IEC TR 63192

Edition 1.0 2019-01

TECHNICAL REPORT

Nuclear power plants – Instrumentation and control systems important to safety – Hazard analysis: a review of current approaches

IEC TR 63192:2019-01(en)

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 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 TR 63192

Edition 1.0 2019-01

TECHNICAL REPORT

Nuclear power plants – Instrumentation and control systems important to safety – Hazard analysis: a review of current approaches

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.160

ISBN 978-2-8322-6408-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – HAZARD ANALYSIS: A REVIEW OF CURRENT APPROACHES

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 closely 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 are 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 be attached 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 63192, which is a technical report, has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

Draft TR	Report on voting
45A/1197/DTR	45A/1231/RVDTR

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

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

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

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

INTRODUCTION

a) Technical background, main issues and organisation of the document

The purpose of the TR is to identify the worldwide situation of HA requirements for digital I&C.

It is not the purpose of this technical report to reconcile the hazards analysis techniques and to harmonise the use of hazards analysis terminology between the many different approaches used by standards bodies (e.g. between the IEEE and IAEA), but rather to document the different approaches. The information provided can then be used to further the development of a consistent approach to hazards analysis within the IEC.

It is intended that this document be used by operators of NPPs (utilities), systems evaluators and by licensors.

b) Situation of the current document in the structure of the IEC SC 45A standard series

IEC 63192 as a Technical Report is a fourth level IEC/SC 45A document.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of the document

It is important to note that a technical report is entirely informative in nature. It gathers data collected from different origins and it establishes no requirements.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, security, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own. IEC 63096 refers in detail to a distinct version of ISO/IEC 27002. A later modification of ISO/IEC 27002 must not automatically influence the modifications, detailing and completions given by IEC 63096 without analysing the consequences from the nuclear I&C perspective.

A fourth level extending the IEC SC 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC/SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC/SC 45A control room standards and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC/SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC/SC 45A to decide how and where general requirements for the design of electrical systems were to be considered. IEC/SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 is published this NOTE 2 of the introduction of IEC/SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – HAZARD ANALYSIS: A REVIEW OF CURRENT APPROACHES

1 Scope

This document provides the comparison of the hazard analysis requirements between IAEA framework and NRC-IEEE framework of standards and guidance. The hazard analysis requirements in the different standards were compared with a set of comparison criteria, including the safety principle, the safety process, the definitions, the hazard analysis process, etc. This document includes the comparison results of the HA requirements of the safety control systems of other safety industries in Annex C.

For a nuclear power plant, the design safety and operation safety shall be analyzed, for example, to meet the IAEA Safety Requirements for Design (SSR-2/1) and Operation (SSR-2/2). The scope of this document is to survey the state of the art in the hazard analysis for the design of I&C system of NPPs.

Figure 1 illustrates the scope of I&C systems important to safety which have hazard analysis requirements, in the form of a three by three matrix which is in IEEE 603-2009. This document covers the hazard analysis for the sense and command features of digital systems. This document also considers the requirements for hazard analysis of the system of systems(SoS), including the software, hardware and human for the digital systems.

