 2, …, and m), are expressed in the following formulas, given that $Q_{ak}(t) \ll 1$ holds for all the MCSs [15]:

$$Q_{aUL}(t) = \sum_{k=1}^{m} [\sum_{S=1}^{h} [(\prod_{i=1}^{n} \lambda_{kSi}) \sum_{r=0}^{n} [\exp(-a_r t)/\{ \prod_{j=0, j\neq r}^{n} (a_j - a_r)\}]]] \quad (36)$$

$$w_{aUL}(t) = \sum_{k=1}^{m} [\sum_{S=1}^{h} [(\prod_{i=1}^{n} \lambda_{kSi}) \sum_{r=0}^{n-1} [\exp(-a_r t)/\{ \prod_{j=0, j\neq r}^{n-1} (a_j - a_r)\}]]] \quad (37)$$

9.2.3.4 Formula in a dynamic state for n = 3

Suppose, for instance, that n = 3 in Figure 13 and the inputs into the PAND gate of Type 1 are E_{kS1} = 1, E_{kS2} = 2 and E_{kS3} = 3 for basic element sequence S of the basic elements 1, 2 and 3 of MCS K_k. Then the frequency of the demand from this PL to the next PL (or FPL) in this event sequence of the basic elements 1, 2 and 3 at time t, $w_{3kS}(t)$, is expressed by the following equation, given that all the basic elements of this MCS are not true at time 0, and $\lambda_1 \neq \mu_2$ and $\mu_1 \neq \lambda_2$ hold [15]:

$$w_{3kS}(t) = [\prod_{i=1}^{3} \{\lambda_i/(\lambda_i+\mu_i)\}][\{\mu_2\mu_3/(\mu_1+\mu_2)\} - \{\mu_2\mu_3/(\mu_2-\lambda_1)\}\exp\{-(\lambda_1+\mu_1)t\} - \{\lambda_2\mu_3/(\lambda_2-\mu_1)\}\exp\{-(\lambda_2+\mu_2)t\}$$

$$+\mu_3\{(\lambda_1/(\lambda_1+\lambda_2)) + (\mu_1/(\mu_1+\mu_2)) + (\mu_1/(\lambda_2-\mu_1)) + (\lambda_1/(\mu_2-\lambda_1))\}\exp\{-(\mu_1+\mu_2)t\}$$

$$+\{\lambda_2\mu_3/(\lambda_1+\lambda_2)\}\exp\{-(\lambda_1+\mu_1+\lambda_2+\mu_2)t\} + \{\mu_2\lambda_3/(\mu_1+\mu_2)\}\exp\{-(\lambda_3+\mu_3)t\} - \{\mu_2\lambda_3/(\mu_2-\lambda_1)\}\exp\{-(\lambda_1+\mu_1+\lambda_3+\mu_3)t\}$$

$$-\{\lambda_2\lambda_3/(\lambda_2-\mu_1)\}\exp\{-(\lambda_2+\mu_2+\lambda_3+\mu_3)t\} + \{\lambda_2\lambda_3/(\lambda_1+\lambda_2)\}\exp\{-(\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)t\}$$

$$+\lambda_3\{(\lambda_1/(\lambda_1+\lambda_2)) + (\mu_1/(\mu_1+\mu_2)) + (\mu_1/(\lambda_2-\mu_1)) + (\lambda_1/(\mu_2-\lambda_1))\}\exp\{-(\mu_1+\mu_2+\lambda_3+\mu_3)t\}] \quad (38)$$

9.3 Final protection layer arranged in a 1-out-of-1 architecture system

9.3.1 General

The possibility of CCF is often measured by the use of the beta factor, β. If β is estimated at several per cent or more, the CCF are often (but not always) dominant over the system failure from the perspective of risk analysis (see Figure A.4, Clauses A.3 and B.4). Therefore it is inevitable to discuss the item arranged in a 1-out-of-1 architecture system because the CCF of multiple Chs can often be modelled as the failure in a single Ch system [27]. Figure 14 to Figure 19 represent FTs and state transition models of an overall system in the context of the demand at an FPL arranged in a 1-out-of-1 architecture system with UD faults only. At first the following postulates are made.

a) In Figure 15 parameter T is the risk exposure time, and π is the quotient of the failure rate of an item that is not operating under a non-demand state to the failure rate of the item operating under a demand state. Generally $0<\pi\leq1$ holds. If π = 1 holds, the failure rate of the item in the operating state is equivalent to that in the non-operating state. If the value of quotient π asymptotically approaches 0, the item cannot fail in the non-operating state. In this document, however, the value of the quotient is hereafter put at 1 for easier discussion (see [24][26] for risk analyses involving the topics for quotient π).

b) When an overall system is in a demand state for (a) function(s) of an item, the item is required to be and only to be operating for the function(s) whereas the item is required to be and only to be not operating under the non-demand state for the function(s). Therefore two failure modes are required to be considered, i.e., the item is not operating under a demand state, and the item is operating under a non-demand state (see 3.1.3, Note 6).

c) The UD fault is found only when the proof test is performed. The proof test is a kind of periodic inspection performed by maintenance mechanic(s) to discover and restore (a) faulty part(s) of int. PLs and FPL. The proof test is usually performed every year or every two years, and several hours or days will be necessary for maintenance. The time required for the maintenance is negligible compared with the interval between proof tests, and therefore here the faulty parts can be assumed to be recovered instantaneously and completely by the proof test (see Clause A.1 for an example of an incomplete proof test).

d) The UD fault cannot be recognised during the interval between proof tests whereas the demand state can be recognised when the int. PL or FPL is operating normally under the demand state, and the final state is also recognisable because the overall system is significantly degraded in this state (see 3.1.13, Note 3). The final event is unrepeatable and the final state is renewable; state transition rates are assumed to be constant in 9.3.2 to 9.4.

9.3.2 Final event rate at initial state (0, 0) for unrepeatable final event

Figure 14 and Figure 15 represent the causation of the final event owing to both the UD failure of the FPL and the demand at the FPL, given that $1/T<<\mu_M$ and $\lambda_{UD}<<1/T$ hold. From Figure 15, $P_{0,0}(1,0)$, $P_{0,0}(0,1)$ and $P_{0,0}(1,1)$ are easily calculated (see notations in 9.1). Thus, FEF at initial state (0,0), $\omega_{0,0}$, FER at initial state (0,0), $\varphi_{0,0}$, and MTFE at initial state (0,0), $T_{0,0}$ are formulated, given that the initial state (0,0) is recognised at t = 0 [18][19][20]:

$$\omega_{0,0} = P_{0,0}(1,0)\lambda_M+P_{0,0}(0,1)\lambda_{UD}$$

$$\varphi_{0,0} = \omega_{0,0}/\{1-P_{0,0}(1,1)\}$$

$$T_{0,0} = 1/\varphi_{0,0}$$

where

$P_{0,0}(0,0) = 1/[1+\{\lambda_M/(\mu_M+\lambda_{UD})\}\{1+(\lambda_{UD}/m)\}+\{\lambda_{UD}/(\lambda_M+\mu_{UD})\}\{1+(\lambda_M/m)\}]$

$P_{0,0}(1,0) = \{\lambda_U/(\lambda_M+\mu_{UD})\}P_{0,0}(0,0)$

$P_{0,0}(0,1) = \{\lambda_M/(\mu_M+\lambda_{UD})\}P_{0,0}(0,0)$

$P_{0,0}(1,1) = [(\lambda_{UD}/m)\{\lambda_M/(\mu_M+\lambda_{UD})\}+(\lambda_M/m)\{\lambda_{UD}/(\lambda_M+\mu_{UD})\}]\ P_{0,0}(0,0)$

given that $2/T<<\mu_{UD}$ and $\pi = 1$ hold (see 9.3).

If the final state in which the final consequence of the risk appears is brought about in both the event sequences (0,0)→(1,0)→(1,1) and (0,0)→(0,1)→(1,1), i.e., according to the final event logics of “failure first and demand later” (logic #1) and “demand first and failure later” (logic #2), FER at initial state (0,0), $\varphi_{0,0}$, is expressed in the following formula, given that $\lambda_{UD}<<(\lambda_M+\mu_{UD})$ and $\lambda_{UD}<<\mu_M$ hold [18][19][20]:

$$\varphi_{0,0}\approx[\{(1-Q_M)\}\lambda_{UD}w_M/\{(1-Q_M)\mu_{UD}+w_M\}]+Q_M\lambda_{UD} \quad (39)$$

where

Q_M is the demand state probability and w_M is the demand frequency, and the following holds:

$$Q_M = \lambda_M/(\lambda_M+\mu_M)$$

$$w_M = \lambda_M\mu_M/(\lambda_M+\mu_M)$$

If the final consequence of risk appears according to logic #1 only, then Equation (39) is rewritten as

$$\varphi_{0,0}\approx(1-Q_M)\lambda_{UD}w_M/\{(1-Q_M)\mu_{UD}+w_M\}$$

If the final consequence of risk appears according to logic #2 only, then Equation (39) is rewritten as

$$\varphi_{0,0}\approx Q_M\lambda_{UD}$$

If $Q_M<<1$ and $w_M<<\mu_{UD}$ hold, then the system seems to be in a low demand mode of operation and the following equation holds from Equation (39):

$$\varphi_{0,0}\approx\lambda_{UD}w_M/\mu_{UD}+Q_M\lambda_{UD}$$

$$= (\lambda_{UD}/\mu_{UD})w_M+(\lambda_{UD}/\mu_M)w_M\approx(P_a+P_b)w_M \quad (40)$$

It is however assumed in IEC 61508 (all parts) that $\varphi_{0,0}\approx P_a w_M$ always holds, i.e., $P_b w_M \equiv 0$ holds in the low demand mode of operation. This means that the final consequence of risk appears according to logic #1 only (see 7.2.3 and Annex B).

If $Q_M<<1$ and $\mu_{UD}<<w_M$ hold, then the system seems in a high demand mode of operation and the following equation holds from Equation (39) (see 7.2.3 and Annex B):

$$\varphi_{0,0}\approx\lambda_{UD}w_M/(\mu_{UD}+w_M)+Q_M\lambda_{UD} \quad (41)$$

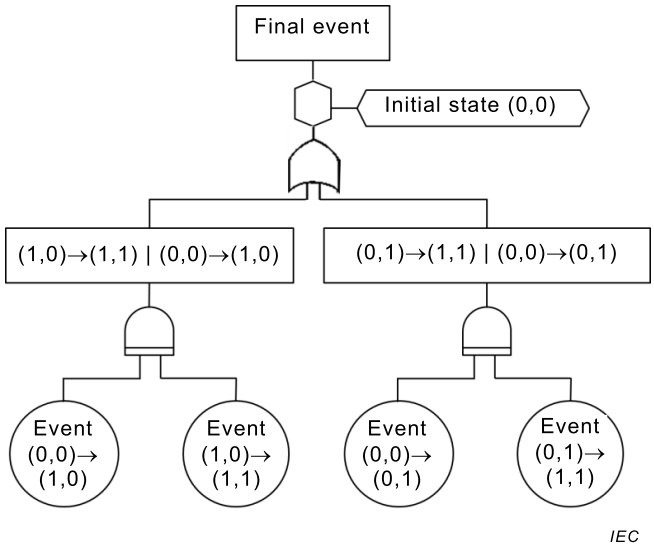


Figure 14 – FT for an unrepeatable final event at initial state (0,0)

