IEC 60744

Edition 2.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Instrumentation and control systems important to safety – Safety logic assemblies used in systems performing category A functions: Characteristics and test methods

Centrales nucléaires de puissance – Systèmes d’instrumentation et de contrôle-commande importants pour la sûreté – Ensembles logiques de sûreté utilisés dans les systèmes réalisant des fonctions de catégorie A: Caractéristiques et méthodes d'essai

IEC 60744:2018-05(en-fr)

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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.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

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms, containing 21 000 terms and definitions 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 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.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 21 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC 60744

Edition 2.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Instrumentation and control systems important to safety – Safety logic assemblies used in systems performing category A functions: Characteristics and test methods

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Ensembles logiques de sûreté utilisés dans les systèmes réalisant des fonctions de catégorie A: Caractéristiques et méthodes d'essai

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 21.120.20

ISBN 978-2-8322-5681-7

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SAFETY LOGIC ASSEMBLIES USED IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS: CHARACTERISTICS AND TEST METHODS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60744 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1983. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) update of the references to standards published or revised since the issue of the first edition of the current standard, including IEC 61513 and IEC 61226;
b) additional requirements for operational and maintenance bypass use; requirements of voting logic; requirements for interfacing with the MCR and SCR.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1188/FDIS	45A/1200/RVD

Full information on the voting for the approval of this International Standard 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.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

This standard IEC 60744 specifically focuses on safety logic assemblies used in NPPs (Nuclear Power Plants). Safety logic assemblies were originally hardwired parts of protection systems mainly used to control actuators. IEC 60744 specifically focuses on the design, including technology, interfaces with MCR and SCR, tests and qualification. It gives requirements for display of the safety system inputs and state.

IEC 60744 is the document concerning safety logic assembly functions and performance.

The use of a computer based equipment or software is covered comprehensively by other standards. The technology used to design SLAs therefore involves mainly hard-wired technologies and submicronic highly integrated components (HPDs), the implementation of which is limited due to the very high safety requirements.

The document addresses the design and test characteristics of safety logic assemblies, especially regarding functional requirements, reliability issues, and associated control means including alarm, indication and control. Also it suggests the requirements for performance, testing and qualification for safety logic assemblies, and the interface requirements for communication between assemblies.

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

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

IEC 60744 is the third level IEC SC 45A document tackling the specific issue of testing and design characteristics of safety logic assemblies.

IEC 60744 is to be read in association with IEC 61513 which is the appropriate IEC SC 45A document which provides guidance on I&C safety system, and IEC 60964 which is the appropriate document for guidance on the Control Rooms, since the safety system has extensive interfaces with the MCR and SCR.

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 Standard

It is important to note that this document establishes no additional functional requirements at safety system level.

Aspects for which special recommendations have been provided in this document are:

- The voting of partial trips to identify each safety actuation
- The output assemblies that provide the trips and actuations
- The design and test characteristics of functional requirements
- The reliability issue of safety logic assemblies
- The performance characteristics of logic assemblies
- Testing, qualification and interface requirements of safety logic assemblies

To ensure that the document will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

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, defense against common cause failure, control room design, electromagnetic compatibility, cybersecurity, 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.

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-3 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, regarding control rooms, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the IEC SC 45A 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 requirement 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 – SAFETY LOGIC ASSEMBLIES USED IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS: CHARACTERISTICS AND TEST METHODS

1 Scope

This document provides requirements and recommendations for the design, construction and test of safety logic assemblies used in safety systems to perform category A safety functions (in accordance with IEC 61226). Safety logic assemblies include logic such as the hardwired logic assembly interfacing computer-based systems to switchgear, actuators or contactors to provide trip or engineered safety feature actuations. Safety logic assemblies are significant parts of a safety system and may include voting logic between redundant channels.

This document provides a general description of safety logic assemblies for safety actuators control. The principles to meet dependability objectives are presented. The main features relating to the design requirements are described and explained.

Various tests and their requirements are given in order to validate the design (including the qualification tests), the manufacturing and the correct installation on site.

Annex A (informative) gives a list of possible applications of safety logic assemblies.

