WORLD NUCLEAR ASSOCIATION

Safety Classification for I&C Systems in Nuclear Power Plants: Comparison of Definitions of Key Concepts

Cooperation in Reactor Design Evaluation and Licensing Working Group of the World Nuclear Association

2019 revision

Title: Safety Classification for I&C Systems in Nuclear Power Plants: Comparison of Definitions of Key Concepts
Produced by: World Nuclear Association
Published: October 2019
Report No. 2019/008

Contents

Foreword

The Cooperation in Reactor Design Evaluation and Licensing Working Group (CORDEL) was established by the World Nuclear Association in 2007 with the aim of stimulating a dialogue between the nuclear industry (including reactor vendors and operators) and nuclear regulators on the benefits and means of achieving a worldwide convergence of industry standards for reactor designs.

The Digital Instrumentation & Control Task Force (DICTF) of CORDEL was set up in 2013 to investigate key issues in digital instrumentation and control (I&C) related to the licensing of new nuclear power plants. The task force collaborates with the International Electrotechnical Commission (IEC) and the Multinational Design Evaluation Programme (MDEP) the Nuclear Energy Association, and (NEA) Digital Instrumentation and Control Working Group (DICWG).

On the basis of a survey of its members, the CORDEL DICTF has identified four main issues for investigation:

- Safety classification for I&C systems in nuclear power plants.
- Defence-in-depth and diversity (DiD&D)[1].
- Field-programmable gate arrays (FPGA): criteria for acceptance.
- Reliability predictions.

These are discussed in more detail in *CORDEL DICTF 2014-2016 Outlook* [1].

This is the second of three reports on *Safety Classification for I&C Systems in Nuclear Power Plants*. The first report describes the current status in classification of I&C systems and identifies key causes of difficulties as well as potential solutions.

The current report investigates the differences between the definitions of key concepts used in different regulatory frameworks. The report also discusses approaches for harmonizing the understanding of several key concepts.

This revision was prepared to address comments on the original version provided by the NEA CNRA DICWG. As a result several errors were corrected, recommendations for bringing more consistency to international terminology were expanded, and the terminology given for the Finish regulator was updated to take account of changes that were incorporated into the Finish Decree 717 released in 2013. This Decree brought the definitions of the terms we studied closer to those used by other nuclear regulators.

As this edition of the report was going to print the 2018 IAEA Safety Glossary became available. The 2018 Glossary made a number of small changes to the IAEA terms and definitions of in the 2007 version. The differences between the 2007 terms used in this report and the terms given in the 2018 version were examined and it was concluded that updating the report to include the current IAEA terminology would not substantively change the conclusions of this report.

This report was drafted by Gary Johnson and Mark Burzynski, with the input and support from the members of the Task Force.

[1] Originally referred to as: diversity and common cause failure (CCF)

Executive Summary

The World Nuclear Association report, *Safety Classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties*, by the Cooperation in Reactor Design Evaluation and Licensing Working Group (CORDEL) identified a number of key concepts which are important for the industry to understand and implement correctly in order to meet licensing requirements, but which are often vaguely or inconsistently defined by regulatory bodies.

Where requirements are not clearly defined, there is room for different interpretation. Divergent understanding could have a large impact over the duration of the project lifecycle.

The safety classification report identified the following five concepts as frequently causing problems in the interpretation of requirements:

- Defence-in-Depth and Diversity.
- Separation (physical separation / electrical isolation / functional independence / independence of communication).
- Redundancy.
- Reliability/Availability.
- Spurious Activation (inadvertent actuation of I&C functions).

The concept of Independence was added to this list of concepts to be reviewed, as several of the terms stated in the first safety classification report dealt with various aspects of Independence.

Each of the above concepts is defined by a series of terms and associated definitions in different regulatory documents and reference codes & standards. As long as there is no harmonized understanding for such top-level concepts there will be risks of misunderstandings in every project, which may lead to conflicts with contractual requirements and regulatory conformance.

This report compares the various definitions by:

- identifying all the terms that are associated with the key concepts and
- highlighting any inconsistencies in the different regulatory bodies' definitions of these terms.

1 Approach

The World Nuclear Association CORDEL report, *Safety Classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties* [2], identified a number of concepts which are important for the industry to understand and implement correctly in order to meet licensing requirements, but which are often inconsistently defined by regulatory bodies.