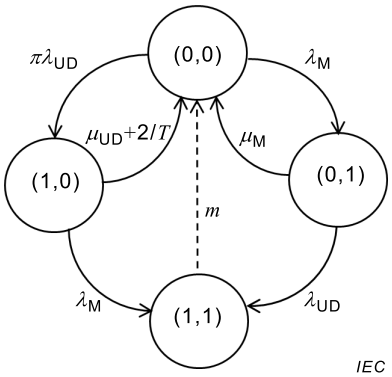


Figure 15 – State transition model for an unrepeatable final event at initial state (0,0)

If the final consequence of risk appears according to logic #1 only, the second term of the right side of Equation (41), $Q_M\lambda_{UD}$, is removed and therefore

$$\varphi_{0,0} \approx \lambda_{UD} w_M/(\mu_{UD}+w_M) \approx \lambda_{UD}$$

Similarly if the final consequences of the risk appear according to logic #2 only, the first term of the right side of Equation (41), $\lambda_{UD} w_M/(\mu_{UD}+w_M)$, is removed and therefore

$$\varphi_{0,0} \approx Q_M\lambda_{UD}$$

If $Q_M \approx 1$ and $\mu_{UD} << w_M$ hold, then the system is in a continuous operation and the following formula holds from Equation (39):

$$\varphi_{0,0} \approx (1-Q_M)\lambda_{UD}+Q_M\lambda_{UD} = \lambda_{UD} \quad (42)$$

9.3.3 Final event rate at recognised state (x, y)

If it is recognised that the FPL is working normally at time t, then it is recognised that the system is in antecedent state (0,1) shown in Figure 16 and Figure 17 at that time. Figure 16 and Figure 17 show how to model and analyse the causation of the final event for the

estimation of FEF at recognised state (0,1), $\omega_{0,1}$, FER at recognised state (0,1), $\varphi_{0,1}$, and MTFE at recognised state (0,1), $T_{0,1}$, given that antecedent state (0,1) is recognised at time t, and $1/T << \mu_M$ and $\lambda_{UD} << 1/T$.

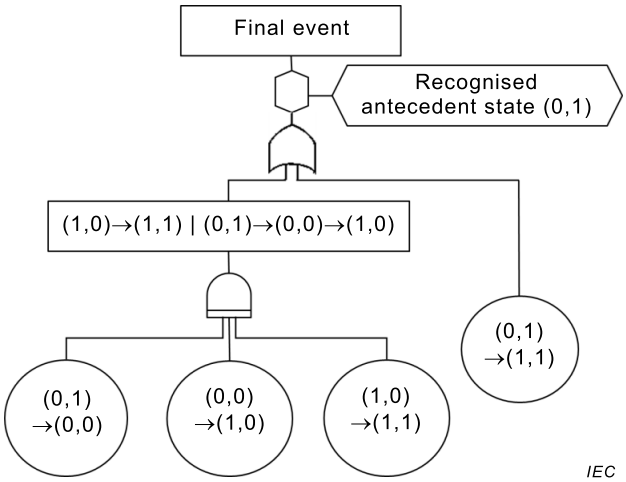


Figure 16 – FT for an unrepeatable final event for recognised state (0,1)

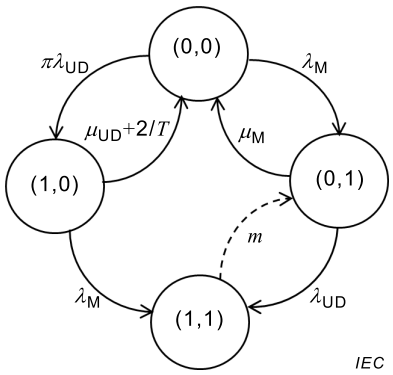


Figure 17 – State transition model for recognised state (0,1)

In Figure 17, the state transition from the final state (1,1) to the recognised state (0,1) is an unreal state transition, i.e., virtual renewal event, to calculate $\omega_{0,1}$ and $\varphi_{0,1}$. Thus, $\omega_{0,1}$, $\varphi_{0,1}$ and $T_{0,1}$ can be formulated in the same manner as shown in 9.3.2 (see 5.4 and 7.2.3):

$$\omega_{0,1} = P_{0,1}(1,0)\lambda_M + P_{0,1}(0,1)\lambda_{UD}$$

$$\varphi_{0,1} = \omega_{0,1}/\{1-P_{0,1}(1,1)\}$$

$$T_{0,1} = 1/\varphi_{0,1}$$

9.3.4 Final event rate at a recognised group state

9.3.4.1 General

If it is recognised that the overall system is in neither antecedent state (0,1) nor final state (1,1) at time t, it is known that the overall system is in group state G1 at that time as shown in Figure 18 and Figure 19. The figures show how to model and analyse the causation of the final event for the estimation of FER at recognised group state G1 and MTFE at recognised group state G1, given that the overall system entered this group at time 0 and has not left there until time t, and $1/T << \mu_M$ and $\lambda_{UD} << 1/T$ hold.

Because it cannot be indicated in which state (0,0) or (1,0) the overall system remains at time t, the FER at recognised group state G1 should be estimated by use of a weighted average.

9.3.4.2 Dynamic estimation of final event rate at recognised group state G*i*

In general, if the probability that the overall system is in system state (X,Y) that composes recognised group state Gi can be expressed in a function of time t, this probability of state (X,Y) at time t, given that the overall system entered this group at time 0 and has not left this group until time t, $P_{\mathrm{Gi(X,Y)}}(t)$, is useful as the weight for the estimation of weighted average FER at recognised group state Gi (see notations in 9.1).

For system states (0,0) and (1,0) that compose the recognised group state G1 in Figure 19, the probabilities of system states (0,0) and (1,0) at time t, given that the overall system entered G1 at time 0 and has not left there until time t, $P_{\mathrm{G1(0,0)}}(t)$ and $P_{\mathrm{G1(1,0)}}(t)$, could be described in a function of time. Then FER at recognised group state G1 at time t, $\varphi_{\mathrm{G1}}(t)$, is formulated as:

$$\varphi_{\mathrm{G1}}(t) = (1/T_{0,0})P_{\mathrm{G1(0,0)}}(t)/\{P_{\mathrm{G1(0,0)}}(t)+P_{\mathrm{G1(1,0)}}(t)\}+(1/T_{1,0})P_{\mathrm{G1(1,0)}}(t)/\{P_{\mathrm{G1(0,0)}}(t)+P_{\mathrm{G1(1,0)}}(t)\}$$

Here, $1/T_{0,0} = \varphi_{0,0}$, $1/T_{1,0} = \varphi_{1,0}$, and $P_{\mathrm{G1(0,0)}}(t)+ P_{\mathrm{G1(1,0)}}(t) = 1$ hold, and therefore $\varphi_{\mathrm{G1}}(t)$ and $T_{\mathrm{G1}}(t)$ are expressed in the following formulas:

$$\varphi_{\mathrm{G1}}(t) = \varphi_{0,0}P_{\mathrm{G1(0,0)}}(t)+\varphi_{1,0}P_{\mathrm{G1(1,0)}}(t);$$

$$T_{\mathrm{G1}}(t) = 1/\varphi_{\mathrm{G1}}(t)$$

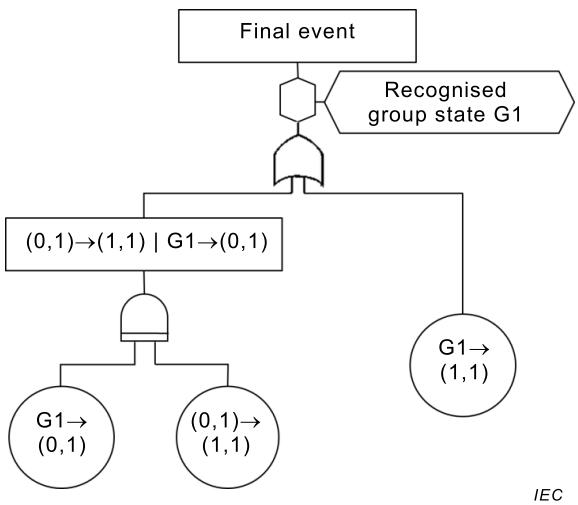


Figure 18 – FT for an unrepeatable final event for recognised group state G1

9.3.4.3 (*x*, *y*) centred final event frequency at group state G*i*

If the state probability that the system is in Gi cannot be described in any function of time, the probability of system state (X,Y) in a steady state, given that the overall system entered (x,y) at time 0 and the final state causes transition only to (x,y), $P_{x,y}(X,Y)$, is useful with respect to the weight (see notations, 9.1). Here, state (x,y) is a true or virtual initial state that is included in recognised group state Gi.

a) (0,0) centred FER at group state G1

For Figure 18 and Figure 19, $P_{0,0}(0,0)$ and $P_{0,0}(1,0)$ are useful for the weights to estimate FER at recognised group state G1. Thus, (0,0) centred FER at group state G1, $\varphi_{G1(0,0)}$, and (0,0) centred MTFE at group state G1, $T_{G1(0,0)}$ are formulated as:

$$\varphi_{G1(0,0)} = \varphi_{0,0}P_{0,0}(0,0)/\{P_{0,0}(0,0)+P_{0,0}(1,0)\}+\varphi_{1,0}P_{0,0}(1,0)/\{P_{0,0}(0,0)+P_{0,0}(1,0)\}$$

$$T_{G1(0,0)} = 1/\varphi_{G1(0,0)}$$

b) (1,0) centred final event rate at group state G1

For Figure 18 and Figure 19, $P_{1,0}(0,0)$ and $P_{1,0}(1,0)$ are useful for the weights to estimate FER at recognised group state G. Thus, (1,0) centred FER at group state G1, $\varphi_{G1(1,0)}$, and (1,0) centred MTFE at group state G1, $T_{G1(1,0)}$ are formulated as:

$$\varphi_{G1(1,0)} = \varphi_{0,0}P_{1,0}(0,0)/\{P_{1,0}(0,0)+P_{1,0}(1,0)\}+\varphi_{1,0}P_{1,0}(1,0)/\{P_{1,0}(0,0)+P_{1,0}(1,0)\}$$

$$T_{G1(1,0)} = 1/\varphi_{G1(1,0)}$$

9.3.4.4 Upper/lower limits of final event rate at recognised group state G*i*

If all $\varphi_{x,y}$ of which (x, y) belong to recognised group state Gi are estimated, then the minimum and maximum values of $\varphi_{x,y}$ can be easily known. The minimum value of $\varphi_{x,y}$ is the lower limit and the maximum value of $\varphi_{x,y}$ is the upper limit of FER at recognised group state Gi. Namely, the reciprocal of the lower limit and the reciprocal of the upper limit give the furthest position (or system state) and the nearest position (or system state) from the final event in the recognised group state, respectively.

The set of FER at recognised group state G1 is $\{\varphi_{0,0}, T_{0,0}, \varphi_{1,0}, T_{1,0}\}_{G1}$, and it would be easy to know the furthest and nearest positions (or system states) from the final event, as well as the MTFE at those positions in this recognised group state.

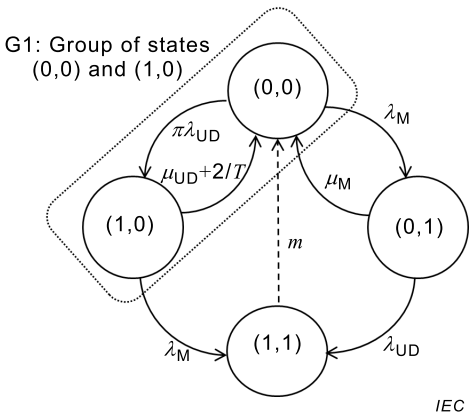


Figure 19 – State transition model for recognised group state G1

9.4 Final protection layer arranged in a 1-out-of-2 architecture system

9.4.1 General

Suppose that an FPL is composed of two Chs, Ch 1 and Ch 2, in which independent D and UD failures as well as common cause D and UD failures occur, and is required to perform a function to cope with an intrinsically variable safe system state like an automated steering function of automobile (see Clause B.2).

