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 It also gives information on projects, replaced and withdrawn publications.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

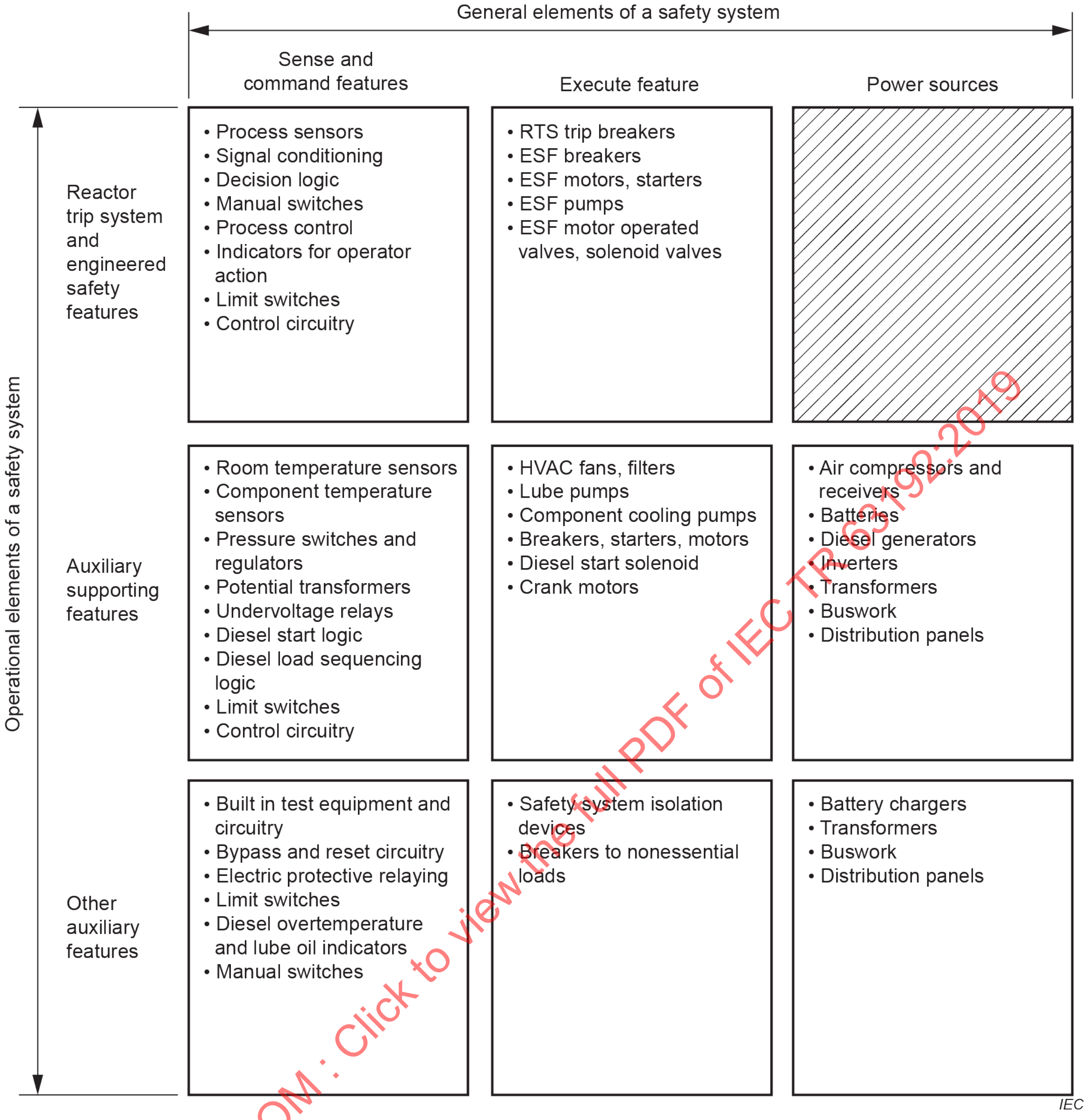
NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – HAZARD ANALYSIS: A REVIEW OF CURRENT APPROACHES

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.



General elements of a safety system

Operational elements of a safety system

	Sense and command features	Execute feature	Power sources
Reactor trip system and engineered safety features	• Process sensors • Signal conditioning • Decision logic • Manual switches • Process control • Indicators for operator action • Limit switches • Control circuitry	• RTS trip breakers • ESF breakers • ESF motors, starters • ESF pumps • ESF motor operated valves, solenoid valves	▨
Auxiliary supporting features	• Room temperature sensors • Component temperature sensors • Pressure switches and regulators • Potential transformers • Undervoltage relays • Diesel start logic • Diesel load sequencing logic • Limit switches • Control circuitry	• HVAC fans, filters • Lube pumps • Component cooling pumps • Breakers, starters, motors • Diesel start solenoid • Crank motors	• Air compressors and receivers • Batteries • Diesel generators • Inverters • Transformers • Buswork • Distribution panels
Other auxiliary features	• Built in test equipment and circuitry • Bypass and reset circuitry • Electric protective relaying • Limit switches • Diesel overtemperature and lube oil indicators • Manual switches	• Safety system isolation devices • Breakers to nonessential loads	• Battery chargers • Transformers • Buswork • Distribution panels

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.

16	Functional safety	(IEC 61508-0) Functional safety: is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.	No definition
17	Functional safety assessment	(IEC 61508-4) Functional safety assessment: investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE (See Table B.1) safety-related systems, other technology safety-related systems or external risk reduction facilities	(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. The scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems.

5 Abbreviated terms and acronyms

ASIC	Application Specific Integrated Circuit
CCF	Common Cause Failure
COTS	Commercial Off-The-Shelf
DSRS	Design Specific Review Standard
ESF	Engineered Safety Features
FPGA	Field Programmable Gate Array
HDL	Hardware Description Language
HA	Hazard Analysis
HVAC	Heating, Ventilation, Air Conditioning
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PLC	Programmable Logic Controller
QA	Quality Assurance
RAMS	Reliability, Availability, Maintainability, and Safety
RTS	Reactor Trip System
SIL	Safety Integrity Level
SoS	System of Systems
SSR	Specific Safety Requirements
V&V	Verification & Validation

6 General

6.1 Hazard analysis of digital instrumentation and control systems

A hazard, in general, is defined as "potential for harm." In this document, the scope of "harm" is limited to the loss of a safety function in a Nuclear Power Plant (NPP). Furthermore, the unintended or spurious action of a safety function can cause harm or in some cases contravene the safety function needed in that particular situation.

In the context of ensuring a safety system of the highest criticality, a hazard (potential for harm, in brief) is the potential to degrade the system's capability to perform its allocated safety function (henceforth, potential to degrade the system). The hazard may be external or internal to the system. (There may be multiple levels of integration of a system, i.e., there may be systems within systems; then the internal-external boundary shifts in accordance with the level of integration in focus.)

The Hazard Analysis (HA) of an Instrumentation and Control (I&C) system is to identify the relationship of the logical faults, error, and failure of I&C systems to the physical harm of the nuclear power plant, and also to find the impact of the external hazard, e.g., tsunami, of the nuclear power plant to the I&C systems.

Hazards analysis, a systems engineering activity, is the application of systematic and replicable methods to identify hazards, their potential adverse effects, their causes, and the changes in system concept or safety requirements needed to meet the overall safety goals of the system.

Although the term "hazard analysis" has been defined in many different ways as shown in 3.7, in this document the comparison scope of HA requirements is related to identify all internal and external hazards of I&C systems boundary shown in Figure 2, leading to the loss or spurious activation of safety functions of the NPP.

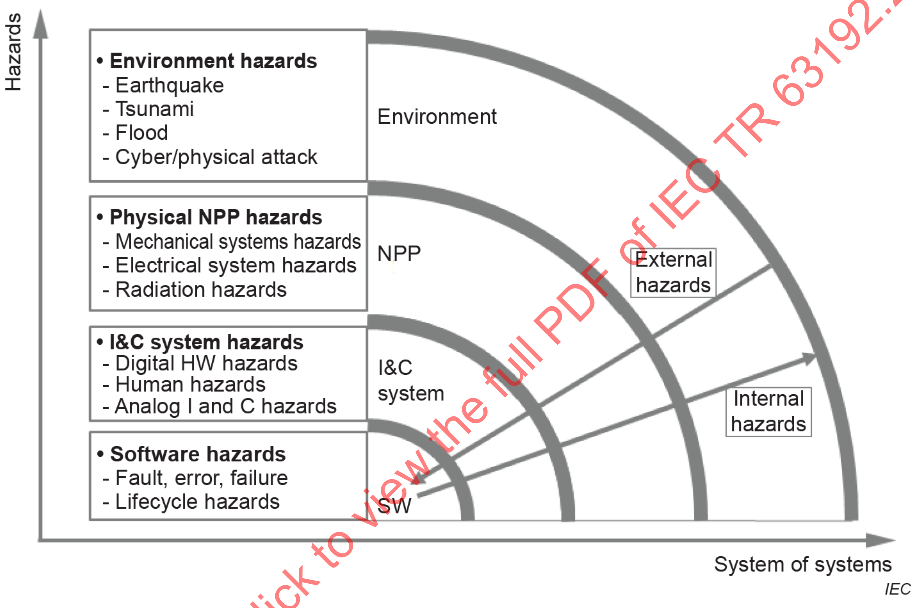


Figure 2 – Internal or external hazards

The hazard analysis is the analysis of internal and external hazards at the boundary of I&C system as shown in Figure 2. Internal hazards include the inherent hazards from software faults introduced throughout the software lifecycle, interaction faults between software and human, and between software and hardware, functional interaction and multiple functional failures such as a common cause failure. External hazards include a loss of power, EMI, RFI, flood, earthquake, and their cascaded events.

6.2 Purpose of hazard analysis

The purpose of HA should be:

a) to identify the hazard and the contributory hazards of I&C system of systems (SoS;.

b) to validate the hazardous aspects of I&C system, software, hardware, and human throughout the lifecycle;

c) to provide solutions for the elimination, control, and mitigation of the hazards.

7 Comparison of hazard analysis requirements and guidance for nuclear industry

7.1 General

There are two major groups of standardization communities in the nuclear industry, the IAEA community and the IEEE community. Each community has developed safety standards and regulatory criteria as shown in Figure 3 and Figure 4. The box in bold in Figures 3 and 4 has some requirements related to the hazard analysis. In this clause, those HA requirements are compared by a template which is defined in Annex C of this document.