Annex B (normative) suggests a list of possible hardwired technologies with their respective requirements to design safety logic assemblies.

Annex C (informative) gives explanations on dependability and its attributes to improve reliability and to reduce the final risk which compromises the safety and the availability of the NPP.

The scope of this document does not address the design of a protection system, it covers only the technological and architectural solutions required to design a safety logic assembly. The design of safety systems using safety logic assemblies is covered by IEC 61513.

The detailed and specific functions implemented in a safety logic assembly strongly depend on the design of each reactor and are not addressed in this document.

As this document is focused on I&C part of the system, the final voting logic made with power breakers is excluded from the scope of this document.

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 60255 (all parts), *Measuring relays and protection equipment*

IEC 60671, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60709, *Nuclear power plants – instrumentation and control systems important to safety – Separation*

IEC/IEEE 60780-323, *Nuclear facilities – Electrical equipment important to safety – Qualification*

IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 60964, *Nuclear power plants – Control rooms – Design*

IEC 60965, *Nuclear power plants – Control rooms – Supplementary control room for reactor shutdown without access to the main control room*

IEC 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61225, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for electrical supplies*

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

IEC 61227, *Nuclear power plants – Control rooms – Operator controls*

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

IEC 62003, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

IEC 62241, *Nuclear power plants – Main control room – alarm functions and presentation*

IEC 62566:2012, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

IAEA-GSR Part 2, *Leadership and Management for Safety*

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
availability
ability of an item or a system to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, given that the necessary external resources are provided

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.2
channel
arrangement of interconnected components within a system that initiates a single output. A channel loses its identity where the single-output signals are combined with signals from another channels (eg; from a monitoring channel or a safety actuation channel)

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.3
dependability
general term describing the overall trustworthiness of a system; i.e. the extent to which reliance can justifiably be placed on this system. Reliability, availability and safety are attributes of dependability

Note 1 to entry: Annex C gives clarifications on this definition.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.4
dynamic logic equipment
system assembly or subassembly employing dynamic logic signals

3.5
dynamic logic signal
periodically changing voltage or current, the frequency being consistent with the required system response time. The different logic states are associated with different values of one or more parameters of the periodic change, for example, amplitude, slope, repetition rate of pulses or alternations, or pulse coding

Note 1 to entry: One logic state may be associated with the absence of periodic change of such a signal.

3.6
engineered safety feature
actuating part of a safety actuation system (actuator associated with its electrical and driving part)

Note 1 to entry: Engineered safety features need energy to operate (valves, motors, etc.). Generally, they are compared with reactor trip breakers which do not need energy to operate.

3.7
failure
loss of the ability of a structure, system or component to function within acceptance criteria

Note 1 to entry: The structure, system or component is considered to fail when it becomes incapable of functioning, whether or not this is needed at that time. A failure in, for example, a backup system may not be manifest until the system is called upon to function, either during testing or on failure of the system it is backing up.

Note 2 to entry: A failure of a structure, system or component is an event that results in a fault of that structure, system or component.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.8
Field Programmable Gate Array
FPGA
integrated circuit that can be programmed in the field by the I&C manufacturer. It includes programmable logic blocks (combinatorial and sequential), programmable interconnections between them and programmable blocks for input and/or outputs. The function is then defined by the I&C designer, not by the integrated circuit supplier

Note 1 to entry: While FPGAs are essentially digital devices, some of them may integrate analogue input/outputs and analogue to digital converters. FPGAs may include advanced digital functions such as hardware multipliers, dedicated memory and embedded processor cores.

[SOURCE: IEC 62566:2012, 3.5]

3.9
hardware description language
HDL
language used to formally describe the functions and/or the structure of an electronic component for documentation, simulation or synthesis

[SOURCE: IEC 62566:2012, 3.6]

3.10
HDL-Programmed Device
HPD
integrated circuit configured (for NPP I&C systems) with hardware description languages and related software tools

[SOURCE: IEC 62566:2012, 3.7]

3.11
operational states
states defined under normal operation and anticipated operational occurrences

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.12
partial trip signal

binary signal provided by a channel of a safety system after processing the signals received from the sensors of this channel, before it has been processed by the final voting logic to give a scram requirement or ESF actuation requirement

3.13
programmable logic device
PLD
integrated circuit that consists of logic elements with an interconnection pattern, parts of which are user programmable

Note 1 to entry: Different kinds of PLDs exist, e.g. Erasable PLD or Complex PLD (CPLD).