Here the D failure results in the D fault that is detected automatically by (a) self-diagnosis function(s), etc., and the UD failure results in the UD fault that is not automatically detected but is recognised by periodic proof tests performed by (a) maintenance mechanic(s) (see 9.3).

The FPL is described, for instance, by the use of an RBD arranged in a 1-out-of-2 architecture system with a CCF part as shown in Figure 20. In Figure 20, the independent failure parts that consist of both Chs are arranged in parallel and the CCF part is connected to the parallel parts in series [8][22].

9.4.2 Independent failure parts of the 1-out-of-2 architecture system

An RBD of the independent parts, i.e., the parallel parts of the Chs in Figure 20, is shown as Figure 21. The D failure part and UD failure part of each Ch are connected in series, and both Chs are connected in parallel.

The RBD shown in Figure 21 is equivalently rewritten again as shown in Figure 22. The “D failure part of Ch 1 and D failure part of Ch 2”, “D failure part of Ch 1 and UD failure part of Ch 2”, “UD failure part of Ch 1 and D failure part of Ch 2”, and “UD failure part of Ch 1 and UD failure part of Ch 2” are arranged in parallel, and those parallel structures are connected in series [8][22].

If one of the four parallel structures described in Figure 22, for instance the parallel structure composed of the UD failure part of Ch 1 and the D failure part of Ch 2, is in a fault and a demand occurs at the FPL, or if the FPL is under a demand state and a failure occurs in one of the four parallel structures, then failure of the FPL could occur (depending on sequential failure logics). Here, assumptions are made that the probability that two or more parallel structures are in faults simultaneously is negligible compared with the probability that any one of the four parallel structures is in a fault and that the probability that the parallel structure and CCF part are in faults simultaneously is also negligible.

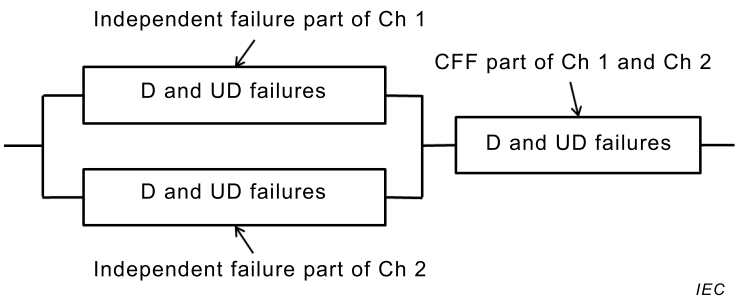


Figure 20 – RBD of FPL arranged in a 1-out-of-2 architecture system

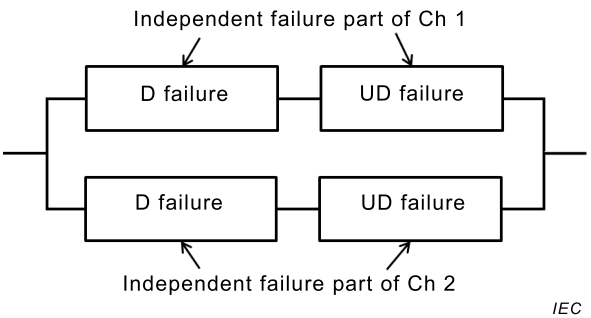


Figure 21 – RBD of the independent parts of Ch 1 and Ch 2

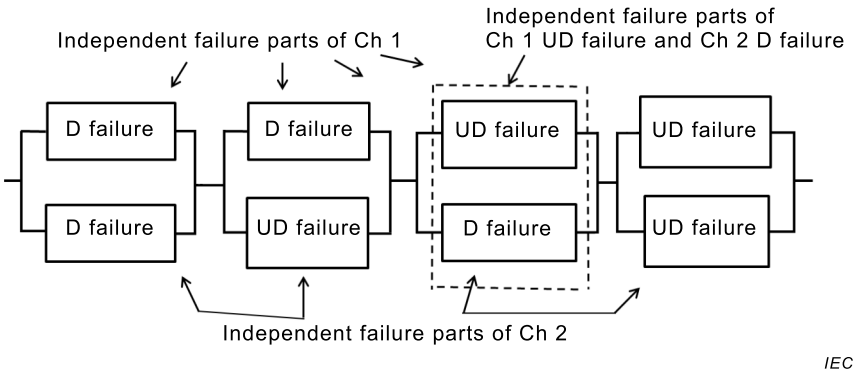


Figure 22 – RBD equivalent to that in Figure 21

9.4.3 Fault tree for independent undetected and detected failures

The causation of a top event, for instance, “final event due to the failure of the parallel structure of the UD failure part of Ch 1 and the D failure part of Ch 2” is developed as an FT shown in Figure 23, given that all the sequential failure logics composed of the events of the UD failure of Ch 1, the D failure of Ch 2, and the demand cause the top event.

The top event of FT becomes true when one of six permutations of the occurrences of three basic elements, i.e., UD failure of Ch 1, D failure of Ch 2 and demand, becomes true. Those three basic elements that are contained in the six permutations are the inputs to a PAND gate of Type 2 in Figure 23.

9.4.4 Final event rate at a given initial state owing to independent failures

The approximate FER at a given initial state for independent Ch 1 and Ch 2 failures is formulated as the sum total of FER at a given initial state due to the failure of each one of the four parallel structures shown in Figure 22, given that the probability that two or more parallel structures are in faults simultaneously is negligible compared with the probability that any one of the parallel structures is in a fault.

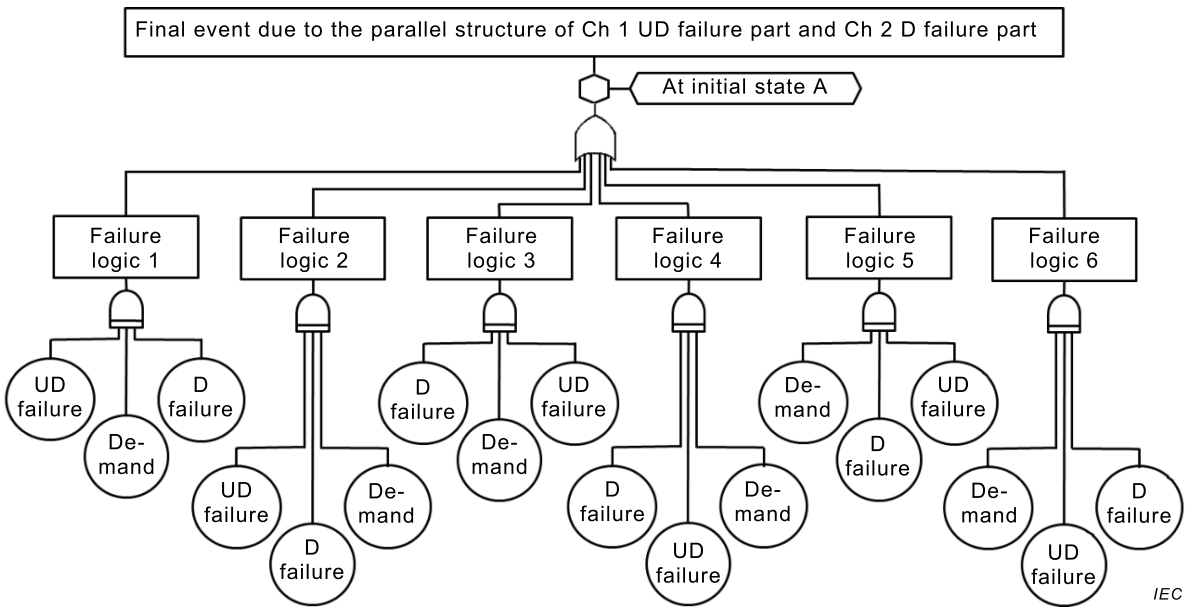


Figure 23 – FT for UD failure of Ch 1, D failure of Ch 2 and demand

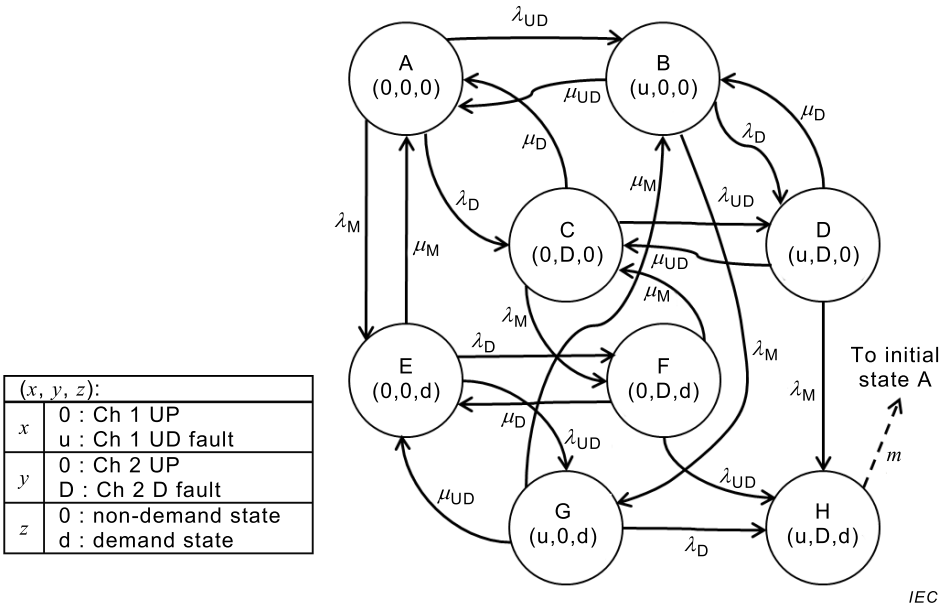


Figure 24 – State transitions due to UD failure of Ch 1, D failure of Ch 2 and demand

The FER at initial state A, i.e., system state (0,0,0), due to, for instance, the failure of parallel structure of UD failure part of Ch 1 and D failure part of Ch 2 is calculated by use of the state transition model shown in Figure 24, where state transition rates are:

1) UD failure and repair rates: λ_{UD} [1/h] and μ_{UD} [1/h] respectively;
2) D failure and repair rates: λ_D [1/h] and μ_D [1/h] respectively;
3) demand and completion rates: λ_M [1/h] and μ_M [1/h] respectively;
4) renewal rate: m [1/h].

Suppose that $P_{0,0,0}(x,y,z)$ is the probability that the system is in system state (x,y,z) described as in Figure 24 in a steady state, given that the initial state is system state (0,0,0). The probabilities the overall system state is in system state (u,0,d), (0,D,d), (u,D,0) and (u,D,d) are $P_{0,0,0}$(u,0,d), $P_{0,0,0}$(0,D,d), $P_{0,0,0}$(u,D,0) and $P_{0,0,0}$(u,D,d), which are easily calculated based on the approach described in 5.4 and 5.5. Thus FEF at initial state (0,0,0), $\omega_{0,0,0}$, FER at initial state (0,0,0), $\varphi_{0,0,0}$, and MTFE at initial state (0,0,0), $T_{0,0,0}$, given that initial state (0,0,0) is recognised at t = 0, are formulated as [22]:

$$\omega_{0,0,0} = P_{0,0,0}(u,0,d)\lambda_D + P_{0,0,0}(0,D,d)\lambda_{UD} + P_{0,0,0}(u,D,0)\lambda_M$$

$$\varphi_{0,0,0} = \omega_{0,0,0}/\{1-P_{0,0,0}(u,D,d)\}$$

$$T_{0,0,0} = 1/\varphi_{0,0,0}$$

A recognised state and recognised group states are referred to in 9.4.5 and 9.4.6.