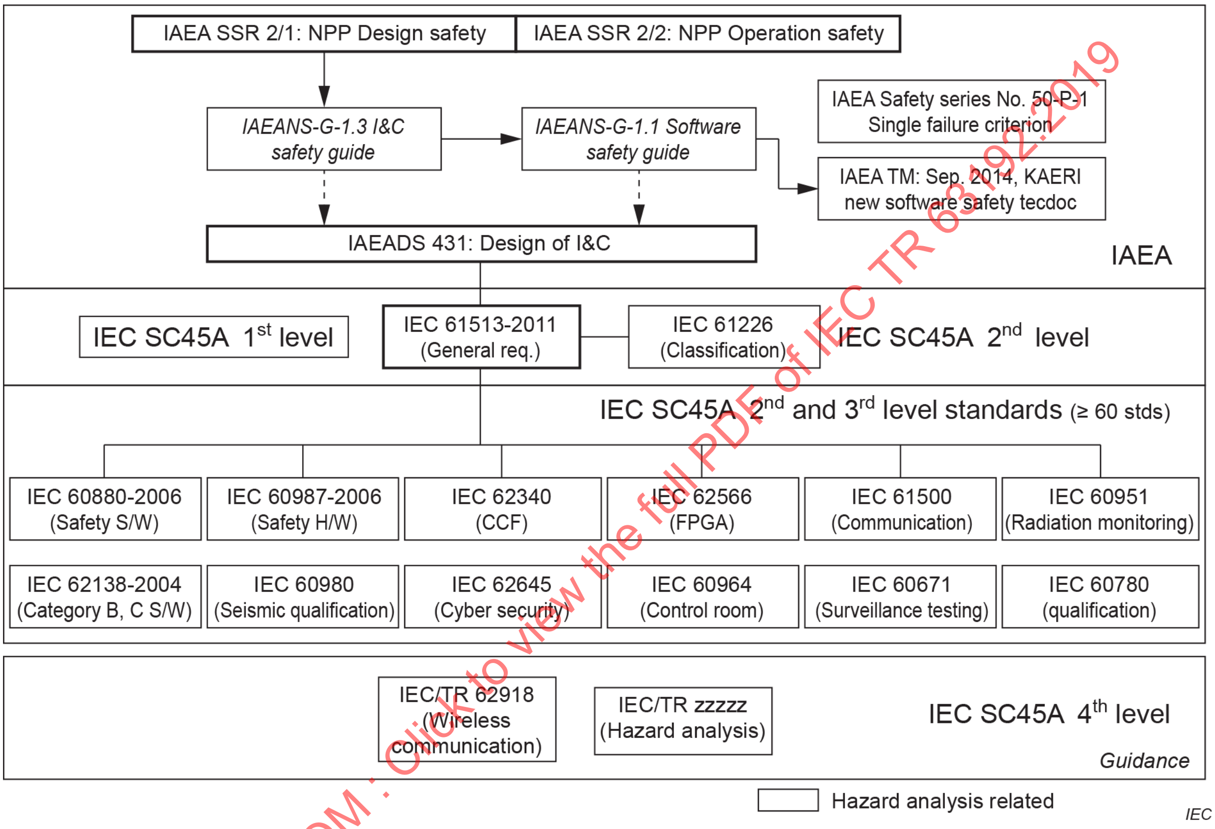

IAEA SSR 2/1: NPP Design safety
IAEA SSR 2/2: NPP Operation safety
IAEANS-G-1.3 I&C safety guide
IAEANS-G-1.1 Software safety guide
IAEA Safety series No. 50-P-1 Single failure criterion
IAEA TM: Sep. 2014, KAERI new software safety tecdoc
IAEADS 431: Design of I&C
IAEA
IEC SC45A 1st level
IEC 61513-2011 (General req.)
IEC 61226 (Classification)
IEC SC45A 2nd level
IEC SC45A 2nd and 3rd level standards (≥ 60 stds)
IEC 60880-2006 (Safety S/W)
IEC 60987-2006 (Safety H/W)
IEC 62340 (CCF)
IEC 62566 (FPGA)
IEC 61500 (Communication)
IEC 60951 (Radiation monitoring)
IEC 62138-2004 (Category B, C S/W)
IEC 60980 (Seismic qualification)
IEC 62645 (Cyber security)
IEC 60964 (Control room)
IEC 60671 (Surveillance testing)
IEC 60780 (qualification)
IEC/TR 62918 (Wireless communication)
IEC/TR zzzzz (Hazard analysis)
IEC SC45A 4th level
Guidance
Hazard analysis related
IEC

Figure 3 – IAEA-IEC framework of I&C standards

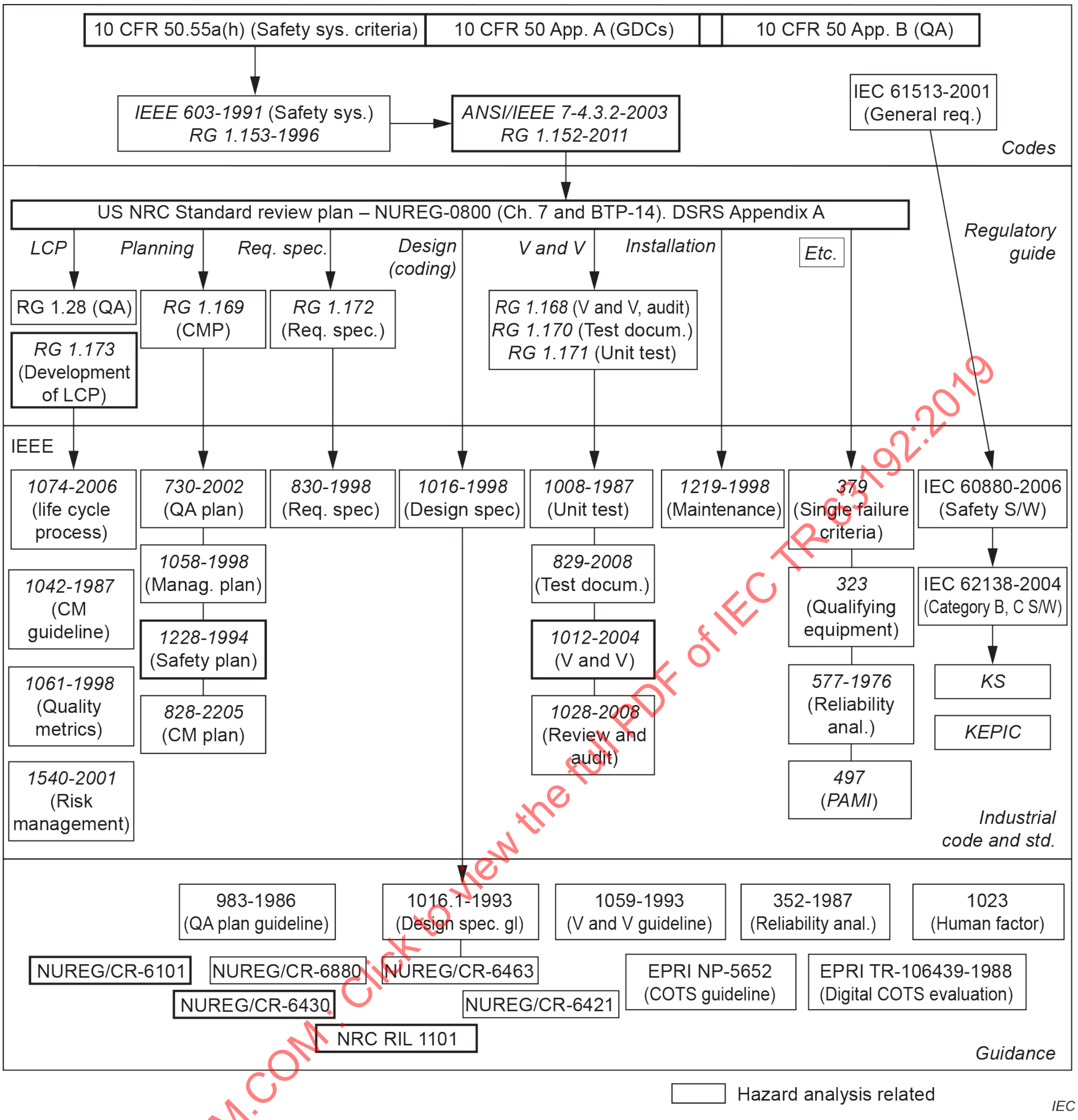


Figure 4 – NRC-IEEE framework of I&C standards

7.2 IAEA Safety Requirements SSR-2/1: Design Safety of NPP:2012

Table 2 presents Hazard Analysis in IAEA Safety Requirements SSR-2/1:2012.

Table 2 – Hazard Analysis in IAEA Safety Requirements SSR-2/1:2012

	Comparison criteria of HA requirements	HA requirements in the safety standard of IAEA SSR-2/1: Design Safety of NPP
1	Safety principles (safety model or safety culture)	Requirement 17: Internal and external hazards. All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.
2	Safety processes	None
3	Definition of HA	Internal hazards 5.16. The design shall take due account of internal hazards such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact and release of fluid from failed systems or from other installations on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised. External hazards 5.17. The design shall include due consideration of those natural and human induced external events (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Natural external events shall be addressed, including meteorological, hydrological, geological and seismic events. Human induced external events arising from nearby industries and transport routes shall be addressed. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and firefighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.
4	Purpose of HA	None
5	Method of HA	None
6	HA process	None
7	Independence of HA (HA organization)	None
8	Harmonized HA of SoS	None
9	Relationship with other requirements (security, reliability)	None
10	Discussion	[Terminology Issue] There are only the top level requirements of the internal and external hazards in IAEA SSR-2/1 without the definitions of the internal and external hazards. There are informal explanations of the internal and external hazards: Internal hazard such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whips, jet impacts, and release of fluid from failed systems or from other installations on the site. natural and human induced external events (i.e., events of origin external to the plant) In IAEA Safety Glossary, there is no definition of internal and external hazards. The internal and external hazards should be decided according to the boundaries of the appropriate systems, such as the plant system, an I&S system, a platform, an operating system, a device, and so on.

7.3 IAEA Safety Requirements SSR-2/2: Operation Safety of NPP:2012

No explicit requirements for operational hazards. There are many implicit requirements of hazards.

7.4 IAEA SSG-39 recommendations for I&C system Hazard Analysis

Table 3 presents HA requirements in IAEA SSG-39:2016.

Table 3 – HA requirements in IAEA SSG-39:2016

	Comparison criteria of HA requirements	HA requirements in the safety standard of IAEA SSG-39
1	Safety principles (safety model or safety culture)	2.56. For the overall I&C architecture, hazard analysis should be performed to identify conditions that might compromise the defense-in-depth strategy of the plant design. 2.57. For safety systems, hazards analyses should be performed to identify conditions that might defeat their safety function.
2	Safety processes	None
3	Definition of HA	None
4	Purpose of HA	None
5	Method of HA	2.58. Hazards to be considered include internal hazards and external hazards, failures of plant equipment, and I&C failures or spurious operation due to hardware failure or to software errors. 2.59. I&C system hazard analysis should consider all plant states and operating modes, including transitions between operating modes.
6	HA process	2.60. The initial results of the I&C system hazard analysis should be available before the design basis for the overall I&C is completed. 2.61. The hazard analysis should be updated during the design of the overall I&C architecture, and during the specification of requirements, design, implementation, installation and modification of safety systems. 2.62. The purpose of updating hazard analysis is to identify hazards that may be caused by specific characteristics of I&C safety systems, by interaction between I&C safety systems and the plant, and by interaction of I&C safety systems with other I&C systems regardless of their safety classification. 2.63. Measures should be taken to eliminate, avoid, or mitigate the consequences of identified hazards that can defeat safety system functions. 2.64. Measures to eliminate, avoid, or mitigate the effects of hazards might, for example, take the form of changes to the I&C requirements, design, or implementation or changes to the plant design. 2.65. The hazard analysis methods should be appropriate for the item being analyzed.
7	Independence of HA (HA organization)	None
8	Harmonized HA of SoS	None
9	Relationship with other requirements (security, reliability)	7.105. The failure modes of computer security features and the effects of these failure modes on I&C functions should be known, documented, and considered in system hazard analysis.
	Discussion	[Terminology Issue] Internal and external hazards should be decided according to the boundaries of I&C systems. However, IAEA SSG-39 uses same meaning applies the same definition of internal and external hazards to the plant as is used in IAEA SSR-2/1.