This report starts by identifying all the terms which are associated with the concepts and which are used to define the concepts. The report then presents all the definitions for each term from the nuclear regulatory bodies that took part in the Nuclear Energy Agency's MDEP, and the international bodies that produce standards for nuclear power instrumentation and control systems. The aim of this exercise is twofold:

- To identify all the terms that are associated with the concepts explored.
- To highlight the difficulties associated with the inconsistency of definitions between the different regulatory bodies and Standard Development Organizations around the world.

This section describes the approach taken to identify and compare definitions for the concepts identified as troublesome in the interpretation of requirements, particularly when addressing different regulatory frameworks.

The first safety classification report identified the following five concepts as frequently causing problems in the interpretation of requirements:

- Defence-in-Depth and Diversity.
- Separation (physical separation/ electrical isolation/functional independence/independence of communication).
- Redundancy.
- Reliability/Availability.
- Spurious Activation (inadvertent actuation of I&C functions).

A sixth concept, Independence, was added to this list, as several of the terms stated in the safety classification report dealt with various aspects of Independence.

The fundamental approach taken was to search regulatory documents to identify the terms and definitions that these organizations use to convey the meaning of these concepts. The terms and definitions related to each concept were then compared to identify consistency and conflicts between the definitions given by the various regulatory organizations. The report then identifies what CORDEL considers to be the terms and definitions that best represent industry's understanding of the main concepts.

1.1 Sources of terms and definitions

Most regulatory organizations provide the definitions of important concepts in their formal regulations, requirements documents or glossaries.

This report examines the documents from the regulatory bodies and standards development organizations (SDO) that participate in or observe the MDEP[2] Digital Instrumentation & Control Working Group (DICWG). The organizations are presented in Table 1.

Glossaries, regulations, and regulatory requirements were chosen as the source of terminology as the definitions they provide are formally accepted by the organizations. Other kinds of documents are available from regulators, but such background papers often include definitions that apply only within that document.

[2] MDEP was a multinational initiative to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities that are currently or will be tasked with the review of new nuclear power reactor designs. The MDEP working group was transferred to the Nuclear Energy Agency Committee on Nuclear Regulatory Activities (CNRA) as the Working Group on Digital Instrumentation and Control (WGDIC).

Table 1. List of organizations whose terms and definitions are considered

Organization	Acronym
Atomic Energy Regulatory Board (India)	AERB
Nuclear Safety Authority (France)	ASN
Canadian Nuclear Safety Commission	CNSC
Federal Authority for Nuclear Regulation (UAE)	FANR
Federal Environmental, Industrial and Nuclear Supervision Service of Russia - Rostechnadzor (Russia)	RTN
International Atomic Energy Agency*	IAEA
International Electro-technical Commission*	IEC
Institute for Electrical and Electronic Engineers*	IEEE
Nuclear Safety and Security Commission (South Korea)	NSSC
National Nuclear Regulator (South Africa)	NNR
National Nuclear Safety Administration (China)	NNSA
Nuclear Regulatory Authority (Japan)	NRA
United States Nuclear Regulatory Commission	NRC
Office for Nuclear Regulation (UK)	ONR
Swedish Radiation Safety Authority	SSM
Radiation and Nuclear Safety Authority (Finland)	STUK
Turkish Atomic Energy Authority	TAEK

*Observers at the MDEP DICWG

Our approach produced an extensive list of definitions related to the concepts identified in the safety classification report [2]. The definitions are not always easily available for all regulatory bodies investigated, and not always in the English language. When necessary, DICTF members provided what they understand to be definitions used by their regulatory organizations. In the case of China we were informed that the Chinese regulators use terminology from the regulatory authority in the country of each plant's origin.

Starting from the basic concepts mentioned above, we examined glossaries, regulations, and requirements documents published by the regulators and SDOs listed in Table 1. This examination found that these organizations used 41 terms to represent the six concepts.

Fourteen of the terms considered deal with special cases of the main concepts. They were retained in the analysis to track which organizations formally defined these terms and to allow for comparisons where a special case term was used by more than one organization.

The final list of terms considered is given in Table 2.

Appendix A lists the concepts and the corresponding definitions for each of the organizations listed in Table 1.

1.2 Identification of similarities and differences

The terms and definitions are organized into groups that deal with the identified concepts. This resulted in further breakdown of some concepts.

No definition was found for the concept of Defence-in-Depth and Diversity but definitions exist for the term Defence-in-Depth and for the term Diversity, thus these two terms are considered separately, despite being strongly related.

The concept of Reliability was expressed by three related concepts: Reliability; Availability; and Dependability. To allow for a direct comparison of terms, this concept was evaluated as three separate, but related concepts.