9.4.5 Recognised states at each part

9.4.5.1 General

A postulate is made at first that the probabilities of simultaneous existence of two or more faults in a single Ch and simultaneous existence of any independent and common cause faults in the 1-out-of-2 architecture system are negligible (see 9.4.2).

9.4.5.2 Ch 1 D failure and Ch 2 D failure part

At this part, the overall system is in initial state (0,0,0) at t = 0, and thereafter can enter a recognised state, a recognised group state or the final state in a moment (see Figure 24 for symbol (x,y,z)).

Then recognised state (D,D,0), (D,0,d) and (0,D,d), and final state (D,D,d) are found from the postulate. Any antecedent state (0,0,0), (D,0,0), (0,D,0) or (0,0,d) is not recognised as a single system state.

9.4.5.3 Ch 1 D failure and Ch 2 UD failure part

Similarly, recognised state (D,0,d) and final state (D,u,d) are found for this part. Any antecedent state (0,0,0), (0,u,0), (D,0,0), (D,u,0), (0,0,d) or (0,u,d) is not recognised as a single system state.

9.4.5.4 Ch 1 UD failure and Ch 2 D failure part

Similarly, recognised state (0,D,d) and final state (u,D,d) are found at this part. Any antecedent state (0,0,0), (u,0,0), (0,D,0), (u,D,0), (0,0,d) or (u,0,d) is not recognised as a single system state.

9.4.5.5 Ch 1 UD failure and Ch 2 UD failure part

Similarly, final state (u,u,d) is found, and any antecedent state (0,0,0), (u,0,0), (0,u,0), (u,u,0), (0,0,d), (u,0,d) or (0,u,d) is not recognised as a single system state at this part.

9.4.5.6 Common cause failures part with UD and D failures

At this part, recognised state (0,d) and (D,0), and final state (u,d) and (D,d) are found in a similar manner to the independent failure parts above. Antecedent state (0,0) or (u,0) is not recognised as a single system state from the postulate (see 9.4.5.1). Here

(0,d) FPL is not in any common cause faults under a demand state;

(D,0) FPL is in common cause D faults under a non-demand state;

(0,0) FPL is not in any common cause faults under a non-demand state;

(u,d) FPL is in common cause UD faults under a demand state;

(D,d) FPL is in common cause D faults under a demand state.

9.4.6 Recognised (group) states and final states for the overall system

For the overall system analysed in 9.4.5.2 to 9.4.5.6, the system states of the overall system are identified comprehensively by system state (0,x,y,z), (D,x,y,z) and (u,x,y,z), which means that the FPL is not in any common cause faults, in a common cause D faults and in a common cause UD faults, given that the independent parts of Ch 1 and Ch 2 and demand are indicated by system state (x,y,z), respectively (see Figure 24 for symbol (x,y,z)). Namely x and y are put as “0”, “D” or “u” to indicate an UP state, D fault or UD fault, respectively, and z is put as “0” or “d” to indicate the non-demand state or demand state, respectively.

Following the recognised states, the recognised group states of G1, G2, G3 and G4, the final states and the operating system states are summarised for the overall system (see 9.4.5):

1) recognised states are (D,0,0,0), (0,D,D,0), (0,D,0,d) and (0,0,D,d);
2) G1 includes system states of (0,0,0,0), (u,0,0,0), (0,u,0,0), (0,0,u,0) and (0,u,u,0);
3) G2 includes system states of (0,0,0,d), (0,u,0,d) and (0,0,u,d);
4) G3 includes system states of (0,D,0,0) and (0,D,u,0);
5) G4 includes system states of (0,0,D,0) and (0,u,D,0);

6) final states are (u,0,0,d), (D,0,0,d), (0,u,u,d), (0,u,D,d), (0,D,u,d) and (0,D,D,d);

7) operating system states are (0,0,0,d), (0,D,0,d), (0,0,D,d), (0,u,0,d) and (0,0,u,d).

The FER at a recognised state and FER at a recognised group state can be analysed and estimated for those recognised states (D,0,0,0), (0,D,D,0), (0,D,0,d) and (0,0,D,d), and recognised group states G1, G2, G3 and G4 in accordance with the procedure illustrated in 9.3.2 to 9.4.4.

9.5 Common cause failures between protection layers and complexity of a system

The possibility of CCF will be a factor of complexity of an overall system. The CCF between not only multiple Chs for a proactive function(s) in a PL but also multiple PLs that may involve original demand sources should be considered. Generally it can be said that the overall system with CCF between multiple PLs will be more complex than that without those CCF.

There can be two types of CCF between multiple PLs, i.e., the predictive and unpredicted. The risk owing to the predictive or known CCF is categorised into the controlled or uncontrolled event risk, and therefore should be included in the scope of this document (see Table 1).

The risks owing to the unpredicted or unknown CCF are categorised as meta-risks, and therefore are beyond the scope of this document (see Table 1). The overall system that can be regarded to contain unknown CCF between multiple PLs will be more complex than that without those CCF.

The predictive CCF between multiple PLs can be treated in a similar manner to that shown in 9.3 and 9.4.

9.6 Summary and remarks

The holistic and integrated approach involving the estimation of FER at a given initial state, FER at a given recognised state and FER at a recognised group state provided by this document is sufficiently powerful to analyse the risks of complex systems that contain electrotechnical items quantitatively or probabilistically as demonstrated in Clause 9.

The int. PLs are assumed to be arranged in arbitrary architecture systems in 9.2, however the FPLs are arranged in the 1-out-of-1 or 1-out-of-2 architecture systems in the examples illustrated in 9.3 and 9.4. The FPLs may be constructed by redundancy in a more complicated way. Then the FTs and state transition models described in those examples of FPLs can be modified and/or remodelled more realistically in such a case.

It would still involve more of an art rather than a science to develop realistic models for risk analysis. It depends on the skill of the analysts whether the developed model is appropriate or not for the risk analysis. A number of articles included in the Bibliography will contribute toward the enhancement of the skill of the risk analysts.

Annex A
(informative)

Risk owing to fault recognised only by demand

A.1 Demand, detection and failure logic

When a fault in an item is not detected by diagnostic tests or proof tests, the fault may be found or recognised by other methods arising from an int. event such as a demand that could activate the function(s) of the item to make the item in an operating state (see 9.3). However, if the fault is not recognised by those methods including overhauls, it will remain for the life of the item. In Annex A an example of risk analysis of an FPL with faults recognised only by demand (hereafter referred to as DU faults) will be demonstrated.

Consider DU faults in an FPL that are revealed only when the FPL is demanded. The demand and completion are assumed to follow the exponential distributions with demand rate λ_M [1/h] and completion rate μ_M [1/h], respectively. The FPL is assumed to be arranged in the 1-out-of-2 architecture system with the independent failure parts of Ch 1 and Ch 2, and the CCF part as shown in Figure A.1 (see 9.4). It is also assumed that if a demand occurs when the FPL is in a DU fault or if the FPL fails under a demand state, an unrepeatable final event occurs. This final event is analysed and expressed by use of an FT as shown in Figure A.2 [33].

The top event of the FT occurs if common cause DU failures and a demand occur (i.e., failure logic #1) or if independent DU failures and a demand occur (i.e., failure logic #2). The failure logics #1 and #2 are further developed as sequential failure logics #1-1 and #1-2, and sequential failure logics #2-1 through #2-6, respectively. It can be clarified through the FTA whether those failure logics can or cannot bring about the final state in which the final consequences of risk appear.

a) Logic #1-1: Common cause DU failures occur under a demand state.

   Logic #1-2: A demand occurs in common cause DU faults.

   The top event occurs if either sequential failure logic #1-1 or #1-2 is true.

b) Logic #2-1: A demand occurs at first, then an independent DU failure of Ch 1 happens and finally an independent DU failure of Ch 2 occurs in both of the demand state and independent DU fault of Ch 1.

   Logic #2-2: A demand occurs at first, then an independent DU failure of Ch 2 happens and finally an independent DU failure of Ch 1 occurs in both of the demand state and independent DU fault of Ch 2.

   The other sequential failure logics #2-3 through #2-6 are analysed in the same manner, and the top event is confirmed to occur if one of the six sequential failure logics #2-1 through #2-6 becomes true.

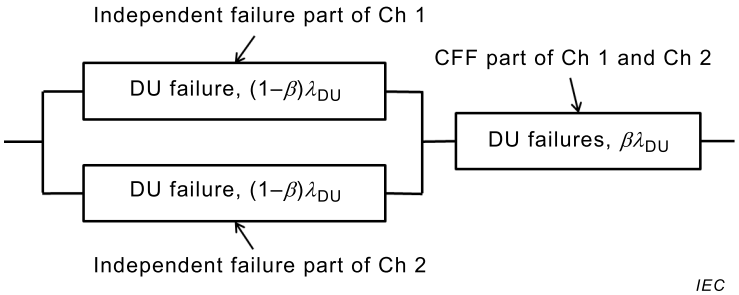


Figure A.1 – Reliability bock diagram with independent and common cause failures

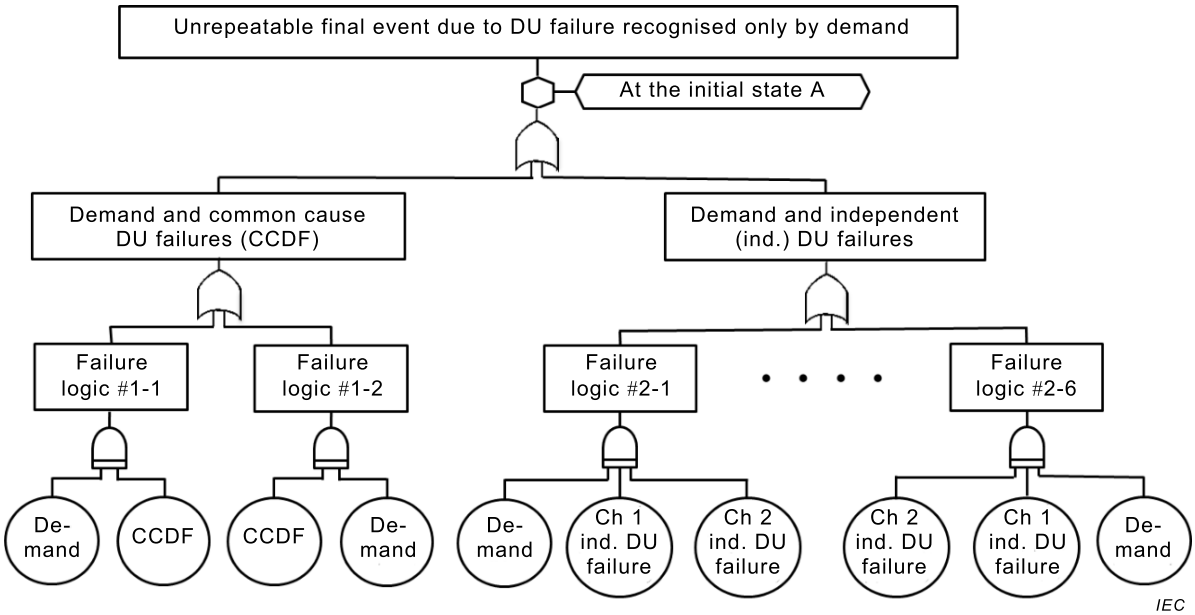
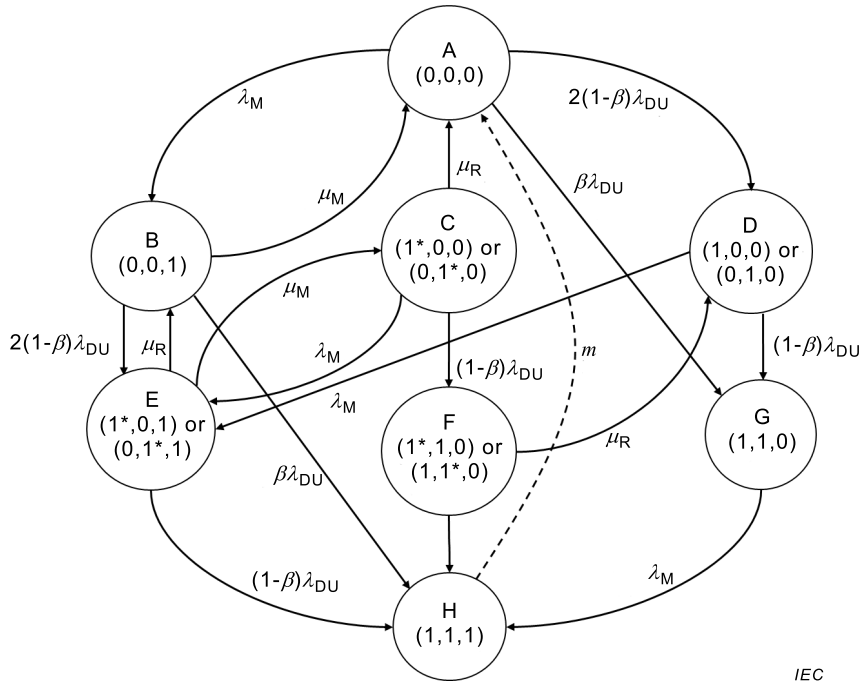