Note 2 to entry: The differences between “FPGA” and “PLD” are not well defined, but “PLD” usually refers to a simpler device than “FPGA”.

[SOURCE: IEC 62566:2012, 3.13]

3.14
qualified life
period for which a structure, system or component has been demonstrated, through testing, analysis or experience, to be capable of functioning within acceptance criteria during specific operating conditions while retaining the ability to perform its safety functions in accident conditions for a design basis accident or a design basis earthquake

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.15
redundancy
provision of alternative (identical or diverse) structures, systems and components, so that any single structure, system or component can perform the required function regardless of the state of operation or failure of any other

Note 1 to entry: This definition has to be clarified for the needs of this document:

- Non-diverse redundancy – to address the risk of single (random) failure.
- Diverse redundancy – to address the risk of random failure or common mode failure.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.16
reliability
probability that a device, system, component or facility will meet its minimum performance requirements when called upon to do so

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.17
safety (nuclear)
protection of people and the environment against radiation risks, and the safety of facilities and activities that give rise to radiation risks

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.18
safety function
specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions

Note 1 to entry: IAEA SSR2/1 establishes requirements on safety functions to be fulfilled by the design of a nuclear power plant in order to meet three general safety requirements:

a) the capability to safely shut down the reactor and maintain it in a safe shutdown condition during and after appropriate operational states and accident conditions;

b) the capability to remove residual heat from the reactor core, the reactor and nuclear fuel in storage after shutdown, and during and after appropriate operational states and accident conditions;

c) the capability to reduce the potential for the release of radioactive material and to ensure that any releases are within prescribed limits during and after operational states and within acceptable limits during and after design basis accidents.

Note 2 to entry: IEC 61226 gives recommendations related to categories of safety functions.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.19
safety logic assembly
equipment, part of a protection system performing simple category A logic functions with a very high level of dependability and generally used to send commands to safety actuators or signals to another safety logic assembly

Note 1 to entry: A simple logic function is combinatory and/or sequential. Consequently, such a function is fully testable.

3.20
safety system
system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the reactor core, or to limit the consequences of anticipated operational occurrences and design basis accidents

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.21
scram
rapid shutdown of a nuclear reactor in an emergency

Note 1 to entry: The term scram is associated with the trip unit which is the part of a circuit breaker that opens the circuit. Then a scram is often called a reactor trip.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.22
single failure
failure which results in the loss of capability of a single system or component to perform its intended safety function(s), and any consequential failure(s) which result from it

Note 1 to entry: A single failure is generally caused by effects such as corrosion, thermal stressing and wear-out which applies to hardware components within a system.

Note 2 to entry: Single failure is also called: ”random failure”.

Note 3 to entry: Due to their random nature, statistical information can be produced from testing and historical data. Thus, the average probability, and hence the risk, associated with the occurrence of a random failure can be calculated.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.23
trip
rapid reduction in the power of a nuclear reactor

Note 1 to entry: A reactor trip is also called “scram”.

[SOURCE: IEC 60050-395:2014, 395-07-91]

4 Abbreviated terms and acronyms

CCF	Common Cause Failure
CPLD	Complex Programmable Logic Device
EMC	Electro Magnetic Compatibility
EMR	Electro Magnetic Relay
EMI/RFI	Electromagnetic Interference / Radiofrequency Interference
ESF	Engineered Safety Feature (and post-trip actions and sequences)
ESFAS	Engineered Safety Feature Actuating System
FMEA	Failure Mode and Effect Analysis
FPGA	Field Programmable Gate Array
HDL	Hardware Description Language
HPD	HDL-Programmed Device
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
MCR	Main Control Room
NPP	Nuclear Power Plant
PIE	Postulated Initiating Event
PLD	Programmable Logic Device