No regulator gave terms and definitions for the concept of Spurious Activation as an unintended initiation of plant I&C functions, but one regulator gave a definition for a similar idea relating to cyber security. Thus to track the different understandings of the concept, we evaluated the concept Spurious Activation as two related concepts. Spurious Activation to mean un-commanded activation of an I&C function and Spurious Initiation meaning initiation of I&C functions resulting from a cyber-attack.

With these additions, 11 concepts were considered in this analysis:

- Defence-in-Depth and Diversity.
- Defence-in-Depth.
- Diversity.
- Separation.
- Redundancy.
- Reliability.
- Availability.
- Dependability.
- Spurious Activation.
- Spurious Initiation.
- Independence.

Each term and associated definition are listed in tables according to the most closely related concept. An attempt was made to list first the definition that seemed to most completely describe the concept involved. Identical or very similar definitions were grouped together and observations are made about the differences between groups. Each concept was then reviewed to develop more general comments about the entire group of definitions for each concept.

The analysis of the terms associated with each concept is given in Appendix B.

Table 2. Complete list of terms considered

Original concepts	Additional concepts related to the original concepts	Final set of terms investigated
Defence-in-Depth and Diversity*	Defence-in-Depth and Diversity	Defence-in-Depth and Diversity*
	Defence-in-Depth	Defence-in-Depth
	Diversity	Diversity
		Diversification
		Diversity [Software]
		Diversity Principle
		Physical Diversity
		Engineering Diversity
		Functional Diversity
		Signal Diversity
		Diverse Instrumentation and Control Systems
		Diverse Protection System
		Diverse Indication System
		Diverse Manual ESF Actuation Switches
Separation	Separation	Separation
		Geographical Separation
		Physical Separation
		Segregation
		Separation of Subsystems
		Separation Principle
		Separation Distance
Redundancy	Redundancy	Redundancy
		Redundancy Principle
		Redundant Equipment or Systems
		Engineering Redundancy
		Standby Redundancy
Reliability	Reliability	Reliability
		System Reliability
		Reliability Targets
		Operational Reliability
	Availability	Availability
		Operational Availability
	Dependability	Dependability
Spurious Activation*	Spurious Activation	Spurious Activation*
	Spurious Initiation	Spurious Initiation
Independence	Independence	Independence
		Independence Principle
		Independent Equipment
		Independent Systems
		Operational Separation
		Functional Isolation
		Functional Separation
		Isolation Device
		Communications Independence*

*No definition found

2 Conclusions and Recommendations

The analysis documented in Appendix B produces both general findings about the full set of concepts and about the individual definitions related to the terms listed in table 2.

2.1 General conclusions

The 17 organizations considered in this study use 43 different terms that are closely related to the 11 concepts identified above.

Six concepts are defined by at least 30% of the organizations: Defence-in-Depth, Diversity, Separation, Reliability, Availability and Independence. In no case are the definitions consistent over all 17 organizations.

The use of different terms is classified as follows:

- Different terms used to describe the 11 concepts considered in this report (19 cases), for example: Separation and Segregation are both used for the concept Separation.
- Terms that describe a condition that is a subset or special case of a concept that was previously defined by the organization (19 cases), for example: Diversity, Signal Diversity.
- Different terms given for the same concept by a given organization (1 case).
- Multiple definitions for the same term within an organization (9 cases).

The wide variety of terms used for what are essentially the same concepts will make communications between vendors and regulatory agencies difficult. As it stands, every time a vendor starts a project in a new country it must ensure that it fully understands the terminology used by the regulators.

Definitions given by the IAEA are used by several organizations, but in no case did all organizations use the IAEA definition of a concept. In many cases the IAEA definition of a concept encompasses the definitions used by the other organizations, *i.e.* some of the other definitions have less detail or are narrower.

For the most part the definitions used by the three standards development organizations (IAEA, IEC, and IEEE) do not conflict with each other. This is not too surprising as for many years IEC SC45A[3] has had the policy of using IAEA definitions wherever possible. Also, IEEE participants include individuals from several countries who also participate in the development of IEC standards. The largest issue is that the IEEE definition of independence covers a narrower range of possible interactions than the IAEA definition.

2.2 Specific conclusions

A summary of the findings for each of the original key concepts is given in Table 3, which presents an overview of the similarity and differences in the definitions given by the organizations. See Appendix B for the details supporting the discussion below.

It is important to note that translations from the native language to English may lead to unintended differences in terminology. We do not know to what extent the differences of terminology are a result of different translations.

Terms outlined in heavy lines represent the originally defined concepts.

Terms in italics represent special cases of the main definition.

The various coloured boxes indicate definitions that are the same or similar.