Figure A.2 – Fault tree of unrepeatable final event due to DU failures



X =	0: Ch 1 is UP.
	1: Ch 1 is in a DU fault and is not being restored.
	1*: Ch 1 is in a DU fault and is being restored.
Y =	0: Ch 2 is UP.
	1: Ch 2 is in a DU fault and is not being restored.
	1*: Ch 2 is in a DU fault and is being restored.
Z =	0: The overall system is in a non-demand state.
	1: The overall system is in a demand state.

Figure A.3 – State transition model for unrepeatable final event caused by DU failures

The Chs have an identical rate of DU failure that is recognised only by demand, and an identical rate of restoration. The DU failure and restoration follow the exponential distributions with constant DU failure rate λ_{DU} [1/h] and repair rate μ_R [1/h]. The rate of independent DU failure of the Ch is $(1\text{-}\beta)\lambda_{DU}$ and the rate of the common cause DU failures is $\beta\lambda_{DU}$ [1/h]. Here symbol β is the beta factor of the Chs, but $0 \leq \beta < 1$, $0 < \lambda_M$, $0 < \mu_M$, $0 < \lambda_{DU}$ and $0 < \mu_R$ hold.

A state transition model is developed in Figure A.3 based on the analysis of the RBD [8] and FTA above (see Table 4), given that the probability that both an independent failure and a CCF occur during a period of time is negligible compared with the probability that the CCF occurs solely during the same period. Eight sequential failure logics are contained in the model, and twelve system states A through H are defined by notation (X, Y, Z) as shown in Figure A.3.

A.2 Final event rate at a given initial state

In Figure A.3, system state (0,0,0) is the initial state A, and system state (1,1,1) is the unrepeatable final state H. Here P_K is defined as the probability that the overall system is in system state K (: B, E, F, G or H) in a steady state.

From Figure A.3, the FEF at initial state A, ω_C [1/h], is expressed in the following equation with system state probabilities and event rates [33]:

$$\omega_C = \beta\lambda_{DU} \cdot P_B + (1-\beta)\lambda_{DU} \cdot P_E + \lambda_M \cdot P_F + \lambda_M \cdot P_G (= m \cdot P_H) \quad \text{(A.1)}$$

From the above equation ω_C can be expressed as

$$\omega_C = X_0 / (1 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_0 / m) \quad \text{(A.2)}$$

Here,

$$X_0 = \beta\lambda_{DU} \cdot X_3 + (1-\beta)\lambda_{DU} \cdot X_1 + \lambda_M (X_2 + X_6)$$

$$X_1 = \{\mu_R + \lambda_M + (1-\beta)\lambda_{DU}\} / \mu_M$$

$$X_2 = (1-\beta)\lambda_{DU} / (\lambda_M + \mu_R)$$

$$X_3 = \{2(1-\beta)\lambda_{DU}\mu_R X_1 - \lambda_M \mu_R X_2\} / 2(1-\beta)\lambda_{DU}[\{2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\} + \{(1-\beta)\lambda_{DU} + \lambda_M\}]$$

$$+ [X_1\{\mu_R + \mu_M + (1-\beta)\lambda_{DU}\} - \lambda_M]\{\lambda_M + (1-\beta)\lambda_{DU}\} / 2(1-\beta)\lambda_{DU}[\{2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\} + \{(1-\beta)\lambda_{DU} + \lambda_M\}]$$

$$X_4 = [X_1\{\mu_R + \mu_M + (1-\beta)\lambda_{DU}\} - \lambda_M]\{2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\}$$

$$/[\lambda_M\{2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\} + \lambda_M\{(1-\beta)\lambda_{DU} + \lambda_M\}]$$

$$+ \{-2(1-\beta)\lambda_{DU}\mu_R X_1 + \lambda_M \mu_R X_2\} / [\lambda_M\{2(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + \mu_M\} + \lambda_M\{(1-\beta)\lambda_{DU} + \lambda_M\}]$$

$$X_5 = \{\mu_M \cdot X_3 + \mu_R + \beta\lambda_{DU} \cdot X_3 + (1-\beta)\lambda_{DU} \cdot X_1 + \lambda_M \cdot X_2 + (1-\beta)\lambda_{DU} \cdot X_4\} / \{2(1-\beta)\lambda_{DU} + \lambda_M\}$$

$$X_6 = \{(1-\beta)\lambda_{DU} \cdot X_4 + \beta\lambda_{DU} \cdot X_5\} / \lambda_M$$

Thus, FER at initial state A, r [1/h], is formulated as:

$$r = \omega_C / (1 - P_H) = \lim_{m \to \infty} X_0 / (1 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_0 / m)$$

$$= \{(1-\beta)\lambda_{DU} \cdot X_1 + \beta\lambda_{DU} \cdot X_3 + \lambda_M (X_2 + X_6)\} / (1 + X_1 + X_2 + X_3 + X_4 + X_5 + X_6) \quad \text{(A.3)}$$

A.3 Comparison between new and conventional analyses

Figure A.4 shows the relationship between the variable of the demand rate λ_M and the FER at initial state A, r, expressed in a function of λ_M, i.e., $r(\lambda_M)$, putting other variables (or parameters) as $\lambda_{DU} = 10^{-6}$ [1/h], $\mu_R = 10^{-1}$ [1/h] and $\mu_M = 10$ [1/h], and putting β at 10 %, 1 % and 0 %, respectively.

In Figure A.4 the loci represented by the broken curves are calculated by use of the formulas given in Clause A.2 and those represented by the straight real lines are calculated by the conventional analysis as shown below.

In IEC 61508-1, IEC 61508-5 and IEC 61508-6, HER, ϖ [1/h], is the target measure of occurrence of a final event (see 3.1.25, Note 2, and Clause B.1) [37][43][44]. Thus the FER at a given initial state refers to the HER in those parts of IEC 61508. The HER ϖ can be formulated by the use of PFD_{avg}, P_a, and demand rate, λ_M [1/h], for the low demand mode of operation [44]. In accordance with IEC 61508-6:2010, B.3.2.5, the HER ϖ is expressed in the following equations for the safety-related item that is arranged in a 1-out-of-2 architecture system with the DU failures shown in Figure A.1 [37]:

$$\varpi = \lambda_M P_a \tag{A.4}$$

where

$P_a = 2((1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta\lambda_{DU}(T_2/2+1/\mu_R)$

and

$t_{CE} = (T_2/2+1/\mu_R)$;

$t_{GE} = (T_2/3+1/\mu_R)$;

$T_2 = 1/\lambda_M$ [h] (mean time to demand);

$1/\mu_R$ is MRT [h] (mean restoration time).

The following can be said for the formulation of IEC 61508-6 [37].

a) Firstly, it is noted that the formulation in IEC 61508-6 is applicable to the low demand mode of operation only and the first order approximation, $\exp\{-\lambda_{DU}T_2\} \approx 1-\lambda_{DU}T_2$, is applied to the formulation. Therefore both of the conditions of the low demand mode of operation, i.e., $\lambda_M \leq 10^{-4}$ [1/h], and the first order approximation, i.e., $\lambda_{DU}T_2 << 1$ (namely, $\lambda_{DU} << \lambda_M$) should be satisfied for the demand rate.

b) Then, if the value of λ_{DU} is, for instance, 10^{-6} [1/h], the value of λ_M should be $10^{-6} << \lambda_M \leq 10^{-4}$ [1/h], namely almost between 10^{-5} and 10^{-4} [1/h].

Thus, it seems that the formula of IEC 61508-6 can be applied within a very limited range of the demand rate (see Figure A.4).

On the other hand, the whole range of the demand rate can be covered by the analysis of this document as shown in Figure A.4.

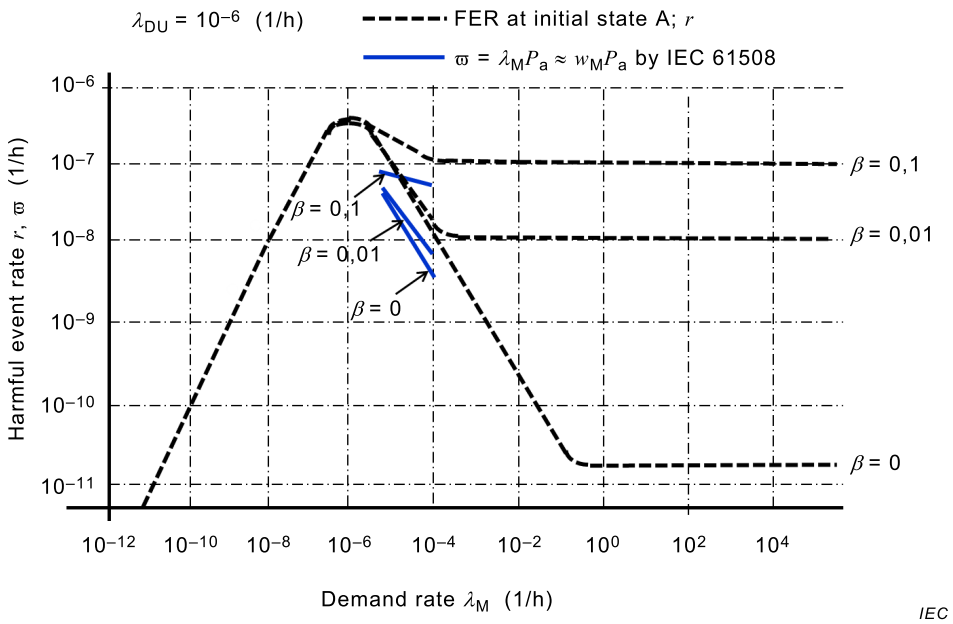


Figure A.4 – Comparison between analyses of $r(\lambda_M)$ and ϖ

The following view is presented by the analysis of this document [33].

a) If the demand rate becomes sufficiently low, then the HER approaches the demand rate, i.e., $r(\lambda_M) \approx \lambda_M$.

b) If the demand rate is sufficiently high, the formula $r(\lambda_M) \approx 2\{(1-\beta)\lambda_{DU}\}^2/\{(1-\beta)\lambda_{DU}+\mu_R\}+\beta\lambda_{DU}$, holds, and this means that $r(\lambda_M) \approx 2\{(1-\beta)\lambda_{DU}\}^2/\mu_R+\beta\lambda_{DU}$ holds given that $\lambda_{DU} << \mu_R$ holds, or, $r(\lambda_M) \approx (2-\beta)\lambda_{DU}$ holds given that $\mu_R << \lambda_{DU}$ holds.

c) It is generally believed that, if a measure of CCF of a multiple-Ch system such as beta factor β is estimated at several per cent or more, the CCF will be dominant over the system failure (i.e., the HER) (see 9.3 and Clause B.4). However, this is not always true. Although the CCF are almost dominant over the HER in the region of high demand rate (i.e., where the demand rate is higher than nearly 10^{-2} [1/h]), the HER is almost not affected by β in the region of the low demand rate (i.e., where the demand rate is lower than nearly 10^{-6} [1/h]) as shown in Figure A.4.

d) If the tolerable HER for the risk is put at 2×10^{-7} [1/h], then the tolerable HER will not be satisfied at the demand rate between 2×10^{-7} [1/h] and 2×10^{-5} [1/h] as well as between 2×10^{-7} [1/h] and 7×10^{-6} [1/h] by the item where β is put at 0,1 and 0,01, respectively.

e) It seems that $\varpi(\lambda_M) \approx (1/2)(1/3)r(\lambda_M)$ holds for the values of λ_M between 10^{-5} and 10^{-4} [1/h]. It is suggested that the coefficients (1/2) and (1/3) placed before T_2 in the formulas given in IEC 61508-6:2010, B.3.2.5, should be removed.

