PD IEC/TR 63039:2016

BSI Standards Publication

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

bsi.

National foreword

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

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

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

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

Published by BSI Standards Limited 2016

ISBN 978 0 580 92982 3
ICS 03.120.01; 03.120.30

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

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

Amendments/corrigenda issued since publication

Date	Text affected

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

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