7.5 IEEE 603 requirements for I&C system Hazard Analysis

IEEE Standard 603-2009:

“There are two groups of requirements for the safety of I&C system of NPP. One group is the safety system design basis (in section 4 of IEEE 603) requirements that will be a basis for the safety analysis (assessment) to assure the safety of I&C design. Section 4, esp. subclause h also implies HA to arrive at the design basis. The other group is the safety system criteria (in section 5 of IEEE 603). The single-failure criterion (5.1) and the common cause failure criteria (5.16) are directly related to the hazard analysis requirements because the purpose of hazard analysis is to identify the relationship between failure and harm.”

Table 4 presents HA requirements in IEEE Standard 603-2009.

Table 4 – HA requirements in IEEE Standard 603-2009

	Comparison criteria of HA requirements	HA requirements in the safety standard of IEEE Standard 603-2009
1	Safety principles (safety model or safety culture)	To protect public health and safety by functioning to mitigate the consequences of design basis events. Top level safety system design basis related to hazard analysis (interpretation of the abstract requirements in IEEE 603-2009 by NRC experts): The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).
2	Safety processes	There is not any prescriptive safety analysis process.
3	Definition of HA	There is no definition of HA, but there are requirements to document the safety system design basis in section 4 of IEEE 603. (The terms hazard and hazard analysis are not used, but if one breaks down these terms into their meanings, one finds that several clauses require identification of hazards and include in the design basis the provisions to prevent degradation of the performance of the safety function. Commented by NRC expert)
4	Purpose of HA	None
5	Method of HA	None
6	HA process	None
7	Independence of HA (HA organization)	None
8	Harmonized HA of SoS	None
9	Relationship with other requirements (security, reliability)	Section 4: i) The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design. The performance of a probabilistic assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion. IEEE Std 352-1987 and IEEE Std 577-2004 provide guidance for reliability analysis. Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in Clause 4 item i) of the design basis, a probabilistic assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.

	Comparison criteria of HA requirements	HA requirements in the safety standard of IEEE Standard 603-2009
		(Probabilistic assessment was not intended for application to systemic pervasive causes, such as engineering deficiencies and organizational and cultural deficiencies. Their effects have been lumped into the "unknown-unknowns" space, which is addressed through diversity and defense in depth. Even for unknowns about physical conditions, the concept of "safety margins" is used.)
10	Discussion	There are no explicit definition and requirements of hazard analysis. However, the top level safety system design basis related to hazard analysis is: h) The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems). This was an interpretation of the abstract requirements in IEEE 603-2009 by NRC experts. Functional and design requirements exist to accomplish the safety function in IEEE 603-2009. In order to meet the single-failure criteria and common cause failure criteria in section 5 of IEEE 603-2009, there shall be some analysis such as a failure or hazard analysis. The failures to meet the safety system criteria in section 5 could cause harm by not accomplishing the safety function.

7.6 IEEE7-4.3.2-2010 requirements for computer based I&C system Hazard Analysis

Table 5 presents HA requirements in IEEE7-4.3.2-2010.

Table 5 – HA requirements in IEEE7-4.3.2-2010

	Comparison criteria of HA requirements	HA requirements in the safety standard of IEEE7-4.3.2-2010
1	Safety principles (safety model, safety culture)	HA to meet "5.5.1 Design for computer integrity" requirement The computer shall be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function.
2	Safety processes	All initial plant level hazards and safety goal of NPP are already identified.
3	Definition of HA	3.1.18 hazard: A condition that is a prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software. (*different definition from IEC 61513 of internal hazard) 3.1.19 hazard analysis: A 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. (*different scope from IEC hazard) 3.1.22 safe state: A state in which potential hazards and operational risks are minimized.
4	Purpose of HA	Annex D The purpose of a hazard analysis is to explore and identify conditions that are not identified by the normal design review and testing process.
5	Method of HA	None
6	HA process	Annex D. Identification and Resolution of Hazards in each phase of the system lifecycle
7	Independence of HA (HA organization)	None

	Comparison criteria of HA requirements	**HA requirements in the safety standard of IEEE7-4.3.2-2010**
8	Harmonized HA of SoS	None
9	Relationship with other requirements (security, reliability)	5.17.1.6 Evaluate computer security COTS items to be used in safety systems shall provide computer security features as required by 5.9 of this standard. The dedicating entity shall perform an evaluation of the computer security risks and hazards associated with this system, including impacts on hardware, software, interfaces to other systems, and life cycle documentation, as well as plant procedures for the COTS items and the interfacing systems.
10	Discussion	There no HA requirements in the main content of 7-4.3.2 There is some explanation of hazards by using the internal and external conditions in Annex D.2 5.5.1 Design for computer integrity The computer shall be designed to conduct its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. There are some requirements of HA for COTS. In addition, a detailed HA is provided in Annex D. 5.17.1.1 Document the system safety function risks and hazards 5.17.1.3 Identify the safety function(s) the COTS item shall perform Annex D D.4.5 Evaluation of hazards in previously developed systems D.4.7 Preliminary hazard analysis questions D.4.2.2 Planning One may encounter resistance to hazard analyses at the beginning of the system development stemming from the desire to keep development costs as low as possible. Real and identifiable hazards do not exist at the start of the design process, thus justifying or assigning resources to the hazard analysis process can be difficult to quantify or justify. However, as discussed in D.4.2.1 above, there are significant advantages to incorporating a hazard identification into the normal design process early on.

7.7 IEEE 1228-1994 requirements for I&C software Hazard Analysis

Table 6 presents HA requirements in IEEE 1228-1994.

Table 6 – HA requirements in IEEE 1228-1994

	Comparison criteria of HA requirements	HA requirements in IEEE 1228-1994
1	Safety principles (safety model or safety culture)	Not defined
2	Safety processes	4. Software safety analyses 4.1 Software safety analyses preparation 4.2 Software safety requirements analysis 4.3 Software safety design analysis 4.4 Software safety code analysis 4.5 Software safety test analysis 4.6 Software safety change analysis
3	Definition of HA	Accident: An unplanned event or series of events that results in death, injury, illness, environmental damage, or damage to or loss of equipment or property Risk: A measure that combines both the likelihood that a system hazard will cause an accident and the severity of that accident Software hazard: A software condition that is a prerequisite to an accident System hazard: A system condition that is a prerequisite to an accident Software safety: Freedom from software hazards System safety: Freedom from system hazards
4	Purpose of HA	This standard establishes the minimum acceptable requirements for the content of a Software Safety Plan (also referred to as the Plan) to address the processes and activities intended to improve the safety of safety critical software.
5	Method of HA	Not defined
6	HA process	Defined as a software safety analyses
7	Independence of HA (HA organization)	The accomplishment of software safety program activities may be performed by dedicated safety personnel, or may be integrated with and performed by personnel performing other activities in the normal course of development.
8	Harmonized HA of SoS	This standard does not contain special provisions required for software used in distributed systems or in parallel processors.
9	Relationship with other requirements (security, reliability)	There are no requirements for the harmonization with security and reliability analysis.
10	Discussion	IEEE 1228-1994 was not revised in the IEEE community and also was not endorsed by US NRC as a regulatory guide.

7.8 IEEE 1012-2012 requirements for system Hazard Analysis

There are requirements for hazard analysis for the system, hardware, and software of SIL level 3 and 4 throughout lifecycle in IEEE 1012-2012.

Table 7 presents HA requirements in IEEE 1012-2012.

Table 7 – HA requirements in IEEE 1012-2012

	Comparison criteria of HA requirements	**HA requirements in IEEE 1012-2012**
1	Safety principles (safety model or safety culture)	Described as a combination of hazard, security, and risk analysis
2	Safety processes	Not defined
3	Definition of HA	hazard: (A) An 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. hazard identification: The process of recognizing that a hazard exists and defining its characteristics.
4	Purpose of HA	The objective for the V&V of hazards is to perform a sufficient set of V&V tasks for all contributors such that the likelihood of reaching a hazardous condition is known to a desired level of confidence.
5	Method of HA	Fault Tree Analysis
6	HA process	a) Traceability of critical requirements through the lifecycle to verify implementation. b) Evaluation of potential hazard contributors to validate that critical requirements are complete and are appropriate for the system operational need. c) Evaluation of architectures and designs to determine whether hazard mitigation functions meet required capabilities and whether additional mitigation strategies are needed.
7	Independence of HA (HA organization)	The hazard analysis may be performed by any organization within the project such as systems engineering, reliability, safety, or V&V.
8	Harmonized HA of SoS	Not defined
9	Relationship with other requirements (security, reliability)	Annex J (informative) Hazard, security, and risk analyses
10	Discussion	There are requirements for a hazard analysis for the system, hardware, and software of SIL level 3 and 4 throughout the lifecycle in IEEE 1012-2012. IEEE 1012-2012 was not developed as a nuclear standard at IEEE NPEC and it was not endorsed as a regulatory guide by US NRC.

7.9 HA Guidance of US NRC

In this subclause, two guidances of US NRC, the Design-Specific Review Standard (DSRS) and the Research Information letter (RIL) 1101, are surveyed by the comparison tables in Table B.1 and Table B.2.

Table 8 presents DSRS APPENDIX A. Hazard Analysis.

Table 8 – DSRS APPENDIX A. Hazard Analysis

	Comparison criteria of HA requirements	HA requirements in the safety standard of US NRC DSRS Appendix A, Hazard Analysis
1	Safety principles (safety model or safety culture)	None
2	Safety processes	None
3	Definition of HA	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.
4	Purpose of HA	to evaluate HAs
5	Method of HA	B. HA Information to be reviewed. 7. Internal hazards that could be generated by the I&C system. For example, excessive load or demand on resources by the I&C system, such as electric power overload due to a short circuit or communication bus overload. 8. External hazards such as disruption in I&C system conditions and physical conditions in the environment that may impair a safety function, e.g.: 8.1. Water intrusion. 8.2. Uncontrolled transfer of energy into the system. Such energy may take various forms, e.g.: heat; light; vibration; radiation; electromagnetic radiation. C. HA Information to be considered for Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) I&C systems development process contributory hazards Software-related contributory hazards
6	HA process	HA is iterative and should be performed at every phase in the system development lifecycle to identify new hazards that could arise as the design is implemented in software and hardware.
7	Independence of HA (HA organization)	Not defined
8	Harmonized HA of SoS	Not defined
9	Relationship with other requirements (security, reliability)	(Commented by NRC expert) HA should analyze any condition on which the SAFETY property depends. For example: If it depends upon security, then identify constraints to prevent the intrusion. If the safety of the system depends upon the correct continued functioning of a hardware component, then perform HA on that component. If the component is self-diagnostic and has prognostics to identify and notify impending failure, and the system has a function to reach a safe state before the failure occurs, then the SAFETY property is preserved. If the system has redundancy to protect against random hardware failure, then the SAFETY property is preserved. There is no justification to demand additional analysis for aspects of security on which the SAFETY property does not depend. There is no justification to demand additional analysis for aspects of reliability on which the SAFETY property does not depend. Key point: Focus on identifying dependencies: {contributor to hazard; its contribution path(s)}.
10	Discussion	DSRS is developed for the staff review process for US NRC, specifically for the mPOWER iPWR Design. The hazard analysis principles, definitions, and requirements are clear and simple. However, these regulatory positions of US NRC are under discussion for a general I&C design in US and also OECD MDEP.

Table 9 present the Research Information Letter of HA review (US NRC RIL 1101:2013).