- Boxes are filled with solid colour where multiple organizations gave the same or similar definitions for a concept that are listed in the second column of Table 2.

[3] The IEC SC 45A is the IEC subcommittee responsible for the standards related to instrumentation, control and electrical power systems of nuclear facilities.

Table 3. Summary of terms used to define key concepts

Country		CAN	CHN	FIN	FRA	IND	JPN	ROK	RUS	ZAF	SDO	SDO	SDO	SWE	TUR	ARE	GBR	USA
Search Terms Organization	Usage	CNSC	NNSA	STUK	ASN	AERB	NRA	NSSC	RTN	NNR	IEEE	IAEA	IEC	SSM	TAEK	FANR	ONR	NRC
Defence-in-Depth and Diversity	0																	
Defence-in-Depth	8				x	x		x		xx		xx		x		x		x
Diversity	9	x			x	x	x					xx	x		x	x	x	
Diversification	1													x				
Diversity [Software]	1																x	
Diversity Principle	2			x					x									
Physical Diversity	1											x						
Engineering Diversity	1																x	
Functional Diversity	3							x				x	x					
Signal Diversity	1							x										
Diverse Instrumentation and Control Systems	1																	x
Diverse Protection System	1							x										
Diverse Indication System	1							x										
Diverse Manual ESF Actuation Switches	1							x										
Separation	2							x			x							
Geographical Separation	1				x													
Physical Separation	7			x	x	x						x		x	x	x		
Segregation	1																xx	
Separation of Subsystems	0																	
Separation Distance	2							x			x							
Redundancy	11			x	x	x	x	x			x	x	x	x		x	x	
Redundancy Principle	2			x					x									
Redundant Equipment or Systems	3							x			x							x
Engineering Redundancy	1																x	
Standby Redundancy	1							x										
Reliability	6					x		x			x	x	x				x	
System Reliability	2							x			x							
Reliability Targets	2							x			x							
Operational Reliability	2							xx			x							
Availability	6	x				x		xx			xx	xx	xx					
Operational Availability	2							x			x							
Dependability	1											x						
Spurious Activation	0																	
Spurious Initiation	1							x										
Independence	6	xx			x	x	x	x			x							
Independence Principle	1								x									
Independent Equipment	2											x	x					
Independent Systems	1								x									
Operational Separation	0																	
Separation Principle	1			x														
Functional Isolation	3			x								x				x		
Functional Separation	1													x				
Isolation Device	2							x			x							
Communications Independence	0																	
Number of definitions found		4		6	6	7	3	22	4	2	13	14	7	5	2	5	8	3

- Boxes are filled with coloured hash marks where multiple organizations gave the same or similar definitions that deal with only part of a concept listed in column 2 of Table 2.

Similarly, coloured boxes in the x columns indicate similar definitions. Note that similar definitions are not always associated with the same term. There are also cases where multiple organizations agree on more than one definition of a concept. In this case different shades of the same colour are used to indicate which organizations agree on similar definitions

A double x indicates that the associated organization gave more than one definition for the term.

For the term 'availability' three definitions were used by more than one organization. Six organizations had the same or similar definitions as indicated by red coloured boxes. NSSC and IEEE agreed on a second definition as indicated by red outlines around their boxes, and IAEA and IEC agreed on a third definition as indicated by green outlines around their boxes

2.2.1 Defence-in-Depth and Diversity

No organization gives a specific definition of Defence-in-Depth and Diversity but the components of this concept are defined. Indeed the term is often applied as a simple concatenation of two different but mutually supporting concepts. Thus a separate definition of the term is not needed.

2.2.2 Defence-in-Depth

Eight of the 17 organizations studied provided definitions for this concept.

The IAEA gives the most general definition. The IAEA definition is also used by FANR, and NNR. The IAEA definition is not consistent with the INSAG-10 [4] approach, which is not universally used.

AERB gives a weaker definition.

NRC gives a definition that is not useful for technical use and appears to be aimed at explaining the concept to the public. This definition is reported to also be used by NSSC.

ASN gives a very specific definition that adopts a portion of the description of Defence-in-Depth that is given in INSAG-10. It is neither fully consistent with INSAG-10 nor with the definition given in the IAEA Safety Glossary. Nevertheless, a design that complies with IAEA SSR 2/1 [3] is likely to satisfy the definition given by ASN.

2.2.3 Diversity

Twelve of the 17 organizations gave definitions for the concept of Diversity. In some of these cases the term Diversification or Diversity Principle was used.

The IAEA provides the most general definition. It is equivalent to those used by most other organizations and in the remaining ones the definitions do not conflict with the IAEA's. CNSC, ONR, AERB, NRA, SSM, and RTN, essentially use the IAEA definition.