A.4 Further development

Risk exposure time T is assumed to be infinite in the above analyses corresponding to the postulate for the estimation of PFD_G and ϖ in IEC 61508-6 [37].

However, if the risk exposure time affects the HER significantly, the state transition diagram in Figure A.3 can be modified for more realistic analysis. If $0 \leq \beta < 1$, $\lambda_{DU} << 1/T$, $1/T << \mu_R$ and $1/T << \mu_M$ hold, for instance, state transitions D to A and G to A with a state transition rate of $2/T$ should be inserted in the diagram.

Thus the FER at the initial state A can be formulated more realistically based on the modified diagram.

A.5 Summary and remarks

If a fault in an item is detected by either diagnostic or proof tests and restored quickly, the impact on the HER made by the demand (by which the fault is recognised and restored) may be negligible compared to the effect of detection on the restoration made by those diagnostic or proof tests, especially in a region of low demand rate. If this is true, the HER that is expressed in a function of the demand rate λ_M, $r(\lambda_M)$, will be continuous and monotonically increasing for the variable λ_M (see Figure B.1).

A type of voting system votes those outputs from their independent Chs to generate normal output to an overall system. If the outputs from the independent Chs are generated by the demand at the Chs, there can be cases where the impact on the HER made by the demand can hardly be neglected in the overall system [30][31][32].

a) It is quite in the natural order of things to suppose that various kinds of faults such as D, UD and DU faults are generally contained in complex items. Thus, the HER function $r(\lambda_M)$ could have (an) inflection point(s), namely, $r(\lambda_M)$ will not be monotonically increasing for the variable λ_M in the overall system (see Clauses B.4 and B.5). This means that the HER in the region of int. demand rate can be higher than those in regions of higher and/or lower demand rates (see Figure A.4).

b) Discussions on the complexity of an overall system should include the complexity in the context of HER function $r(\lambda_M)$. Namely, it can be said that an overall system where $r(\lambda_M)$ is not a monotonically increasing function will be more complex compared to that where $r(\lambda_M)$ is monotonically increasing for the variable λ_M in the perspective of risk analysis (see Clause 6, 9.1, 9.2, 9.5, and Clause B.3).

Thus, it is demonstrated in Annex A that the approach presented by this document is sufficiently powerful to cope with the complex systems where HER functions are not only monotonically increasing but also not monotonically increasing for the variable λ_M easily and rationally.

Annex B
(informative)

Application to functional safety

B.1 Risk-based target failure measures in functional safety

Most technologies for quantitative risk analysis originated in the field of system safety and have been developed by bringing both fields of the system safety and reliability (or dependability) together [14][17].

The risk-based safety standards of the IEC 61508 series were published and have been widely applied to various sectors such as the process, railroad, machinery, medical electrical equipment, automobile and robotics industries [10]. The IEC 61508 series specifies a risk-based quantitative measure of performance of safety-related items called safety integrity. Target failure measures of the safety integrity are

– the average probability of failure on demand (PFD_{avg}), P_a, for the safety-related item in a low demand mode of operation;
– the average frequency of dangerous failure per hour (PFH), $\underline{\lambda}$ [1/h], for the safety-related item in a high demand mode or continuous operation.

Those target failure measures specify the performance of safety-related items called E/E/PE safety-related systems to control and/or reduce safety-related risks in order that the residual risks become tolerable or acceptable levels (see 3.1.1, Note 3, 3.1.32 and 3.1.33).

One side of the elements of safety-related risk, namely, the probability of harm, is measured by HER, φ [1/h], and this is the quantitative target measure of the safety-related risk to be controlled and/or reduced by the E/E/PE safety-related system in IEC 61508 (all parts) (see 3.1.1, Note 2, and 3.1.25, Note 2). The relationships between PFD_{avg} (i.e., P_a), PFH (i.e., $\underline{\lambda}$) and φ are described in IEC 61508-6 as

– $\varphi \approx P_a \lambda_M \approx P_a w_M$ for the item in the low demand mode of operation;
– $\varphi \approx \underline{\lambda}$ for the item in the high demand mode of/continuous operation.

Here, λ_M and w_M are the demand rate and demand frequency, respectively (see notations in 9.1).

At the very early stage of drafting of the first edition of IEC 61508 [39][41], the HER was calculated using the formula $\varphi \approx P_a \lambda_M \approx P_a w_M$ only. Namely, the target failure measure of E/E/PE safety-related systems was only PFD_{avg} (see 9.3.2). The feasibility of the formulation was studied in the field of machinery where the demand rate was significantly high, for instance, $\lambda_M \approx w_M \approx 1\ 000$ [1/h] and $\varphi \approx P_a \lambda_M \approx P_a w_M \approx 1{,}0$ [1/h]. The research findings showed that those values of HER estimated by the formula were much higher than those statistical data collected in this field.

The ideas were then established as follows:

a) If the E/E/PE safety-related system is operated continuously or in sufficiently high demand rates, the HER φ owing to the dangerous failure of E/E/PE safety-related system would approximate to its dangerous failure rate $\underline{\lambda}$ [1/h] because the dangerous failure will result in a harmful event immediately.
b) From that idea three kinds of mode of operation, i.e., a low demand mode (i.e., conventional one), high demand mode of operation and continuous operation (i.e., newly introduced ones), were adopted into the early draft standard of the first edition of IEC 61508 [39][41].

c) The formula $\varphi \approx P_a \lambda_M \approx P_a w_M$ was assigned to the low demand mode of operation and the formula $\varphi \approx \underline{\lambda}$ to the two newly introduced modes of operation, i.e., the high demand mode of operation and continuous operation.

Thus, in the early CD (Committee Draft) stage of the first edition of IEC 61508-4 [41], the low demand mode of operation was defined as “the mode of operation where the demand rate is sufficiently low”, and the high demand mode of operation as “the mode of operation where the demand rate is sufficiently high”, respectively. Here, it is noted that in this document a failure means a dangerous failure in case of the application to safety (see Clause B.2).

While some experts asked: “How shall we address the intermediate region where the demand rate is neither sufficiently low nor sufficiently high?” this issue was resolved by:

– drawing a line of demarcation between the low demand mode and the high demand mode of operation;

– expanding the regions of those modes of operation into the new regions involving those intermediate sections on both sides of the line, respectively.

The low demand mode of operation was defined in the first edition of IEC 61508-4 as the mode of operation “where the frequency of demands for operation made on a safety-related system is no greater that one per year and no greater than twice the proof test frequency”. The demand frequency of one per year approximately equals $w_M \approx \lambda_M \approx 10^{-4}$ [1/h]. Here w_M and λ_M are constant demand frequency and rate, respectively. The first editions of IEC 61508-1 and IEC 61508-4 were published in 1998 [39][41].

Currently the low demand mode operation is defined in the second edition of IEC 61508-4 as the mode of operation “where the safety function only performs on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year” [40].

Then the reasons why formula, $\varphi \approx P_a \lambda_M \approx P_a w_M$, can hardly be applied to the E/E/PE safety-related systems operated in the high demand/continuous mode of operation became clear later.

a) The formula $\varphi \approx P_a \lambda_M \approx P_a w_M$ holds approximately for both of repeatable and unrepeatable final events, given that the demand rate is sufficiently low and the completion rate is sufficiently high. However, the formulation hardly applies to the unrepeatable final event if the demand rate is not sufficiently low or the completion rate is not sufficiently high [17][18][19].

b) The formulation hardly applies to such a specific case as the airbag control system for automobiles or the overall system described in Annex A (see 7.2.3, 9.3.2) [31][33].

c) Which mode of operation should be adapted to a system depends on the relationships between the demand rate and HER, and therefore the choice between modes of operation should be based on not only the demand rate but also on such parameters as completion rates, failure and repair rates of items and risk exposure time (see 7.2.3, and clauses B.4 to B.8) [18][19][20][22][23][33].

d) The harmful events in the machinery sector, where the demand rates are significantly high, can be judged to be unrepeatable final events.

B.2 Safe/dangerous system states and failures

An E/E/PE safety-related system performs (a) safety function(s) to maintain (a) safe system state(s) of an overall system in order that (a) residual safety-related risk(s) is/are kept at a tolerable level (see 3.1.1, Note 3). Generally if an item that composes an E/E/PE safety-related system fails, the failure could show a number of failure modes. Those failure modes are categorised into a safe mode and a dangerous mode in the context of safe/dangerous system states. Thus the failure resulting in the safe mode or the dangerous mode is simply called a safe failure or a dangerous failure, respectively [10][40].

a) The safe failure is defined as the failure that results in the spurious operation of the safety function(s) or in the increment of the probability of the spurious operation, maintaining the safe system state(s) of the overall system, and consequently the safe system state remains [40].

b) The dangerous failure is defined as the failure that prevents a safety function from operating or decreases the probability that the safety function(s) operates correctly when required [40].

c) The safe state is defined as the system state of a targeted overall system when safety is achieved, i.e., when (a) safety-related risk(s) is/are kept at (an) acceptable level(s).

For example, int. state D in Figure 10 means that an airbag control system is in a shutdown state. It will be clear that the FER at int. state D is smaller than the FER at initial state A, namely, the D failure that brings the airbag control system to a shutdown state is a safe failure, given that initial state A is a safe system state. On the other hand, if the FER at int. state C is larger than the FER at initial state A, the UD failure could be a dangerous failure that brings the overall system to the system state with a higher level of risk compared to initial state A.

Generally, from the perspective of safe and dangerous failures of safety-related items that compose an E/E/PE safety-related system, the safe system states of overall systems are classified into the following three types [27]:

– invariable;

– intrinsically variable;

– reciprocally variable.