Table 9 – Research Information Letter of HA review (US NRC RIL 1101:2013)

	Comparison criteria of HA requirements	HA requirements in the safety standard of US NRC RIL 1101:2013
1	Safety principles(safety model, safety culture)	The primary object of hazard analysis is the product. Dependency analysis leads to process factors.
2	Safety processes	None
3	Definition of HA	Hazard Potential for harm Contributory hazard Factor contributing to potential for harm. Aviation Glossary.com, “Contributory Hazard,” <http://aviationglossary.com/aviation-safety-terms/contributory-hazard/>, October 15, 2012. Hazard analysis (HA) is the 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. “Hazard identification” part of HA includes the identification of losses (harm) of concern.
4	Purpose of HA	Hazard analysis (HA) is the 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.
5	Method of HA	Appendix C.
6	HA process	Appendix C.
7	Independence of HA (HA organization)	Appendix C.
8	Harmonized HA of SoS	Appendix C.
9	Relationship with other requirements (security, reliability)	See Appendix C RIL 1101. HA should analyze any condition on which the SAFETY property depends. For example: If it depends upon security, then identify constraints to prevent the intrusion. If the safety of the system depends upon the correct continued functioning of a hardware component, then perform HA on that component. If the component is self-diagnostic and has prognostics to identify and notify impending failure, and the system has a function to reach a safe state before the failure occurs, then the SAFETY property is preserved. If the system has redundancy to protect against random hardware failure, then the SAFETY property is preserved. There is no justification to demand additional analysis for aspects of security on which the SAFETY property does not depend. There is no justification to demand additional analysis for aspects of reliability on which the SAFETY property does not depend. Key point: Focus on identifying dependencies: {contributor to hazard; its contribution path(s)}.

	Comparison criteria of HA requirements	HA requirements in the safety standard of US NRC RIL 1101:2013
10	Discussion	If the concept of a contributory hazard is borrowed from the FAA system safety handbook, its concept in RIL1101 seems to be excessively expanded to a systemic cause of the development process. The concept of a contributory hazard is also found in the research by Professor Tim Kelly at the University of York, UK. RIL-1101 states that it does not focus on well-known or well-understood causes (e.g., random hardware failure). Systemic causes are not well understood and their effects are pervasive. The proportion of their contribution (relative to the well understood causes) is increasing rapidly in a wide range of critical digital systems. (This increase is obscured under the label “complexity.”) However, the engineering capability does not improve as rapidly, i.e., the gap is expanding. “Deviations are malfunctions, degradation, errors, failures, faults, and system anomalies. They are unsafe conditions and/or acts with the potential for harm. These are termed *contributory hazards* in this FAA System Safety Handbook.” A “deviation” does not have the same meaning elsewhere. Not all deviations (e.g., faults; errors; etc.) are contributory hazards. The rapidly growing (yet not well recognized) contributor: Incomplete, incorrect, inconsistent, ambiguous requirements, and constraints, leading to deficient architectures (the next biggest contributor) (commented by US NRC expert).

8 MDEP common position on hazard identification and controls for digital I&C systems

8.1 General

Faults within I&C systems may lead to failures that may be potential hazards which can affect plant safety, block or prevent the actuation of a safety system protective function or cause an operating condition for which the safety systems protective functions cannot mitigate. Examples of the cause of such faults include incorrect requirements and interface specifications, software errors, and errors as a result of maintenance and periodic testing. Such faults can lead to undesirable behaviour of I&C systems, which could create hazards that challenge plant safety. In comparison to hazards associated with localized failures (e.g. conventional hardware component failures), hazards associated with digital I&C systems can be more difficult to identify and control. These difficulties arise from system complexity and the pervasive and latent impact of faults due to interconnectivity or functional relationships of systems. Therefore, a systematic approach to identify and control such hazards is necessary.

8.2 Hazard identification [59]

a) For each I&C system, hazards that could challenge plant safety should be identified.

b) Hazard identification should complement the plant safety analysis (e.g. consider hazards not analyzed).

c) Hazard identification should be performed for all stages of the system life span (including development, commissioning, modifications, operation, maintenance and decommissioning).

   1) Hazard identification should assess for hazards during the entire system life cycle development process from the planning through the testing phases.

   2) Hazard identification should also consider hazards induced by activities such as commissioning, maintenance and testing, equipment ageing, operational procedures, etc.

   3) Hazard identification should be revisited at appropriate times (e.g. digital upgrades, changing or emerging information regarding internal or external hazards to I&C systems, etc.).

d) Hazard identification should consider hazards that arise from interactions between I&C systems and other plant systems. Other hazards may arise during the I&C system lifecycle due to organizational interactions between different technology areas.

e) Regardless of the technique used to perform hazard identification (e.g. hazard and operability analysis (HAZOPs), functional failure modes and effects analyses (FFMEAs), systemic theoretic process analysis (STPA), top-down fault tree analysis (FTA), or purpose graph analysis (PGA)), the limits of the technique should be understood. Documentation should be provided to justify the techniques used.

f) All identified hazards, including the causes and consequences for the identified hazards, should be properly documented.

8.3 Hazard control [59]

a) Hazard controls should be implemented for the identified hazards from Section A of this common position. Hazard controls can include, but are not limited to:

   1) Preventing the hazard by removing the cause of the hazard (e.g. design the system such that the hazard cannot arise)

   2) Inherent design features within the I&C system (e.g. independence, automated self-testing, diversity, etc.)

   3) Analyses that demonstrate plant safety is ensured in the presence of the hazard

   Hazard controls using measures such as external I&C systems, mechanical controls, operational procedures, etc., should be considered. Engineered features, however, are preferable.

b) Hazard controls should be as simple as possible to facilitate activities such as inspections, configuration management, fulfilling procedural requirements, etc.

c) The hazard control process should be performed for all stages of the system life span. Unidentified hazards should be reduced as the life span progresses.

d) Hazard controls should consider the potential consequences of each hazard that could challenge plant safety.

e) The evaluation or testing of hazard controls should verify the effectiveness of each hazard control.

f) Hazard controls should not prevent the system from meeting its functional and performance requirements.

g) Hazard controls should be adequately documented. Hazard control documentation should clearly and concisely describe criteria to trigger re-evaluation when changes occur to internal and external hazards that may impact the I&C system.

h) Hazard controls should be periodically reviewed and re-evaluated when necessary. A review may be triggered by changes to I&C system design requirements and constraints, emerging information, mandatory periodic review, etc.

9 Further works for hazard analysis of I&C for NPPs

9.1 The harmonized HA for I&C system of systems(SoS), software, hardware, and human

The hazard analysis process for I&C systems should be integrated with the I&C system development process. A hazard analysis should support and drive the activities related to the system development by evaluating the functions and the design of the I&C system, as well as its parts (i.e. subsystems, elements including software and hardware) to identify the hazardous/failure conditions, and the requirements to address those conditions, as shown in Figure 5.

a) Harmonization of techniques: Figure 5 shows the scope of hazard analysis for I&C SoS, the relationship with other qualifying aspects such as the security analysis and reliability analysis, and then the relationship between the qualification activities and the safety maturity to decide the acceptability of the safety. (Figure 5 a)

b) Harmonized lifecycles between a qualification and a development: There should be a clear description of the activities related to a hazard analysis, the input information for each activity, and the deliverable output. The communication, i.e., information flow, between the activities of a hazard analysis and system development should be clearly defined. It should be planned (probably described through a safety or qualification plan) how hazard analysis activities along with the system development activities provide evidence to the demonstration of system safety. (Figure 5 b)

c) Dependability analysis through a lifecycle: Owing to the iterative nature of the development process, the changes made to the functions and the design of the system can introduce new hazardous conditions. Therefore, at each phase of the development lifecycle, the respective product or the result of the phase should be analyzed to identify new hazardous conditions, and propose new or derived requirements to address these conditions. Such a hazard analysis conducted throughout the system development lifecycle is required to ensure that the system as a whole achieves the overall safety objectives. Moreover, a hazard analysis is fundamental to the demonstration of safety of the system, by providing the required evidence on the achievement of the overall system safety. (Figure 5 c)

d) Integrated dependability analyses for a system of systems: For an integrated system constituting several parts as well as several interfaces to the environment (i.e. other systems including humans), an integrated hazard analysis process is important to identify hazardous conditions, establish appropriate requirements, identify integrity levels, apportion requirements, and integrity levels to the parts of the system, and identify lower-level conditions related to the parts of the systems causing the system-level conditions. (Figure 5 d)

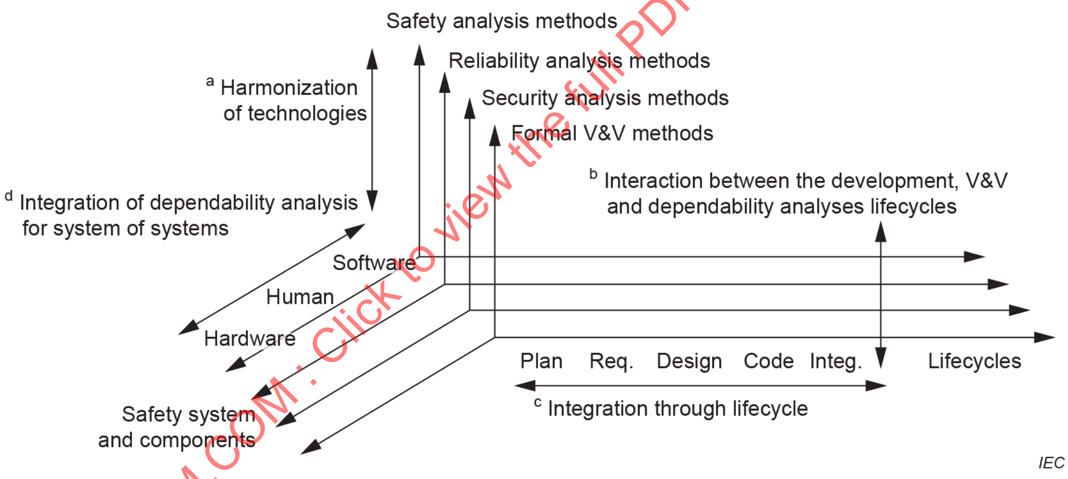

Safety analysis methods
Reliability analysis methods
Security analysis methods
Formal V&V methods
a Harmonization of technologies
b Interaction between the development, V&V and dependability analyses lifecycles
d Integration of dependability analysis for system of systems
Software
Human
Hardware
Safety system and components
Plan
Req.
Design
Code
Integ.
Lifecycles
c Integration through lifecycle
IEC

Figure 5 – Harmonization of HA requirements for I&C system of systems

9.2 The harmonized HA with the security, and reliability of I&C systems

The security requirements are similar to the safety requirements, as they state what or how to avoid unwanted behavior or aspects of a system. Whereas safety is concerned with avoiding hazards leading to accidental harm, security is about considering responses to threats in order to avoid intentional harm. Accidental and intentional harm can be both damage and injury to humans, property, or the environment, in which case the safety and security will be closely related. Contradictions between security requirements and safety requirements shall be resolved.

A hazard analysis process for an I&C system resembles the threat analysis process that has to be undertaken for the same system. In both cases, the system has to be examined through the complete lifecycle in order to identify potential harm (hazards and threats) and its causes (both inherent and contributory), in order to identify the requirements and constrains to eliminate, prevent, or control the potential harm. These requirements and constraints can either be related to each other, e.g., in conflict, reinforcing or dependent on each other, or unrelated. If related, it is important to analyze them and resolve conflicts or take advantage of a reinforcement.