Some organizations define the terms for specific types of diversity such as Functional Diversity or Diverse Instrumentation and Control Systems. These do not conflict with the general definition of Diversity. Although the different types of diversity are considered by most organizations in the assessment of I&C systems, definitions of the various types are not always given in high-level documents.

2.2.4 Separation

Ten of the 17 organizations give definitions for the concept Separation. In some of these cases the terms Physical Separation, Geographical Separation, Separation of Subsystems, Separation Principle or Segregation were used. Most definitions of Separation deal with physical separation.

The ASN uses two terms, Physical Separation and Geographical Separation to encompass the concept of separation. Physical Separation is limited to separation by barriers. Geographical Separation is separation by distance. This has the potential for creating confusion if other organizations are unaware of how French terminology differs from that of other countries.

The IAEA gives the most general definition. AERB, NSSC, IEEE, SSM, FANR, TEK, and ONR use some form of the IAEA definition.

ONR uses the term Segregation instead of Physical Separation. The term Segregation may be a more precise use of the English language, but the deviation from the more common term may cause confusion. ONR also has two different definitions of Separation. The two definitions seem to have the same meaning, but are worded differently.

The term Separation Distance does not deal with the overall concept of separation. It further defines conditions that must be met to credit separation by distance.

2.2.5 Redundancy

Thirteen of the 17 organizations give definitions for the term Redundancy. In some of these cases the terms Redundant Equipment or System, Engineering Redundancy, or Redundancy Principle are used. The IAEA definition is the most general and it does not suffer from

restrictions that unnecessarily limit the concept.

Eight organizations (STUK, ASN, NSSC, IEEE, IEC, FANR, ONR, and NRC) give definitions that are consistent with the IAEA definition, but no single definition encompasses all of the definitions given by the various organizations.

Four organizations (STUK, NSSC, IEEE, and ONR) give more than one definition and these definitions are not always fully consistent with each other. In some cases these may be attempts to describe specific means of accomplishing redundancy, but the usefulness in having these various definitions is not clear.

ONR uses both the term Redundancy and Engineering Redundancy. The meanings of both appear to be the same, but the wording of the definitions is different.

SSM limits the use of the term to safety systems.

AERB and NRA definitions exclude the possibility that redundant systems may also be diverse.

The ASN and one of the NSSC definitions do not discuss the use of redundancy to address unavailability of systems and equipment for reasons other than failure.

RTN extends the concept of Redundancy from just systems to functions and information as well.

The term Standby Redundancy does not deal with the overall concept of redundancy but describes one specific form of redundancy that might be used.

2.2.6 Reliability

Reliability was expanded to include the terms Availability and Dependability.

Six of the 17 organizations give definitions for Reliability. The main differences between the definitions are that some describe Reliability as a characteristic of an item, *e.g.*, a system, structure, component, or even humans. Others define Reliability in terms of the statistical measurement of reliability.

The definition given in IEEE Std 577 describes both interpretations, thus it seems to be the most complete and it encompasses all other definitions. The other definitions are similar but focus on Reliability as a probability.

IEEE NPEC gives definitions for three special cases, Reliability Targets System Reliability, and Operational Reliability. It is reported that these definitions are also used by NSSC. It is reported that NSSC also uses a second definition of Operational Reliability taken from IEEE Computer Society standards. This standard is not included in the IEEE nuclear power standards.

2.2.7 Availability

Six of the 17 organizations give definitions for the term Availability. As with Reliability, the main differences between the definitions have to do with whether the term represents the characteristic of an item, a probability, or both. The inconsistency in application found for the term Reliability applies here also.

Again, the IEEE Std 577 definition describes both interpretations, thus it seems to be the most complete and it encompasses all other definitions.

IEC gives an additional definition that is specific to cyber security systems.

The IEEE Nuclear Power Engineering Committee defines one specific type of availability, Operational Availability. It is reported that this definition is also used by NSSC.

2.2.8 Dependability

Only the IAEA gives a definition for Dependability. As this is a little used term, further consideration of the term seems unnecessary.

2.2.9 Spurious Activation

Only NSSC gives a definition that relates to the concept Spurious Activation and uses the term Spurious Initiation. Its definition is specific to the domain of computer security and is out of the scope of this report.

2.2.10 Independence

Independence was added to the original list of concepts because several of the concepts in the safety classification report deal with various aspects of Independence.

Nine of the 17 organizations give definitions for Independence. In some of these cases the terms Independent Equipment, or Independence Principle is used.