Suppose that an E/E/PE safety-related system has to cope with one or more hazards in order to achieve safe system states of an overall system, then the following can be said:

1) If a safe system state for a hazard (or a risk) is achieved by an E/E/PE safety-related system being in an activated or an inert state only, and this feature of the E/E/PE safety-related system does not change while the overall system is exposed to the hazard (or risk), then this safe system state is invariable in the context of both of the hazard (or the risk) and the failure of the E/E/PE safety-related system (see 3.1.2.2, Notes 1 to 3). When an E/E/PE safety-related system maintains an invariable safe system state, it may suffer both of safe and dangerous failures. Some chemical process plants would involve safety-instrument systems (i.e., a kind of E/E/PE safety-related system) with typical examples of this invariable safe system state [27].

2) If a safe system state for a hazard (or a risk) is achieved by an E/E/PE safety-related system changing from an activated to an inert state or from an inert to an activated state or both while the overall system is exposed to the hazard (or the risk), then the safe system state is intrinsically variable in the context of both of the hazard (or the risk) and the failure of the E/E/PE safety-related system. When an E/E/PE safety-related system has to maintain an intrinsically variable safe system state, then it could not have any safe failures. For example, an automated steering control system for self-driving cars (i.e., a typical E/E/PE safety-related system) is composed of electrotechnical items such as sensors, controllers and actuators (see 9.1). It controls the courses of the automobile according to variable circumstances to create safe courses, where the safe system state, i.e., the safe course is intrinsically variable. Therefore, any failure of the automated steering control system could be dangerous because the safe system state is intrinsically variable [27][30].

3) Suppose that a failure of an E/E/PE safety-related system is related to safe system state S1 against hazard H1 (or risk R1) and safe system state S2 against hazard H2 (or risk R2), and S1 is an invariable safe system state achieved by the E/E/PE safety-related system being an activated or an inert state. Thus if S2 is an invariable safe system state achieved by the E/E/PE safety-related system being an inert or activated state, or if S2 is intrinsically variable, the overall system is defined as being in reciprocally variable safe system states against H1 (or R1) and H2 (or R2), and the hazards of H1 and H2 are defined as mutually reciprocal hazards in the context of the failure of the E/E/PE safety-

related system of concern. The safe system state of the overall system is to be changed against the reciprocal hazards, i.e., the safe system states against reciprocal hazards are reciprocally variable. If an E/E/PE safety-related system has to maintain the reciprocally variable safe system states of S1 and S2, then its safe failure for S1 will be dangerous for S2 (see for example Table B.1) [27][30][31][32].

For example if an automated brake control system for self-driving cars, which is composed of such electrotechnical items as sensors, controllers and actuators fails to stop the automobile approaching dangerously another automobile in front, then a rear-end collision will occur whereas if the automated brake control system fails and stops the automobile suddenly and unnecessarily, it could be struck from behind. Therefore, both hazards of rear-end collision and being struck from behind are mutually reciprocal hazards regarding the failure of the automated brake control system, and the safe system states against those reciprocal hazards are reciprocally variable. Thus, the automated brake control system for self-driving cars has to cope with the reciprocally variable safe system states for such mutually reciprocal hazards as

– the primary hazard caused by the failure to stop the automobile;

– the reciprocal hazard caused by bringing unnecessarily the automobile to a stop.

Table B.1 shows the relationships between the failure modes of the automated brake control system, mutually reciprocal hazards, and safe and dangerous failures [32].

Table B.1 – Relationship between failure modes, hazards, and safe/dangerous failures

Hazards to be controlled by an automated brake control system	Failure modes of an automated brake control system for a self-driving car	
	Failure mode 1 (e.g., short–circuit)	Failure mode 2 (e.g., disconnection)
Primary hazard	Safe failure	Dangerous failure
Reciprocal hazard	Dangerous failure	Safe failure

In general, the following can be said for the safety-related item [31][32].

– If the item is arranged in a 1-out-of-2 architecture system for a primary hazard, then it will be structured in a 2-out-of-2 architecture system for a reciprocal hazard.

– If tolerable risk levels are set up to respective reciprocal hazards, the architecture and the profile of failure rates and failure modes of the safety-related items will be designed to satisfy those tolerable risk levels coincidentally based on analyses of FER at a given initial state.

B.3 Complexity of safety-related systems

The complexity of a safety-related system will depend not only on the scale of the overall system, i.e., the amount of components and hazards created by the overall system and CCF between PLs involving original demand sources but also on the complexity of failure logics such as sequential failure logics that dominate the occurrence of the final event resulting in the appearance of final consequences of the risk (see Clause 6, 9.1, 9.2, 9.5 and Clause A.5). In addition, the complexity of safe system states should be taken into account for the discussion about the complexity of safety-related systems. The following can be said on the complexity:

a) The overall system with intrinsically variable and/or reciprocally variable safe system states is of higher complexity compared to that only with invariable safe system states.

b) The safety-related system with all kinds of faults such as D, UD and DU faults is of higher complexity compared to that only with limited types of faults (see Clause A.5).

c) The safety-related system with the items of which failure rates vary between the operating and non-operating states of the items is of higher complexity compared to that only with

the items of which failure rates are invariable, however this is out of the scope of this document (see Figure 15 and 9.3.1) [24][26].

d) A possibility that a meta-risk could be contained in the overall system will be another factor of the complexity of the overall system, however this is out of the scope of this document (see Table 1, Clause 6, 9.1, 9.2, 9.5 and Clause A.5).

B.4 Comparison between conventional and new analyses

Figure B.1 typically illustrates the relationship between the variable of the demand rate, λ_M, and the HER that is expressed in a function of λ_M, $\varphi(\lambda_M)$, fixing a systems architecture and other variables (or parameters) such as failure/repair and completion rates at certain conditions in an overall system including an E/E/PE safety-related system that carries out a safety function of an FPL.

In the figure, the horizontal and vertical axes indicate the demand rate, λ_M, and HER, $\varphi(\lambda_M)$, respectively.

a) The straight solid line with slope and the horizontally straight line indicate the HER that could be calculated by the formulas, $\varphi(\lambda_M) \approx P_a \lambda_M \approx P_a w_M$ and $\varphi(\lambda_M) \approx \underline{\lambda}$, based on IEC 61508-6, respectively [37].

b) The curved loci expressed as Cases 1 to 3 indicate the HER $\varphi(\lambda_M)$ that could be calculated by use of the FER at an initial state provided by this document.

Because the HER is analysed separately using the two formulas in IEC 61508-1, IEC 61508-5 and IEC 61508-6, $\varphi(\lambda_M) \approx P_a \lambda_M \approx P_a w_M$, and, $\varphi(\lambda_M) \approx \underline{\lambda}$, for the low and high demand modes of operation respectively, there are often gaps disconnecting the HER of those two modes of operation as shown in Figure B.1 (hereafter referred to as conventional analysis).

The FER at a given initial state provides seamless and more realistic analyses regardless of the modes of operation for the HER shown as in the figure (hereafter referred to as new analysis), because not only the failure and repair rates of the systems but also all the parameters involving the demand and completion rates that affect the HER significantly are analysed holistically in the new analysis of this document. The following can be said.

– The formula $\varphi(\lambda_M) \approx \underline{\lambda}$ presents the upper limit of HER that may be adapted generally to the continuous mode of operation for the overall system where the HER is described in a monotonically increasing (hereafter referred to as m-increasing) function $\varphi(\lambda_M)$ under particular conditions.

– In Figure B.1, the curved loci that are denoted as Cases 1 to 3 are formed typically by m-increasing HER functions.

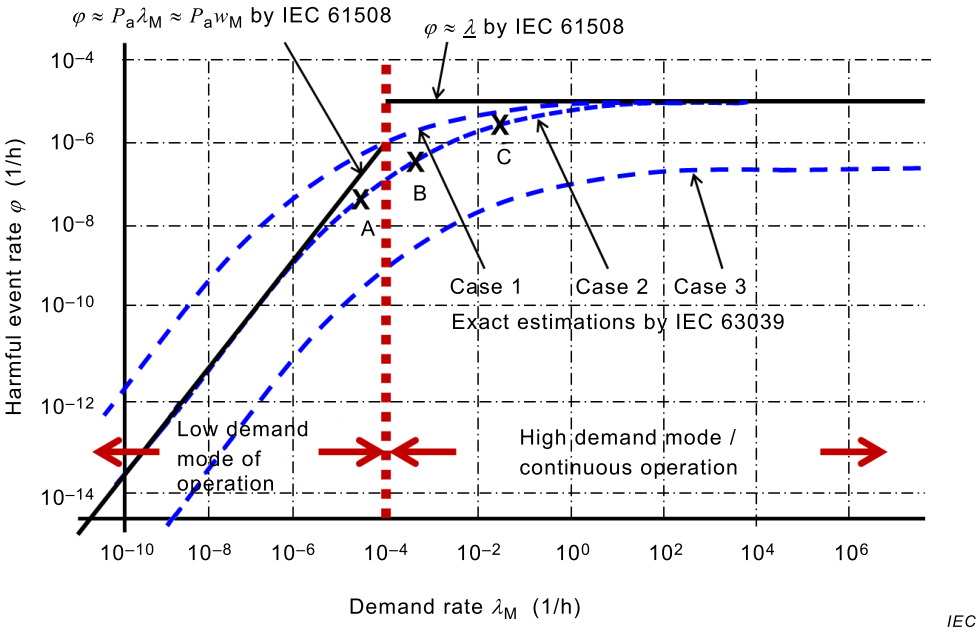


Figure B.1 – Comparison between conventional and new analyses

However, the formula $\varphi(\lambda_M) \approx \underline{\lambda}$ does not necessarily present the upper limit of HER for the overall systems where $\varphi(\lambda_M)$ is not an m-increasing function (see Figure A.4 and Clause A.5). Thus, there are significant differences between the conventional and new analyses.

1) If both of the target failure measures PFD_{avg} and APF_{drg} are dominant over the HER and if the demand rate becomes sufficiently high, then the FER at a given initial state tends to the target failure measure of PFH (see Case 1 in Figure B.1).
2) However, if only one of the target failure measures PFD_{avg} or APF_{drg} dominates the HER and if the demand rate becomes sufficiently high, then the new analysis, that provides the realistic and exact estimations of HER, may present much lower estimations than those approximations presented by the conventional analysis (see Case 3 in Figure B.1).
3) If the demand rate is sufficiently low and if only the target failure measure PFD_{avg} dominates the HER, the conventional analysis may provide good approximations to the HER (see Case 2 in Figure B.1).
4) However if both of the target failure measures PFD_{avg} and APF_{drg} are dominant over the HER, or if only the target failure measure APF_{drg} dominates the HER, then the new analyses could present much lower or higher estimations than those approximations provided by the conventional analyses, depending on the specific conditions of the overall system (see 7.2.3, 9.3.3, and Cases 1 and 3 in Figure B.1).

B.5 Splitting up mode of operation

Generally, HER, φ, can be mathematically a function of a significant number of variables (or parameters) such as failure/repair rates, demand rate λ_M, completion rate μ_M, demand frequency w_M, renewal rate m and risk exposure time T from the perspective of risk analysis (see for example Figure 10). If those variables except the demand rate λ_M are fixed at certain values, then φ is described in a function of the variable of λ_M, i.e., $\varphi = \varphi(\lambda_M)$ holds.

a) If the HER function $\varphi(\lambda_M)$ is continuous, monotonic and increasing, then the overall system will be called an m-increasing system for the risk of concern, and vice versa, that is typically shown as the curved loci, Cases 1 to 3, in Figure B.1.
b) However, $\varphi(\lambda_M)$ is not always monotonic for such an overall system as shown in Annex A, where (an) inflection point(s) exist(s) in the loci formed by λ_M and $\varphi(\lambda_M)$ (see Figure A.4) [30][31][32][33]. In such a case it will not be adequate to draw a line to split up the mode

of operation simply into two sections because the HER in the region of int. demand rate can be higher than the one in a region of higher demand rate and/or in a region of lower demand rate (see Figure A.4 and Clause A.5).

c) In that regard it is necessary to establish a procedure for choosing a suitable mode of operation in order that SIL-related requirements should be fulfilled appropriately in accordance with Table B.2 that is specified in IEC 61508 (all parts) (see Clause B.7) [10].