As the processes of a hazard analysis and threat analysis can be closely related, as shown in Figure 6, it is of importance to align them. Both processes should be integrated with the I&C system development process, and they are then likely to have overlapping activities during the various phases of the development lifecycle. The overlap can be related to stakeholders involved in an analysis, the product that is subject to the analysis, the techniques and tools used, or the resulting outcome of a phase. Some of the activities from a hazard and threat analysis might be conducted sequentially or even combined.

The reliability requirements describe a system’s ability to function correctly under certain conditions for a certain time. This is related to hazard analysis requirements, because certain functions of a system are critical to safety and can lead to hazardous events if not functioning correctly under the given conditions in the given time period.

In order to demonstrate the overall safety of a digital I&C system, there shall be clear definitions of the role of the overall safety assessment, a risk assessment, a safety analysis, a security analysis, a failure analysis, the hazard analysis, the threat analysis, and the vulnerability analysis, and how they are related to each other as shown in Figure 6.

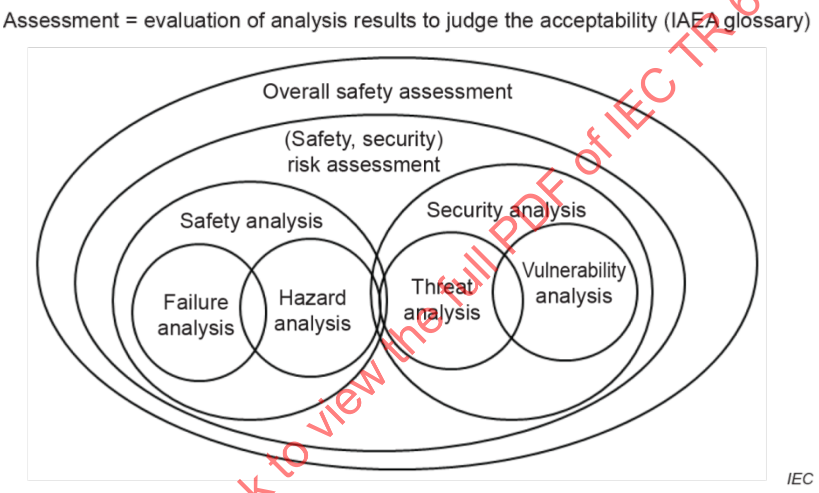

Assessment = evaluation of analysis results to judge the acceptability (IAEA glossary)
Overall safety assessment
(Safety, security) risk assessment
Safety analysis
Security analysis
Failure analysis
Hazard analysis
Threat analysis
Vulnerability analysis
IEC

Figure 6 – Overall safety assessment

10 Conclusion

This document surveyed the status on the hazard analysis requirements for the instrumentation and control (I&C) systems important to safety in the nuclear industry in Clause 7. The hazard analysis requirements in other safety industries are summarized in Annex B.

In Clause 7, the hazard analysis requirements in IAEA, IEEE standards for the nuclear industry, and the HA recommendation in US NRC guidance have been compared by the nine criteria in Annex C, the safety principle, safety process, definitions, purposes, methods, HA process, independence of HA, HA of system of systems, harmonized requirements among safety, security, and reliability.

In Clause 8, the part of MDEP common position on hazard identification and controls for digital I&C systems has been included as a reference to develop the requirements of HA of digital I&C systems for a nuclear power plant. Clause 9 describes further work for preparing the requirements proposals in a new standard of hazard analysis of I&C systems.

Annex A
(informative)

Survey of practical techniques for Hazard Analysis

A.1 General

A number of hazard analysis techniques have been proposed, performed and extended for decades as target systems have evolved from sequential processing plants to complex electro-mechanical systems. Traditional techniques such as FTA (Fault Tree Analysis), HAZOP (HAZard and OPerability) and FMEA (Failure Mode and Effect Analysis) still work well, but new ones such as Safety Case and STPA (System Theoretic Process and Analysis) are gaining recognitions from various safety-critical domains (e.g., nuclear power plants, avionics, railroads, etc.). This annex summarizes a few widely-used hazard analysis techniques. New techniques as well as old ones are also explained and compared according to the criteria such as 'time of use' and 'application domain.' It does not include all hazard analysis techniques but the ones which can be used appropriately for nuclear I&C design and implementation.

A.2 Practical techniques for Hazard Analysis

PHA (Preliminary Hazard Analysis)

- It provides a method for identifying and analyzing hazards in a system and establishing initial system safety requirements from preliminary system design information. [4], [5], [6]
- It tries to affect the system design for safety as early as possible in the system development life-cycle.
- It identifies hazards, their associated causal factors, effect, level of risk and mitigating design measures.

HAZOP (HAZard and Operability)

- It is a structured technique for identifying and analyzing hazards and operational concerns of a system from conceptual design through decommissioning.
- It utilizes key guide words (e.g., more, no, less) to identify potential deviations in designed operations.[HAZOP]

FMEA (Failure Mode and Effect Analysis)[FMEA]

- It is a reliability analysis tool for evaluating the effects of potential failure modes of each part of a system.
- It includes failure rates for each failure mode to achieve a quantitative probabilistic analysis.
- It is more effective when performed as early as possible in Software Development Life Cycle (SDLC) in conjunction with HAZOP.

FTA (Fault Tree Analysis)[FTA]

- It is a top-down tree-construction method for searching combinations of causes of a root failure or accident. [1]
- It can be used in all SDLC phases, but would be effective when detailed design is established.
- It can be performed against software design and implementation.

Safety Case (Dependability Case)[SC]

- It requires developers to provide direct evidence and logical argument, which can claim that safety goals and requirements are well satisfied in a context. [7], [8]
- Analysis results from other hazard analysis techniques can be used as evidence.

STPA (System-Theoretic Process and Analysis) [STPA]

- It is based on a new accident model STAMP (System-Theoretic Accident Model and Process) to identify causal factors. [2]
- It can analyze the entire accident process, including social and human factors.

A.3 Use of the techniques for performing the HA for I&C systems

Every hazard analysis technique has its own ‘time of use’ and an appropriate ‘application domain.’ In case of I&C systems, the techniques in Clause A.2 have been used to perform hazard analysis. Many other techniques can be referred in a book titled Hazard Analysis Techniques for System Safety [3]. Safety experts should select a set of hazard analysis techniques above and organize them in a systematic manner, thoroughly considering two important factors. The first one is that the chosen techniques should be interconnected in the process of I&C system development lifecycle. The output-to-input relationship is similar with cause-to-consequence in analysis techniques. For example, the result of PHA can be used as an input to HAZOP, FTA, and so on.

The other factor is that the cause-to-consequence relationship should be traceable forward as well as backward [9]. A result (i.e., cause) from a higher level of analysis technique should be analyzed in more details by subsequent techniques of the lower level, which result in more concrete causes. For each failure or accident, a set of concrete causes will be analyzed by a sequence of analysis techniques.

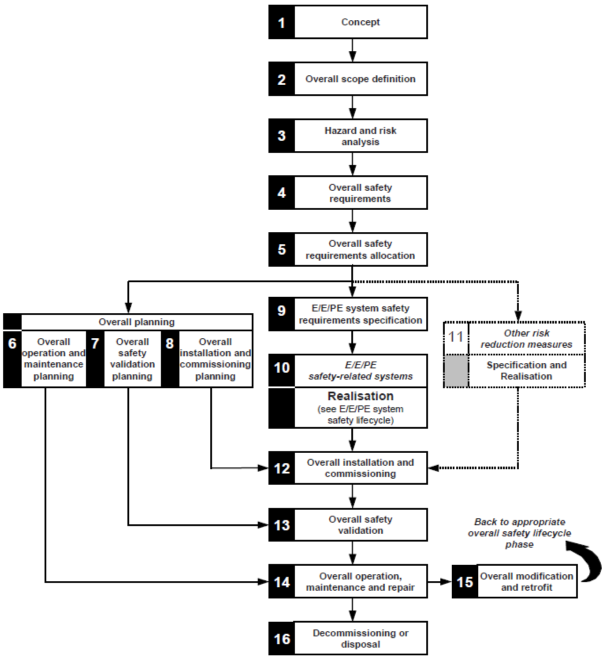
Annex B
(informative)

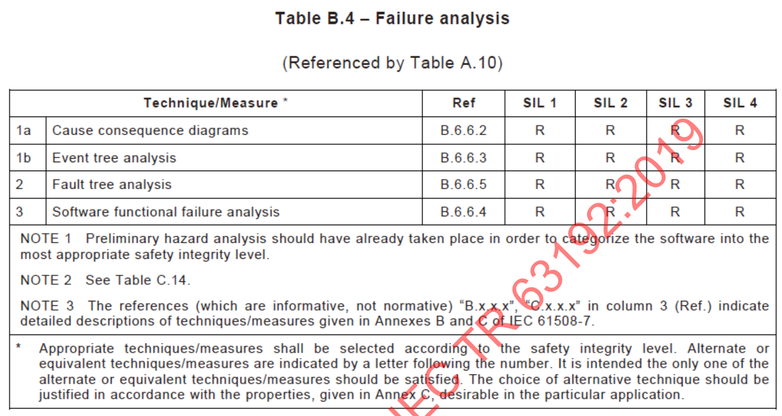
Comparison of Hazard Analysis guidance and requirements of safety industries

B.1 [Safety industry general] IEC 61508 requirements for system hazard analysis

Table B.1 presents HA requirements in the functional safety standard IEC 61508.

Table B.1 – HA requirements in the functional safety standard IEC 61508

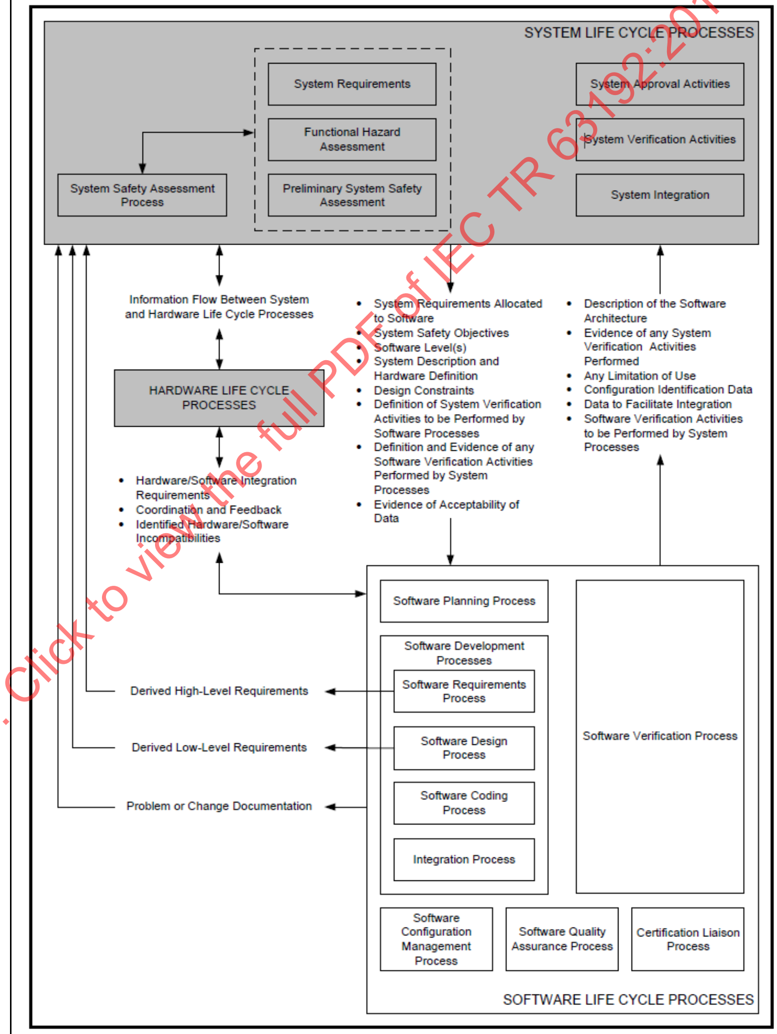
	Comparison criteria of HA requirements	HA requirements in the safety standard IEC 61508
1	Safety principles (safety model or safety culture)	This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic (E/E/PE) systems are used to carry out safety functions. A major objective of this standard is to facilitate the development of product and application sector international standards by the technical committees responsible for the product or application sector. This will allow all the relevant factors, associated with the product or application, to be fully taken into account and thereby meet the specific needs of users of the product and the application sector. A second objective of this standard is to enable the development of E/E/PE safety-related systems where product or application sector international standards do not exist. It is mainly concerned with the E/E/PE safety-related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognized that the consequences of failure could also have serious economic implications and in such cases this standard could be used to specify any E/E/PE system used for the protection of equipment or product;
2	Safety processes	considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, though design, implementation, operation and maintenance to decommissioning) when E/E/PE systems are used to perform safety functions;  1 Concept 2 Overall scope definition 3 Hazard and risk analysis 4 Overall safety requirements 5 Overall safety requirements allocation Overall planning 6 Overall operation and maintenance planning 7 Overall safety validation planning 8 Overall installation and commissioning planning 9 E/E/PE system safety requirements specification 10 E/E/PE safety-related systems Realisation (see E/E/PE system safety lifecycle) 11 Other risk reduction measures Specification and Realisation 12 Overall installation and commissioning 13 Overall safety validation Back to appropriate overall safety lifecycle phase 14 Overall operation, maintenance and repair 15 Overall modification and retrofit 16 Decommissioning or disposal
3	Definition of HA	Non