Several organizations define the term Independence in ways that address only some of the possible types of dependencies between systems and components. These definitions may represent gaps in their regulations, but such gaps might be compensated for by other terms or requirements that are not considered in this study.

The IAEA definition is most complete and covers all aspects of independence between systems and components. IEC uses the same definition and the ASN uses a similar definition to the IAEA.

STUK, AERB, FANR, NRA, RTN, and CNSC give definitions that do not address dependencies that may result from widespread hazards such as natural phenomena or support system failures.

The RTN and CNSC definitions also do not deal with dependencies that may result from local hazards. One CNSC definition does not deal with dependencies that might result from shared information.

Three special cases were also identified: Functional Isolation used by IAEA and FANR, Functional Separation used by SSM, and Isolation Device used by NSSC and IEEE.

A fourth special case, Communications Independence, was expected as the term is in common use within the I&C community, but no formal definition was found.

2.3 Recommendations

1. It is clear that different organizations use different terms and definitions for the concepts considered in this report. It is unlikely that this situation is only confined to the small set of concepts studied here. Therefore, any organization starting work under a new regulatory regime should gain a clear understanding of the terms used to describe important concepts and of how these terms are used in regulation. Although it is helpful to understand the terminology used by the various organizations, this does not eliminate the need to fully understand the regulatory requirements and how these requirements should be implemented in the countries in which they apply.

2. CORDEL should encourage the various organizations to harmonize terminology where possible. The IAEA terminology studied here is generally of high quality; this indicates that an effective means for defining concepts and definitions would be for organizations to work together within the IAEA framework.

3. IAEA safety terminology is provided in the IAEA Safety Glossary. One drawback of the Safety Glossary is that it is infrequently updated. The document would be much more useful as a continuously updated "living document" with the express goal of providing a consistent set of terminology that would be adopted by nuclear regulators worldwide. It is recommended that CORDEL together with nuclear regulators encourage IAEA to develop such a living safety glossary. To this effect contact should be made through the members of the Nuclear Safety Standards Committee (NUSSC). NUSSC has the charter to provide IAEA with advice on enhancing their usefulness of safety standards.

4. IAEA's Nuclear Knowledge Management section already has a project underway to apply semantic technologies to help identify and resolve inconsistencies in terms and definitions used within the nuclear community. CORDEL, perhaps together with nuclear regulators should encourage IAEA to put this system into operation.

5. Often terms and definitions have an important interaction with regulatory requirements thus it should be recognized that it may be difficult for some countries to change their terminology without also changing some wording of regulatory documents. Such changes take time and even after common terminology are accepted; it could take even longer to implement the changes in all of the affected documents.

6. This study has revealed some inconsistencies within organizations. These organizations should consider harmonizing definitions internally.

   The standards development organizations have already made progress in this area. The IAEA controls its terminology as a part of the editorial review process for safety standards.

   About 15 years ago IEC SC45A began harmonizing terminology in its standards. It took about 10 years for the harmonized definitions to propagate to all existing standards. SC45A reviews all terms every 15 to 18 months. One major decision at the outset of this work was to harmonize SC45A terms with those of the IAEA. The IEEE Nuclear Power Engineering Committee is now endeavouring to harmonize its terminology. The process used by SC45A could be used as a source of methods and lessons learned.

7. For seven of the 11 final concepts considered in this report there is one definition that seems to be the most useful. These definitions are:

   - Defence-in-Depth (IAEA): "A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions."

     This definition is equally valid whether or not an organization embraces the defence-in-depth model given in INSAG-10.

   - Diversity (IAEA): "The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different

attributes so as to reduce the possibility of common cause failure, including common mode failure."

- Independent Equipment (IAEA): "Equipment that possesses both of the following characteristics: (a) The ability to perform its required function is unaffected by the operation or failure of other equipment; (b) The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function."

  This preferred definition seems to encompass all of the other definitions.

  It may be useful to expand the IAEA definition to include other forms of independence other than independence of equipment, such as, independence between systems, communications independence, and organizational independence, for example.

- Redundancy (IAEA): "Provision of alternative (identical or diverse) SSC, so that anyone can perform the required function regardless of the state of operation or failure of the other."

  Most organizations give definitions similar to the IAEA's. Others give definitions that contain unnecessary restrictions, which might conflict with the definitions given by some organizations.

- Availability (IEEE Std 577): "The characteristic of an item expressed by the probability that it will be operational at a randomly selected future instant in time."

- Reliability (IEEE Std 577): "The characteristic of an item expressed by the probability that it will perform a required function under stated conditions for a stated time." This definition has the advantage of noting that Reliability is a characteristic of an item and that Probability is simply a means to measure the characteristic.