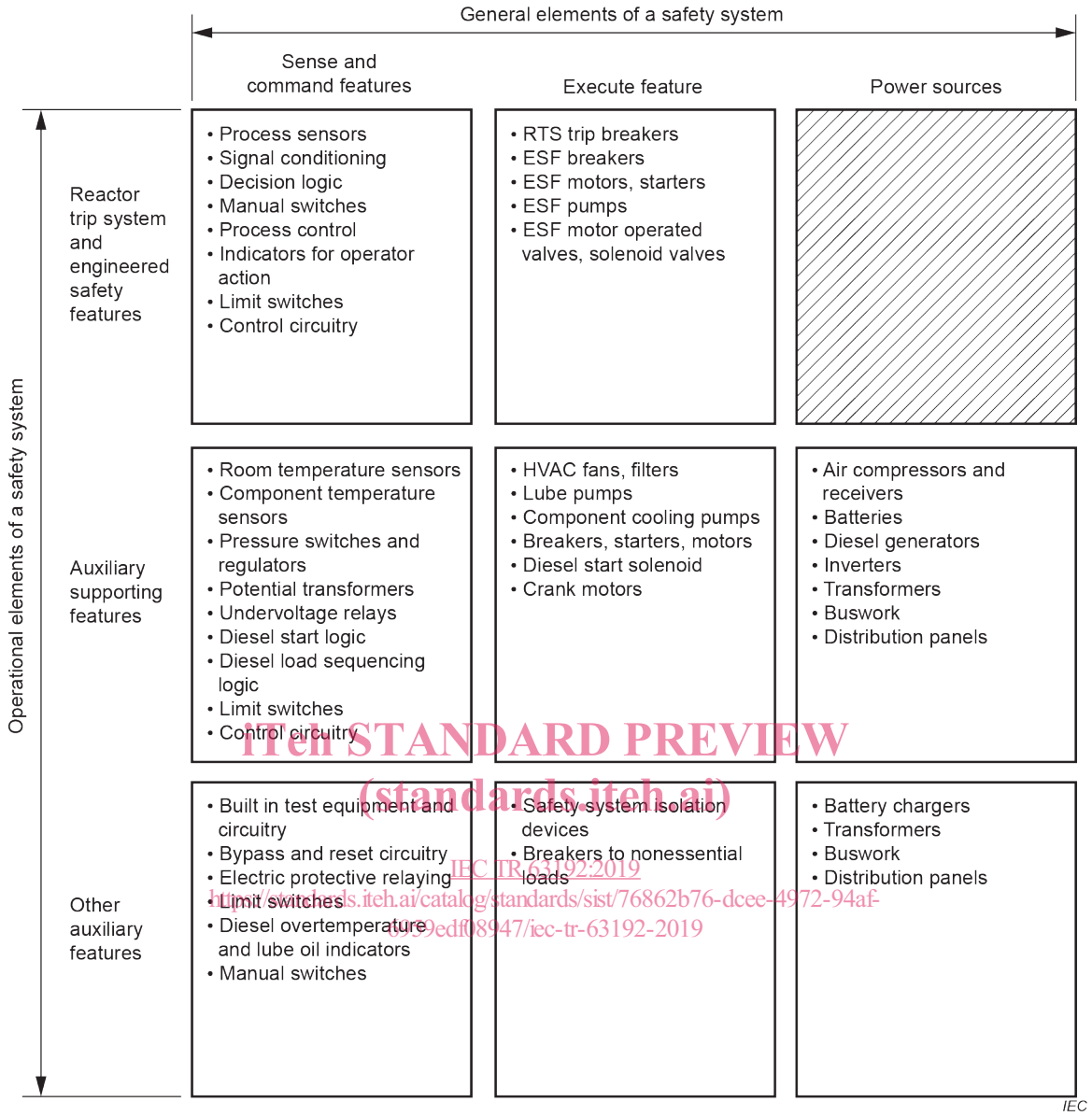

Figure 1 – I&C Layer and Defence-in-Depth Level

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 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 61226:2009, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

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

IEC TR 61508-0, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61513:2011, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

IAEA Safety Standards Specific Safety Requirements SSR-2/1:2012, *Safety of Nuclear Power Plants: Design*

IAEA Safety Standards, Specific Safety Requirements SSR-2/2:2012, *Safety of Nuclear Power Plants: Commissioning and Operation*

IAEA Safety Standards, Safety Guide SSG-39:2016, *Design of Instrumentation and Control Systems for Nuclear Power Plants*

IEEE Standard 7-4.3.2-2010, *IEEE standard criteria for Digital Computers in safety systems for nuclear power generating stations*

IEEE Standard 603-2009, *IEEE standard criteria for safety systems for nuclear power generating stations*

IEEE Standard 1012-2012, *IEEE standard for system and software verification and validation*

IEEE Standard 1228-1994, *IEEE standard for Software Safety Plans*

Research Information Letter (RIL) 1101: *Technical basis to review hazard analysis of digital safety systems, US NRC,* August, 2013

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
safety analysis
evaluation of the potential hazards associated with the conduct of an activity

Note 1 to entry: Safety analysis is often used interchangeably with safety assessment. However, when the distinction is important, safety analysis should be used for the study of safety, and safety assessment for the valuation of safety — for example, evaluation of the magnitude of hazards, evaluation of the performance of safety measures and judgment of their adequacy, or quantification of the overall radiological impact or safety of a facility or activity.

[SOURCE: IAEA Safety Glossary, edition 2007]

3.2
assessment
the process, and the result, of analyzing systematically and evaluating the hazards associated with sources and practices, and associated protection and safety measures. Assessment is often aimed at quantifying performance measures for comparison with criteria.

Note 1 to entry: In IAEA publications, assessment should be distinguished from analysis. Assessment is aimed at providing information that forms the basis of a decision on whether or not something is satisfactory. Various kinds of analysis may be used as tools in doing this. Hence an assessment may include a number of analyses.