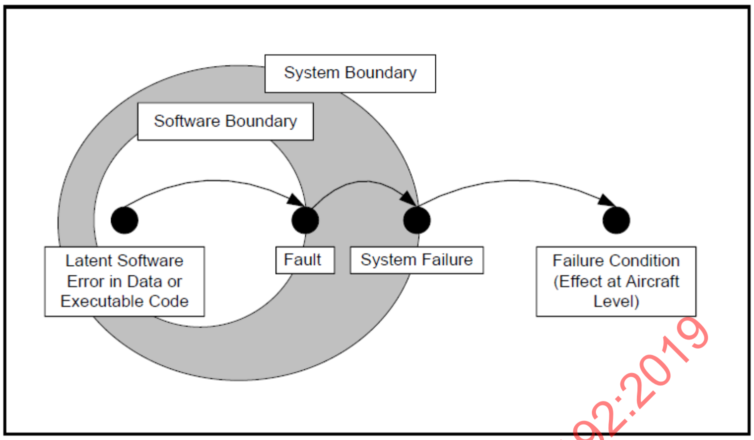
<table>
<tr><td>4</td><td>Purpose of HA</td><td>7.4.1:
To determine the hazards, hazardous events and hazardous situations relating to the Equipment Under Control (EUC) and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances, including fault conditions and reasonably foreseeable misuse (see 3.1.14 of IEC 61508-4);
To determine the event sequences leading to the hazardous events;
To determine the EUC risks associated with the hazardous events.</td></tr>
<tr><td>5</td><td>Method of HA</td><td>
<b>Table B.4 – Failure analysis</b>
(Referenced by Table A.10)
<table>
<tr><th colspan="2">Technique/Measure *</th><th>Ref</th><th>SIL 1</th><th>SIL 2</th><th>SIL 3</th><th>SIL 4</th></tr>
<tr><td>1a</td><td>Cause consequence diagrams</td><td>B.6.6.2</td><td>R</td><td>R</td><td>R</td><td>R</td></tr>
<tr><td>1b</td><td>Event tree analysis</td><td>B.6.6.3</td><td>R</td><td>R</td><td>R</td><td>R</td></tr>
<tr><td>2</td><td>Fault tree analysis</td><td>B.6.6.5</td><td>R</td><td>R</td><td>R</td><td>R</td></tr>
<tr><td>3</td><td>Software functional failure analysis</td><td>B.6.6.4</td><td>R</td><td>R</td><td>R</td><td>R</td></tr>
<tr><td colspan="7">NOTE 1 Preliminary hazard analysis should have already taken place in order to categorize the software into the most appropriate safety integrity level.
NOTE 2 See Table C.14.
NOTE 3 The references (which are informative, not normative) “B.x.x.x”, “C.x.x.x” in column 3 (Ref.) indicate detailed descriptions of techniques/measures given in Annexes B and C of IEC 61508-7.</td></tr>
<tr><td colspan="7">* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. It is intended the only one of the alternate or equivalent techniques/measures should be satisfied. The choice of alternative technique should be justified in accordance with the properties, given in Annex C, desirable in the particular application.</td></tr>
</table></td></tr>
<tr><td>6</td><td>HA process</td><td>None</td></tr>
<tr><td>7</td><td>Independence of HA (HA organization)</td><td>None</td></tr>
<tr><td>8</td><td>Harmonized HA of SoS</td><td>None</td></tr>
<tr><td>9</td><td>Relationship with other requirements (security, reliability)</td><td>None
It does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet a security policy that may be required by the E/E/PE safety-related system.</td></tr>
<tr><td>10</td><td>Discussion</td><td></td></tr>
</table>

B.2 [Aerospace industry] DO-178C

Table B.2 presents HA requirements in the aerospace safety standards ARP 4761[61], DO-178C[62].

Table B.2 – HA requirements in the aerospace safety standards ARP 4761, DO-178C

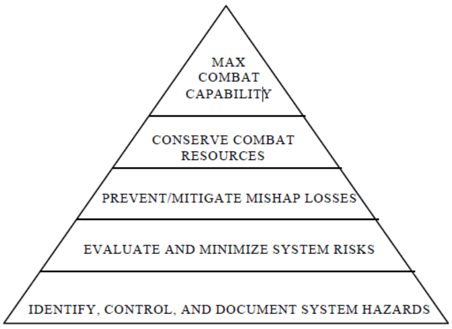
	Comparison criteria of HA requirements	**HA requirements in the safety standards of ARP 4761, DO-178C**
1	Safety principles (safety model or safety culture)	To provide guidance for the production of software for airborne systems and equipment that performs its intended function with a level of confidence in safety that complies with airworthiness requirements.
2	Safety processes	System safety assessment process – An ongoing, systematic, comprehensive evaluation of the proposed system to show that relevant safety-related requirements are satisfied. The major activities within this process include: functional hazard assessment, preliminary system safety assessment, and system safety assessment. →Out of the scope of DO-178C, included in the system life cycle processes defined in SAE ARP4754A.  SYSTEM LIFE CYCLE PROCESSES System Requirements Functional Hazard Assessment Preliminary System Safety Assessment System Safety Assessment Process System Approval Activities System Verification Activities System Integration Information Flow Between System and Hardware Life Cycle Processes HARDWARE LIFE CYCLE PROCESSES • Hardware/Software Integration Requirements • Coordination and Feedback • Identified Hardware/Software Incompatibilities • System Requirements Allocated to Software • System Safety Objectives • Software Level(s) • System Description and Hardware Definition • Design Constraints • Definition of System Verification Activities to be Performed by Software Processes • Definition and Evidence of any Software Verification Activities Performed by System Processes • Evidence of Acceptability of Data • Description of the Software Architecture • Evidence of any System Verification Activities Performed • Any Limitation of Use • Configuration Identification Data • Data to Facilitate Integration • Software Verification Activities to be Performed by System Processes Derived High-Level Requirements Derived Low-Level Requirements Problem or Change Documentation Software Planning Process Software Development Processes Software Requirements Process Software Design Process Software Coding Process Integration Process Software Verification Process Software Configuration Management Process Software Quality Assurance Process Certification Liaison Process SOFTWARE LIFE CYCLE PROCESSES
3	Definition of HA	None A complete description of the system life cycle processes, including the system safety assessment and validation processes, or the certification process is not intended.
4	Purpose of HA	None
5	Method of HA	None
6	HA process	None
7	Independence of HA (HA organization)	None

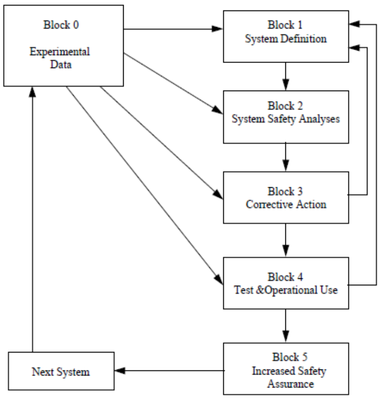
	Comparison criteria of HA requirements	**HA requirements in the safety standards of ARP 4761, DO-178C**
8	Harmonized HA of SoS	 System Boundary Software Boundary Latent Software Error in Data or Executable Code Fault System Failure Failure Condition (Effect at Aircraft Level) **Figure 2-2 Sequence of Events for Software Error Leading to a Failure Condition**
9	Relationship with other requirements (security, reliability)	None 12.3.3 Software Reliability Models Many methods for predicting software reliability based on developmental metrics have been published, for example, software structure, defect detection rate, etc. This document does not provide guidance for those types of methods, because at the time of writing, currently available methods did not provide results in which confidence can be placed.
10	Discussion	

B.3 [Air Force System Safety handbook], 2000[63]

Table B.3 presents HA requirements in Air Force System Safety handbook.

Table B.3 – HA requirements in Air Force System Safety handbook

	Comparison criteria of HA requirements	**HA requirements in the safety standard of Air Force System Safety handbook**
1	Safety principles (safety model or safety culture)	The ultimate objective of system safety is MAXIMIZED COMBAT CAPABILITY. A safe system is achieved through the implementation and careful execution of a system safety program. Figure 1-1  MAX COMBAT CAPABILITY CONSERVE COMBAT RESOURCES PREVENT/MITIGATE MISHAP LOSSES EVALUATE AND MINIMIZE SYSTEM RISKS IDENTIFY, CONTROL, AND DOCUMENT SYSTEM HAZARDS System Safety Goals System Safety: The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle. The handbook was recently revised to incorporate the provisions of the DoD Acquisition reform program and the new MIL-STD-882E.