B.6 Tolerable hazardous/harmful event rate and residual risk

If an E/E/PE safety-related system carries out (a) safety function(s) of an FPL to keep a safe system state of an overall system, the residual risks resulting from the risk control/reduction achieved by the safety function are required to be lower than tolerable risk levels, i.e., the HERs due to the failure of the E/E/PE safety-related system have to be lower than tolerable levels.

a) Suppose for instance that an E/E/PE safety-related system is operated along the locus of Case 2 in Figure B.1 to control and reduce a risk of an overall system. Thus, three operating points A, B and C can be represented by a combination of λ_M [1/h] and φ [1/h], i.e., "λ_M and φ" as "3×10^{-5} and 4×10^{-8}", "4×10^{-4} and 3×10^{-7}", and "3×10^{-2} and 2×10^{-6}", respectively.

b) When the tolerable HER of the residual risk is, for instance, put at 10^{-6} [1/h], then the operating points A and B will satisfy the tolerable HER of the residual risk for safe operation, but the HER of the operating point C will not reach the tolerable level of the residual risk (see 3.1.1, Note 3).

B.7 Procedure for determining the safety integrity level (SIL) of an item

A resolution of the difficulty in coping with the target failure measures, modes of operation and determination of SIL mentioned above will be made by the approach provided by this document.

a) At first a target measure of the risk-reduction ratio, φ/λ_M, is introduced by use of FER at a given initial state as described in 7.2.3. Here, the symbol λ_M is the demand rate at a PL of concern. Symbol φ is the demand rate of the next PL if the PL of concern is an int. PL or the FER at a given initial state if the PL of concern is an FPL (see 9.2 and 9.3). The φ/λ_M and φ are risk-based generic target measures to assess the performance of items operating in the low demand mode and in the high demand/continuous mode, respectively. The PFD_{avg} and PFH in IEC 61508 (all parts) are the approximations of φ/λ_M and φ, respectively [10]. It is noted that the approximations are valid under particular circumstances as described above.

b) Based on the perspective above, a procedure for choosing between the modes of operation and determining the SIL of an item is as follows [23]:

   – adopt φ/λ_M and φ as the target failure measures of an item for the low demand mode of operation and for the high demand mode of/continuous operation, respectively;

   – select SIL X (X = 1, 2, 3 or 4) and SIL Y (Y = 1, 2, 3 or 4) by referring φ/λ_M and φ to Table B.2, respectively;

   – choose a lower SIL between the selected SIL X and SIL Y for the item if $X \neq Y$ holds;

   – choose SIL Y for the item if $X = Y$ holds (because the functional safety standards such as IEC 61508 (all parts) and IEC 61511 (all parts) usually burden the item assigned SIL Y with heavier requirements compared to the item assigned SIL X, given $X = Y$ holds) [10][42].

Table B.2 – Safety integrity levels (SILs) in IEC 61508 (all parts)

SIL	Target failure measures	
	Low demand mode of operation PFD_{avg} or risk reduction ratio φ/λ_M (SIL X)	High demand mode of/continuous operation PFH or hazardous/harmful event rate φ [1/h] (SIL Y)
4	$\geq 10^{-5}$ to $<10^{-4}$ C (SIL 4)	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-4}$ to $<10^{-3}$ B (SIL 3)	$\geq 10^{-8}$ to $<10^{-7}$ A (SIL 3)
2	$\geq 10^{-3}$ to $<10^{-2}$ A (SIL 2)	$\geq 10^{-7}$ to $<10^{-6}$ B (SIL 2)
1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$ C (SIL 1)

Suppose for instance that the combination of φ/λ_M (SIL X) and φ (SIL Y) [1/h], i.e., "φ/λ_M (SIL X) – φ (SIL Y)", is estimated at three operating points A, B and C along the locus expressed as Case 2 in Figure B.1 as follows:

1) "$1{,}3 \times 10^{-3}$ (SIL 2) – 4×10^{-8} (SIL 3)" at operating point A;
2) "$7{,}5 \times 10^{-4}$ (SIL 3) – 3×10^{-7} (SIL 2)" at operating point B;
3) "$6{,}6 \times 10^{-5}$ (SIL 4) – 2×10^{-6} (SIL 1)" at operating point C.

Thus the lower SIL between SIL X and SIL Y, namely, SIL 2 (SIL X), SIL 2 (SIL Y) and SIL 1 (SIL Y) are chosen for the items at operating points A, B and C, respectively. From the discussion in Clause B.6, it can be known that if an item is at operating point C (SIL 1), a higher SIL (maybe SIL 2) is to be allocated to the item to meet the tolerable level of the residual risk of the overall system.

B.8 Summary and remarks

This document helps to determine SILs rationally and appropriately for overall systems where their HERs are represented in not only m-increasing but also non-m-increasing functions for the variable λ_M as illustrated in Figure B.1 and Figure A.4 respectively.

Thus this document provides:

– the theoretical grounds of the relationship between the target failure measures of an item (e.g., an E/E/PE safety-related system) and the HER;
– the way to analyse the HER holistically and easily for the estimation of the performance of the item to control and/or reduce (a) risk(s);
– the guidance to evaluate and assess risks appropriately and to carry out functional safety assessment appropriately.

Bibliography

[1] ISO Guide 73:2009, *Risk management – Vocabulary*

[2] ISO 9000:2015, *Quality management systems – Fundamentals and vocabulary*

[3] ISO 31000:2009, *Risk management – Principles and guidelines*

[4] IEC/ISO 31010:2009*, Risk management – Risk assessment techniques*

[5] IEC 60050-192:2015, *International electrotechnical vocabulary – Part 192: Dependability*

[6] IEC 60300-3-1:2003*, Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

[7] IEC 61703:2001, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*

[8] IEC 61078:2006, *Analysis techniques for dependability – Reliability block diagram and Boolean methods*

[9] IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

[10] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[11] IEC 61882:2016, *Hazard and operability studies (HAZOP studies) - Application guide*

[12] Vesely, W.E., Narumu, R.E.: PREP and KITT; Computer cords for automatic evaluation of fault trees, IN-1349, 1970

[13] Fussell, J.B., Aber E.F., Rahl R.G.: On the quantitative analysis of priority AND failure logic, *IEEE Trans. Reliability*, Vol.R-25, No.5, 324-326, 1976

[14] Henley, E.J., Kumamoto, H., *Reliability Engineering and Risk Assessment*, Englewood Cliffs, Prentice Hall, 1981

[15] Sato, Y., Inoue, K., Kumamoto, H., The safety assessment of human-robot systems (3rd Report); On the quantification of consecutive failure logic, *Bulletin of JSME*, Vol.29, No.257, Nov., 3945-3951, 1986

[16] Sato, Y., Henley, E.J., Inoue, K.: An action-chain model for the design of hazard-control systems, *IEEE Trans. on Reliability*, Vol.39, No.2, 151-159, 1990

[17] Misumi, Y., Sato, Y., Estimation of average hazardous-event-frequency for allocation of safety-integrity, *Reliability Engineering & System Safety*, 66 (1999), 135-144, 1999

[18] Kawahara, T., Ichitsuka, A., Sato, Y.: State transition Model of Safety-Related Systems with Automatic Diagnosis and its Formulation for Functional Safety Assessment, *IEICE Trans.* Vol.J86-A, No.3, 241-249, March 2003

[19] Yoshimura, I., Sato, Y.: Safety-Integrity Levels Model for Safety-Related Systems in Dynamic Demand State, *IEICE Trans.* Vol.J86-A, No.11, 1188-1196, Nov. 2003

[20] Yoshimura, I., Sato, Y., Suyama, K.: Safety Integrity Level Model for Safety-related Systems in Dynamic Demand State, Proceedings of the 2004 Asian International Workshop on Advanced Reliability Modelling (AIWARM 2004), Hiroshima, 577–584, 2004

[21] Börcsök, J.: Functional Safety, Hüthig, 2005

[22] Shimodaira T., Sato, Y., Suyama, K.: Estimation of Hazardous Event Rate for Repairable *1-out-of-2* Safety-Related Systems Based on State transition Models, *IEICE Trans.* Vol.J88-A, No.8, 962-973, Aug. 2005

[23] Shimodaira T., Sato, Y., Suyama, K.: Estimation of Average Hazardous-Event Rate for Steady-State Demands and Determination of SIL, *JSME Trans.(C),* Vol.72, No.715, 953-959, March 2006

[24] Yoshimura, I., Sato, Y.: Safety-Integrity Levels of Safety-Related System with Self-diagnosis Functions in Dynamic Demand State, *Jour. Reliability Engineering Association of Japan,* Vol.151, No.3, 219-227, May 2006

[25] Braband, J.: Safety analysis based on IEC 61508 – Lessons Learned and Way Forward, Keynote talk at SAFECOMP 2006, Gdansk, http://kio.pg.gda.pl/safecomp2006/, 2006

[26] Yoshimura, I., Sato, Y.: Estimation of Hazardous Event Rate for Safety-Related Systems with Self-diagnosis Function, *Jour. Japan Society for Safety Engineering*, Vol.46, No.1, 16-23, Jan. 2007

[27] Yoshimura, I., Sato, Y.: Safety Achieved by the Safe Failure Fraction (SFF) in IEC 61508, *IEEE Trans. on Reliability*, Vol.57, No.4, 662-669, Dec. 2008

[28] Braband, J., Schäbe, H., vom Hövel, R.: Probability of Failure on Demand – the Why and the. in: Proc. SAFECOMP2009, Hamburg, 46-54, 2009

[29] Yoshimura, I., Sato, Y.: Estimation of Calendar-Time- and Process-Operative-Time-Hazardous-Event Rates for the Assessment of Fatal Risk, *Int. Jour. of Performability Engineering*, Vol.5, No. 4, July 2009, 377-386

[30] Kushibiki, T., Sato., Y.: Functional Safety Assessment of the Motor Vehicles Steer-by-Wire Systems with both Faults Detectable only by Demands and Commission Faults, *JSME Trans.(C),* Vol.76, No.762, 388-396, Feb. 2010

[31] Takeichi, M., Suyama, K., Sato Y.: Functional Safety Assessment of Air Bag Systems for Automobiles, *Trans. Soc. of Automotive Engs. of Japan*, Vol.44, No.2, 627-633, March 2013

[32] Takeichi, M., Suyama, K., Sato Y.: Functional Safety Assessment of Pre-Crash Systems for Reciprocal Hazards, *JSME Trans.(C),* Vol.79, No.806, 3839-3853, Oct. 2013

[33] Muta, H., Sato, Y.: Functional Safety Assessment of Safety-related Systems with Non-perfect Proof-tests, *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E97-A, No. 8, 1739-1746, Aug. 2014

[34] IEC 61025:2006, *Fault tree analysis (FTA)*

[35] IEC 61165:2006, *Application of Markov techniques*

[36] IEC 62502:2010, *Analysis techniques for dependability – Event tree analysis (ETA)*

[37] IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[38] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

[39] IEC 61508-1:1998[2], *Functional safety of electrical/electronic/programmable electronic safety-related system – Part 1: General requirements*

[40] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related system – Part 4: Definitions and abbreviations*

[41] IEC 61508-4:1998[3], *Functional safety of electrical/electronic/programmable electronic safety-related system – Part 4: Definitions and abbreviations*

[42] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

[43] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[44] IEC 61508-5, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

2 Withdrawn.

3 Withdrawn.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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