- Physical Separation (IAEA): "Separation by geometry (distance, orientation, *etc.*) by appropriate barriers, or by a combination thereof."

The other four concepts, Defence-in-Depth and Diversity, Dependability, Spurious Activation and Spurious Initiation, were not defined, not defined in a way appropriate for the scope of this report or defined by only one organization. Definitions for Defence-in-Depth and Diversity and for Dependability could help resolve some of the issues identified in the World Nuclear Association report, *Defence-in-Depth and Diversity: Challenges Related to I&C Architecture*, which outline the challenges in defining "defence-in-depth" and "diversity" as well as recommendations for potential solutions. [5] It may be worthwhile for the industry to develop a common term and a common definition for the concept of Spurious Activation.

Appendix A Terms and Definitions Given by Each Organization

A.1 Canada – Canadian Nuclear Safety Commission (CNSC)

The following CNSC documents were considered:

- Nuclear Energy Act [6].
- General Nuclear Safety Regulations (SOR/2000-202) [7].
- Design of Reactor Facilities: Nuclear Power Plants (REGDOC-2.5.2) [8].
- Design of New Nuclear Power Plants (RD-337) [9].

CNSC also makes use of certain nuclear specific Canadian Standards Association documents. These were not immediately available for the development of this report.

The following definitions were found.

Table 4. CNSC definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Diversity	REGDOC 2.5.2	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common-cause failure.
Reliability	Availability	REGDOC 2.5.2	The fraction of time that a component or system is able to function. "Availability" can also mean the probability that a component or system will be able to function at any given time.
Independence	Independent Systems	REGDOC 2.5.2	Systems that are each capable of performing a required function while remaining unaffected by the operation or failure of the other system.
Independence	Independent Systems	RD-337	Systems that do not share any components.

A.2 China – National Nuclear Safety Administration (NNSA)

No English language material was found giving definitions used by NNSA. Chinese colleagues indicated that in considering any given design, NNSA adopts the terminology used by the regulators from the country of the plant's origin.

A.3 Finland – Radiation and Nuclear Safety Authority (STUK)

The following STUK documents were considered:

- Government Degree [sic] on the Safety of Nuclear Power Plants (717/2013) [10]
- Regulatory Oversight of Safety in the Use of Nuclear Energy (YVL A.1) [11].
- Safety Design of a Nuclear Power Plant (YVL B.1) [12].
- Electrical and I&C Equipment of a Nuclear Facility (YVL E.7) [13].

The following definitions were found.

Table 5. STUK definitions of terms

Concept	Additional Term	Source Document	Definition
Defence-in-Depth and Diversity	Diversity principle	Decree 717/2013	Ensuring of functions through systems or components having different operating principles or differing from each other in some other manner, with all systems or components able to implement a function separately
Independence	Functional Isolation	Decree 717/2013	The isolation of systems from one another so that the operation or failure of one system does not adversely affect another system; functional isolation also covers electrical isolation and isolation of the processing of information between systems
Independence	Separation Principle	Decree 717/2013	Physical separation and functional isolation
Separation	Physical Separation	Decree 717/2013	The separation of systems or components from one another by means of adequate barriers, distance or placement, or combinations thereof
Redundancy	Redundancy principle	Decree 717/2013	The use of several parallel subsystems, so that the system can perform the required function even though individual subsystems are out of operation e.g. due to maintenance or failures
Redundancy	Redundancy	YVL B.1	The use of alternative (identical or diverse) structures, systems or system components, so that any one of them can perform the required function regardless of the state of operation or failure of any other.

A.4 France – Nuclear Safety Authority (ASN)

The Decision 2006-001 of 20 November 2006 of the Nuclear Safety Authority establishing the Nuclear Safety Authority's rules of procedure was examined but it contained no definitions for the key concepts and terms. French participants located and translated into English definitions from the following documents:

- Nuclear Facilities Order (2012) [14].
- EPR Safety Report (Flamanville 3) [15].

It is also often stated that the French industry uses IEC definitions, which are harmonized with the IAEA terminology. It appears that this approach is not consistently applied by the regulatory organization as the definitions found in their documents are different from the IEC definitions. Nevertheless the basic ideas are similar.

The following definitions were found.