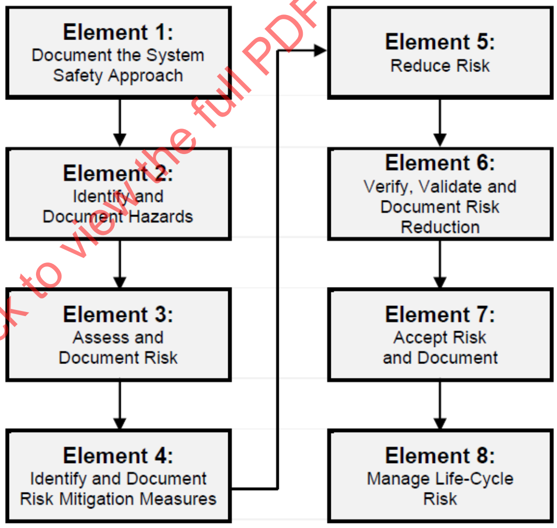
	Comparison criteria of HA requirements	**HA requirements in the safety standard of Air Force System Safety handbook**
2	Safety processes	The system safety process can be applied at any point in the system lifecycle, but the greatest advantages are achieved when it is used early in the acquisition stage of the life cycle. This process is normally repeated as the system evolves or changes and as problem areas are identified. The System Safety Process  Block 0 Experimental Data Block 1 System Definition Block 2 System Safety Analyses Block 3 Corrective Action Block 4 Test &Operational Use Block 5 Increased Safety Assurance Next System Figure 2-2
3	Definition of HA	5.6 Hazard Analysis The SSPP should describe: a The analysis techniques and formats to be used in qualitative or quantitative analysis to identify hazards, their causes and effects, hazard elimination, or risk reduction requirements and how those requirements are met. b The depth within the system to which each technique is used, including hazard identification associated with the system, subsystem, components, personnel, ground support equipment, GFE, facilities, and their interrelationship in the logistic support, training, maintenance, and operational environments. c The integration of subcontractor hazard analyses with overall system hazard analyses. (30:102-3)
4	Purpose of HA	Hazard analysis is the means of identifying hazards.
5	Method of HA	9.0 ANALYSIS TECHNIQUES 9.1 Fault Hazard Analysis 9.2 Fault Tree Analysis 9.3 Common Cause Failure Analysis 9.4 Sneak Circuit Analysis 9.5 Energy Trace 9.6 Evaluation of Analyses (General) 9.7 Preliminary Hazard Analysis Evaluation 9.8 Subsystem Hazard Analysis Evaluation 9.9 System Hazard Analysis Evaluation 9.10 Operating and Support Hazard Analysis Evaluation 9.11 Fault Tree Analysis Evaluation 9.12 Quantitative Techniques Evaluations
6	HA process	None
7	Independence of HA (HA organization)	None 11.0 PROGRAM OFFICE SYSTEM SAFETY 11.1 Program Office Description 11.2 System Safety Manager's Role 11.3 System Safety Manager's Responsibilities

	Comparison criteria of HA requirements	HA requirements in the safety standard of Air Force System Safety handbook
8	Harmonized HA of SoS	None
9	Relationship with other requirements (security, reliability)	None
10	Discussion	

B.4 [Military Industry] MIL-STD-882E (System Safety)[44]

Table B.4 presents HA requirements in the military safety standard MIL 882 E.

Table B.4 – HA requirements in the military safety standard MIL 882 E

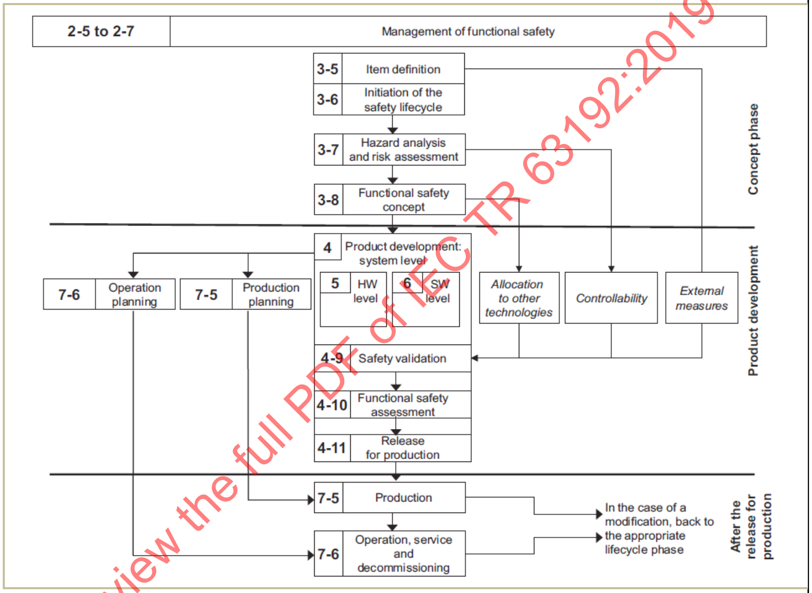
	Comparison criteria of HA requirements	HA requirements in the safety standard of MIL 882 E
1	Safety principles (safety model or safety culture)	To provides a standard, generic method for the identification, classification, and mitigation of hazards. A key DoD objective is to expand the use of this system safety methodology to integrate risk management into the overall SE (System Engineering) process rather than addressing hazards as operational considerations.
2	Safety processes	 Element 1: Document the System Safety Approach Element 2: Identify and Document Hazards Element 3: Assess and Document Risk Element 4: Identify and Document Risk Mitigation Measures Element 5: Reduce Risk Element 6: Verify, Validate and Document Risk Reduction Element 7: Accept Risk and Document Element 8: Manage Life-Cycle Risk **FIGURE 1. Eight elements of the system safety process** HTS(Hazard Tracking System) is used for safety demonstration through lifecycle The safety and risk assessments are conducted in system and software level separately.
3	Definition of HA	3.2.44 System safety engineering. An engineering discipline that employs specialized knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated. There is not a definition of hazard analysis, but System Safety Approach/Engineering is used.
4	Purpose of HA	The use of a system safety approach to identify hazards and manage the associated risks.

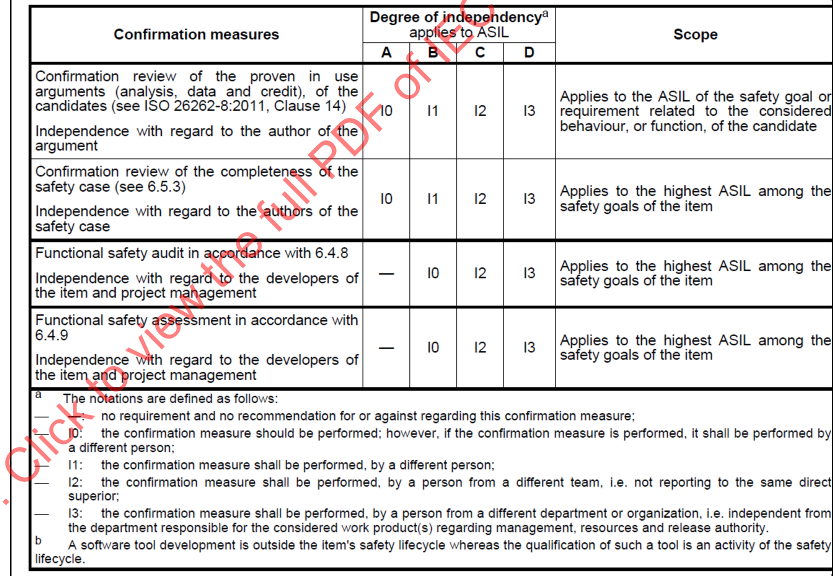
	Comparison criteria of HA requirements	HA requirements in the safety standard of MIL 882 E
5	Method of HA	The tasks in this Standard can be selectively applied to fit a tailored system safety effort TASK SECTION 100 – MANAGEMENT TASK 101 HAZARD IDENTIFICATION AND MITIGATION EFFORT USING THE SYSTEM SAFETY METHODOLOGY TASK 102 SYSTEM SAFETY PROGRAM PLAN TASK 103 HAZARD MANAGEMENT PLAN TASK 104 SUPPORT OF GOVERNMENT REVIEWS/AUDITS TASK 105 INTEGRATED PRODUCT TEAM/WORKING GROUP SUPPORT TASK 106 HAZARD TRACKING SYSTEM TASK 107 HAZARD MANAGEMENT PROGRESS REPORT TASK 108 HAZARDOUS MATERIALS MANAGEMENT PLAN TASK SECTION 200 – ANALYSIS TASK 201 PRELIMINARY HAZARD LIST TASK 202 PRELIMINARY HAZARD ANALYSIS TASK 203 SYSTEM REQUIREMENTS HAZARD ANALYSIS TASK 204 SUBSYSTEM HAZARD ANALYSIS TASK 205 SYSTEM HAZARD ANALYSIS TASK 206 OPERATING AND SUPPORT HAZARD ANALYSIS TASK 207 HEALTH HAZARD ANALYSIS TASK 208 FUNCTIONAL HAZARD ANALYSIS TASK 209 SYSTEM-OF-SYSTEMS HAZARD ANALYSIS TASK 210 ENVIRONMENTAL HAZARD ANALYSIS TASK SECTION 300 – EVALUATION TASK 301 SAFETY ASSESSMENT REPORT TASK 302 HAZARD MANAGEMENT ASSESSMENT REPORT TASK 303 TEST AND EVALUATION PARTICIPATION TASK 304 REVIEW OF ENGINEERING CHANGE PROPOSALS, CHANGE NOTICES, DEFICIENCY REPORTS, MISHAPS, AND REQUESTS FOR DEVIATION/WAIVER TASK SECTION 400 – VERIFICATION TASK 401 SAFETY VERIFICATION TASK 402 EXPLOSIVES HAZARD CLASSIFICATION DATA TASK 403 EXPLOSIVE ORDNANCE DISPOSAL DATA e: Identify the hazard analyses to be performed (e.g., Preliminary Hazard Analysis [PHA], Subsystem Hazard Analysis [SSHA]), analytical techniques to be used (e.g., Fault Tree Analysis [FTA], Failure Modes and Effects Criticality Analysis [FMECA]), and documentation of the results in the HTS.
6	HA process	None
7	Independence of HA (HA organization)	None
8	Harmonized HA of SoS	TASK 209 SYSTEM-OF-SYSTEMS HAZARD ANALYSIS 209.1 Purpose. Task 209 is to perform and document an analysis of the System-of-Systems (SoS) to identify unique SoS hazards. This task will produce special requirements to eliminate or mitigate identified unique SoS hazards which otherwise would not exist.
9	Relationship with other requirements (security, reliability)	None
10	Discussion	

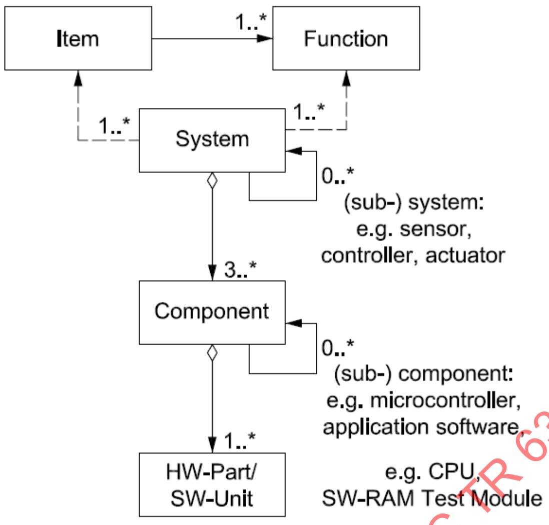
B.5 [Car Safety] ISO 26262 (Auto)[46],[47],[48],[49]

Table B.5 presents HA requirements in the car safety standard ISO 26262.