[SOURCE: IAEA Safety Glossary, edition 2007]

3.3
safety assessment
a) assessment of all aspects of a practice that are relevant to protection and safety; for an authorized facility, this includes siting, design and operation of the facility. This will normally include risk assessment.

b) analysis to predict the performance of an overall system and its impact, where the performance measure is the radiological impact or some other global measure of the impact on safety

c) the systematic process that is carried out throughout the design process to ensure that all the relevant safety requirements are met by the proposed (or actual) design. Safety assessment includes, but is not limited to, the formal safety analysis

[SOURCE: IAEA Safety Glossary, edition 2007]

3.4
hazard
a) potential source of harm

[SOURCE: ISO/IEC Guide 51:2014, 3.2]

b) intrinsic property or condition that has the potential to cause harm or damage. (B) A source of potential harm or a situation with a potential for harm in terms of human injury, damage to health, property, or the environment, or some combination of these

[SOURCE: IEEE 1012-2012]

3.5
hazard identification
process of recognizing that a hazard exists and defining its characteristics

[SOURCE: IEEE 1012-2012]

3.6
contributory hazard
factor contributing to potential for harm

[SOURCE: AviationGlossary.com, “Contributory Hazard,” <http://aviationglossary.com/aviation-safety-terms/contributory-hazard/>, October 15, 2012]

3.7
hazard analysis
a) process of examining a system throughout its lifecycle to identify inherent hazards and contributory hazards, and requirements and constraints to eliminate, prevent, or control them

[SOURCE: US NRC RIL 1101]

b) systematic qualitative or quantitative evaluation of software for undesirable outcomes resulting from the development or operation of a system

these outcomes may include injury, illness, death, mission failure, economic loss, property loss, environmental loss, or adverse social impact. This evaluation may include screening or analysis methods to categorize, eliminate, reduce, or mitigate hazards

[SOURCE: IEEE 1012-1998]

c) process of examining a system throughout its lifecycle to identify inherent hazards and contributory hazards, and requirements and constraints to eliminate, prevent, or control them

Note 1 to entry: The scope of hazard analysis extends beyond design basis accidents for the plant by including abnormal events and plant operations with degraded equipment and plant systems.

[SOURCE: IAEA SSG-39, 2016]

d) process that explores and identifies conditions that are not identified by the normal design review and testing process

the scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems. Hazard analysis focuses on system failure mechanisms rather than verifying correct system operation

[SOURCE: IEEE Std 7-4.3.2-2003 and 2010]

e) a hazard analysis (HA) is a process for examining an instrumentation and control (I&C) system throughout its development lifecycle to identify hazards (i.e., factors and causes), and system requirements and constraints to eliminate, prevent, or control them. Hazard analyses examine safety related I&C systems, subsystems, and components, their interrelationships and their interactions with other systems, subsystems, and components to identify unintended or unwanted I&C system operation including the impairment or loss of the ability to perform a safety function

[SOURCE: US NRC DSRS App A]

4 Terminologies in IAEA-IEC and NRC-IEEE

There are some differences in the concept, definitions and principles of the safety aspects between IAEA and IEEE communities. Table 1 shows the differences as a summary.

Table 1 – Definitions of IAEA and IEEE nuclear standards

		IAEA	IEEE
1	Framework	IAEA-IEC	NRC-IEEE
2	Risk based qualification	Graded application of quality and reliability features	No graded application
3	Classification	SIL in IEC 61508, Categories in IEC 61226	Class IE, Non1E
4	Safety view	Safety requirements specification is the main activity in the lifecycle.	Safety Analysis in all phases of the lifecycle
5	Software qualification principle	Safety goal and requirements shall be met through good engineering. 1 Simple, separate safety systems design 2 System quality – Complete and correct safety requirements – Correct implementation – Producing quality products 3 Defense-in-depth and diversity	Same approach, but different in direct hazard analysis 1 Simple, separate safety systems design 2 System quality – Complete and correct safety requirements – Correct implementation – Producing quality products 3 Defense-in-depth and diversity 4 Hazard avoidance / identification / resolution
6	Accident	Deviations from normal operation	(IEEE 1228) An unplanned event or series of events that results in death, injury, illness, environmental damage, or damage to or loss of equipment or property
7	Hazard	(IEC 61508-4) Potential source of harm	(IEEE 7-4.3.2) A condition that is a prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software
8	Risk	(IEC 61508-4) Combination of the probability of occurrence of harm and severity of that harm	(IEEE 1228) A measure that combines both the likelihood that a system hazard will cause an accident and the severity of that accident
9	Safety	(IEC 61508-4) Freedom from unacceptable risk	
10	Software hazard		(IEEE 1228) A software condition that is a prerequisite to an accident
11	System hazard		(IEEE 1228) A system condition that is a prerequisite to an accident
12	Software safety		(IEEE 1228) Freedom from software hazards
13	System safety		(IEEE 1228) Freedom from system hazards
14	Hazard analysis	(IEC 61508-0) Hazard Analysis derives Safety Function Requirements	(IEEE 7-4.3.2) Hazard Analysis: A process that explores and identifies conditions that are not identified by the normal design review and testing process. Hazard analysis focuses on system failure mechanisms rather than verifying correct system operation. (NUREG-CR 6430)[50][1] Hazard Analysis is the process of identifying and evaluating the hazards of a system, and then either eliminating the hazard or reducing its risk to an acceptable level.
15	Risk assessment	(IEC 61508-0) Risk assessment derives safety integrity requirements	No definition

[1] Numbers in square brackets refer to the Bibliography.