Table B.5 – HA requirements in the car safety standard ISO 26262

	Comparison criteria of HA requirements	HA requirements in the safety standard of (ISO 26262)
1	Safety principles (safety model or safety culture)	Safety issues are intertwined with common function-oriented and quality-oriented development activities and work products. ISO 26262 addresses the safety-related aspects of development activities and work products ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems.
2	Safety processes	Safety lifecycle provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases.  2-5 to 2-7 Management of functional safety 3-5 Item definition 3-6 Initiation of the safety lifecycle 3-7 Hazard analysis and risk assessment 3-8 Functional safety concept Concept phase 4 Product development: system level 5 HW level 6 SW level 7-6 Operation planning 7-5 Production planning Allocation to other technologies Controllability External measures 4-9 Safety validation 4-10 Functional safety assessment 4-11 Release for production Product development 7-5 Production 7-6 Operation, service and decommissioning In the case of a modification, back to the appropriate lifecycle phase After the release for production
3	Definition of HA	Hazard Analysis and Risk Assessment (26262-1) Method to identify and categorize hazardous events (1.59) of items (1.69) and to specify safety goals (1.108) and ASILs (1.6) related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk (1.136) Safety Analysis (26262-9) The scope of the safety analyses includes: the validation of safety goals and safety concepts; the verification of safety concepts and safety requirements; the identification of conditions and causes, including faults and failures, that could lead to the violation of a safety goal or safety requirement; the identification of additional requirements for detection of faults or failures; the determination of the required responses (actions/measures) to detected faults or failures; and the identification of additional requirements for verifying that the safety goals or safety requirements are complied with, including safety-related vehicle testing
4	Purpose of HA	The objective of the hazard analysis and risk assessment is to identify and to categorise the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.

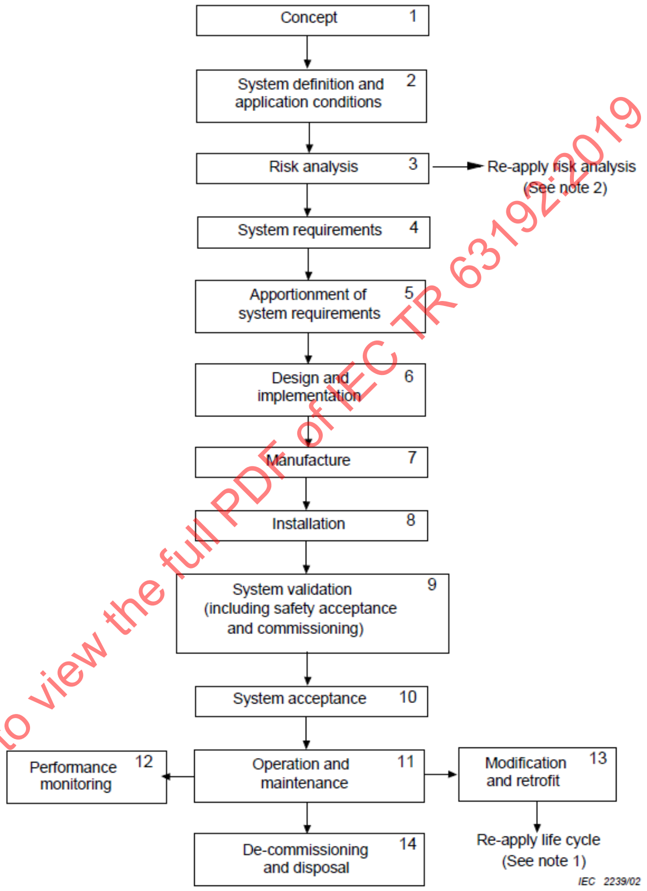
<table>
<tr><th></th><th>Comparison criteria of HA requirements</th><th>HA requirements in the safety standard of (ISO 26262)</th></tr>
<tr><td>5</td><td>Method of HA</td><td>7.4.2.2 Hazard identification
7.4.2.2.1 The hazards shall be determined systematically by using adequate techniques.
NOTE Techniques such as brainstorming, checklists, quality history, FMEA and field studies can be used for the extraction of hazards at the item level.
7.4.2.2.2 Hazards shall be defined in terms of the conditions or behavior that can be observed at the vehicle level.
7.4.2.2.3 The hazardous events shall be determined for relevant combinations of operational situations and hazards.
7.4.2.2.4 The consequences of hazardous events shall be identified.</td></tr>
<tr><td>6</td><td>HA process</td><td>ISO 26262-2:2011, Figure 2 – Safety Lifecycle
7.4.2.1 Situation Analysis
7.4.2.2 Hazard Identification
7.4.2.3 Classification of Hazardous events
7.4.4 Determination of ASIL and safety goals</td></tr>
<tr><td>7</td><td>Independence of HA (HA organization)</td><td>
<table>
<tr><th rowspan="2">Confirmation measures</th><th colspan="4">Degree of independency[a] applies to ASIL</th><th rowspan="2">Scope</th></tr>
<tr><th>A</th><th>B</th><th>C</th><th>D</th></tr>
<tr><td>Confirmation review of the proven in use arguments (analysis, data and credit), of the candidates (see ISO 26262-8:2011, Clause 14)
Independence with regard to the author of the argument</td><td>I0</td><td>I1</td><td>I2</td><td>I3</td><td>Applies to the ASIL of the safety goal or requirement related to the considered behaviour, or function, of the candidate</td></tr>
<tr><td>Confirmation review of the completeness of the safety case (see 6.5.3)
Independence with regard to the authors of the safety case</td><td>I0</td><td>I1</td><td>I2</td><td>I3</td><td>Applies to the highest ASIL among the safety goals of the item</td></tr>
<tr><td>Functional safety audit in accordance with 6.4.8
Independence with regard to the developers of the item and project management</td><td>—</td><td>I0</td><td>I2</td><td>I3</td><td>Applies to the highest ASIL among the safety goals of the item</td></tr>
<tr><td>Functional safety assessment in accordance with 6.4.9
Independence with regard to the developers of the item and project management</td><td>—</td><td>I0</td><td>I2</td><td>I3</td><td>Applies to the highest ASIL among the safety goals of the item</td></tr>
<tr><td colspan="6">[a] The notations are defined as follows:
— —: no requirement and no recommendation for or against regarding this confirmation measure;
— I0: the confirmation measure should be performed; however, if the confirmation measure is performed, it shall be performed by a different person;
— I1: the confirmation measure shall be performed, by a different person;
— I2: the confirmation measure shall be performed, by a person from a different team, i.e. not reporting to the same direct superior;
— I3: the confirmation measure shall be performed, by a person from a different department or organization, i.e. independent from the department responsible for the considered work product(s) regarding management, resources and release authority.
[b] A software tool development is outside the item's safety lifecycle whereas the qualification of such a tool is an activity of the safety lifecycle.</td></tr>
</table>
ISO 26262-2:2011, Table 1 – Required confirmation measure, including the required level of independency
5.4.3 Competence management (26262-2)
5.4.3.1 The organization shall ensure that the persons involved in the execution of the safety lifecycle have a sufficient level of skills, competence and qualification corresponding to their responsibilities.</td></tr>
</table>

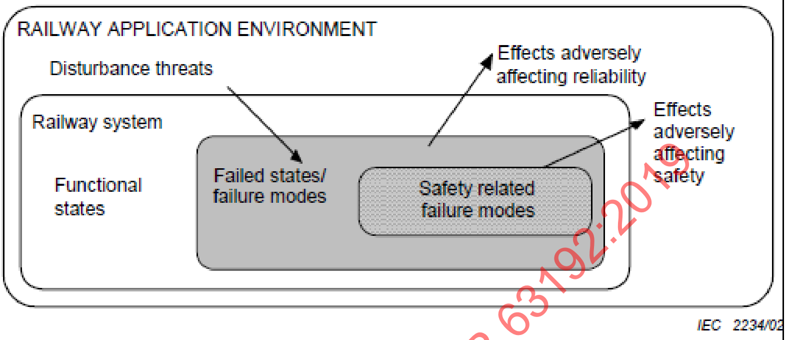
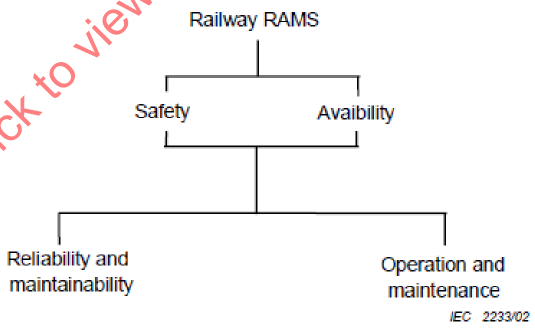
	Comparison criteria of HA requirements	**HA requirements in the safety standard of (ISO 26262)**
8	Harmonized HA of SoS	 Item Function 1..* System 1..* 1..* 0..* (sub-) system: e.g. sensor, controller, actuator 3..* Component 0..* (sub-) component: e.g. microcontroller, application software, 1..* HW-Part/ SW-Unit e.g. CPU, SW-RAM Test Module ISO 26262-10, Figure 3 – Relationship of item, system, component, hardware part and software unit
9	Relationship with other requirements (security, reliability)	ISO 26262-10, 11.3 An example of ASIL decomposition 11.3.3 Hazard analysis and risk assessment SAE J3061 – Security Process
	Discussion	

B.6 [Railway Industry] IEC 62278:2002(RAMS)[45]

Table B.6 presents HA requirements in the railway safety standard IEC 62278:2002.

Table B.6 – HA requirements in the railway safety standard IEC 62278:2002

	Comparison criteria of HA requirements	HA requirements in the safety standard of IEC 62278:2002
1	Safety principles (safety model or safety culture)	Not specified the safety alone. Provides a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS. Processes for the specification and demonstration of RAMS requirements are the cornerstones of this standard.
2	Safety processes	 Concept 1 System definition and application conditions 2 Risk analysis 3 Re-apply risk analysis (See note 2) System requirements 4 Apportionment of system requirements 5 Design and implementation 6 Manufacture 7 Installation 8 System validation (including safety acceptance and commissioning) 9 System acceptance 10 Operation and maintenance 11 Performance monitoring 12 Modification and retrofit 13 Re-apply life cycle (See note 1) De-commissioning and disposal 14 IEC 2239/02 NOTE 1 The phase at which a modification enters the life cycle will be dependent upon both the system being modified and the specific modification under consideration. NOTE 2 Risk analysis may have to be repeated at several stages of the life cycle (see item d) of 6.3.1). **Figure 8 – System life cycle** Each phase has safety tasks as well as other elements.
3	Definition of HA	None 3.17 Hazard: Physical situation with a potential for human injury and/or damage to environment 3.35 Safety: Freedom from unacceptable risk of harm
4	Purpose of HA	To identify hazards and assess risk in phase 2 and 3.
5	Method of HA	None
6	HA process	None
7	Independence of HA (HA organization)	None

	Comparison criteria of HA requirements	**HA requirements in the safety standard of IEC 62278:2002**
8	Harmonized HA of SoS	4.3.7 Failures in a system, operating within the bounds of an application and environment, will have some effect on the behaviour of the system. All features adversely affect the system reliability whereas only some specific failures will have an adverse effect on safety within the particular application. Environment may also influence the functionality of the system and in turn the safety of the railway application.  RAILWAY APPLICATION ENVIRONMENT Disturbance threats Effects adversely affecting reliability Railway system Effects adversely affecting safety Functional states Failed states/ failure modes Safety related failure modes IEC 2234/02 **Figure 3 – Effects of failures within a system**
9	Relationship with other requirements (security, reliability)	Enables conflicts between RAMS elements to be controlled and managed effectively. 4.3.8 A dependable railway system can only be realized through consideration of the interactions of RAMS elements within a system and the specification and achievement of the optimum RAMS combination for the system.  Railway RAMS Safety Availibility Reliability and maintainability Operation and maintenance IEC 2233/02 **Figure 2 – Inter-relation of railway RAMS elements** 4.3.4 However, consideration of security is outside the scope of this standard.
10	Discussion	

B.7 [Medical Industry] IEC 60601-1:2005, Medical electrical equipment – Part 1: General requirements for basic safety and essential performance[64]

Table B.7 presents HA requirements in the medical safety standard IEC 60601-1:2005.