Table 6: ASN definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Defence-in-depth	Nuclear Facilities Order	The operator applies the Defence-in-depth principle, consisting in the implementation of successive, and sufficiently independent, levels of defence, aiming, as far as operation is concerned, at: • Preventing anticipated operational occurrences (AOOs). • Detecting AOOs and implementing those actions allowing, firstly, to prevent them from leading to an accident, and, secondly, to come back to normal operation, or, at least, to reach and maintain a safe state. • Controlling the accidents, should they occur, or, at least, limiting their degradation, by having the situation under control, in order to reach and maintain a safe state. • Managing the accident conditions which have not been controlled, in order to limit the consequences, in particular for the people and the environment. Note: IAEA defines AOO (anticipated operational occurrence) as an operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.
Defence-in-Depth and Diversity	Diversity	EPR Safety Report	The existence of redundant components or systems performing a given function, with those components or systems considered as a whole, having one or several characteristics which differ from one to another.
Separation	Geographical Separation	EPR Safety Report	The geographical separation of equipment consists in arranging them at a sufficient distance or in orientating them in sufficiently different manners, in order to prevent their simultaneous failure in case of hazard or initiating event. The sufficient distance depends on the considered hazard or initiating event.
Separation	Physical Separation	EPR Safety Report	The physical separation of two pieces of equipment consists in separating them with an appropriate barrier (*e.g.* a wall).
Redundancy	Redundancy	EPR Safety Report	The implementation of a number of systems or equipment (identical or different) which is higher than the necessary number, so that the failure of one of them does not lead to the loss of the function that they perform.
Independence	Independence	EPR Safety Report	A system or equipment is said independent if it respects both following conditions: • Its capacity to perform its function is not affected by the operation or the failure of other systems or equipment. • Its capacity to perform its function is not affected by the consequences of the initiating event for which its operation is required.

A.5 India – Atomic Energy Regulatory Board (AERB)

The following AERB documents were considered:

- Design of Light Water Reactor Based Nuclear Power Plants (AERB/NPP-LWr/SC/D) [16].
- Computer Based Systems of Pressurized Heavy Water Reactors (AERB/NPP-PHWR/SG/D-25) [17].
- Design of Pressurized Heavy Water Reactor Based Nuclear Power Plants (AERB/NPP-PHWR/SC/D-1) [18].
- Safety Classification and Seismic Categorization for Structures Systems and Components of Pressurized Heavy Water Reactors (AERB/NPP-PHWR/SG/D-1) [19].
- Safety Related Instrumentation and Control for Pressurised Heavy Water Based Nuclear Power Plants (AERB/NPP-PHWR/SG/D-20 [20].

The following definitions were found.

Table 7. AERB definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Defence-in-Depth	SC-D1	Provision of multiple levels of protection for ensuring safety of workers, the public, or the environment.
Defence-in-Depth and Diversity	Diversity	SG/D-25	The presence of two or more different components or systems to perform an identified function, where the different components or systems have different attributes, so as to reduce the possibility of common cause failure.
Separation	Physical Separation	SC-D1	A means of ensuring independence of equipment by separation by geometry (distance, orientation, *etc.*), appropriate barriers or combination of both.
Redundancy	Redundancy	SC-D1	Provision of alternative structures, systems, components of identical attributes, so that anyone can perform the required function, regardless of the state of operation or failure of the other.
Reliability	Availability	SG/D-20	The fraction of time that an entity is capable of performing its intended purpose.
Reliability	Reliability	SC-D1	The probability that a structure, system, component or facility will perform its intended (specified) function satisfactorily for a specified period under specified conditions.
Independence	Independence	SC-D1	The ability of equipment, channel or system to perform its function irrespective of the normal or abnormal functioning of any other equipment, channel or system. Independence is achieved by functional isolation and physical separation.
Independence	Functional Isolation	SC-D-20	Prevention of influences from the mode of operation or failure of one circuit or system on another.

A.6 Institute for Electrical and Electronic Engineers (IEEE)

The IEEE Dictionary – IEEE Std 100 – contains all the definitions given in the IEEE standards. The definitions considered were from the following standards produced by the IEEE Nuclear Power Engineering Committee (NPEC).

- IEEE Std 338-2012 [21].
- ANSI/IEEE Std 352-1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems [22].
- IEEE Std 384-2008, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits [23].
- IEEE Std 577-2012, IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations [24].
- IEEE Std 603-2009, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations [25].
- ANSI/IEEE Std 622-1987, IEEE Recommended Practice for the Design and Installation of Electric Heat Tracing Systems for Nuclear Power Generating Stations [26].
- IEEE Std 690-1984-2004, IEEE Standard for the Design and Installation of Cable Systems for Class 1E Circuits in Nuclear Power Generating Stations [27].
- IEEE Std 933-1999, IEEE Guide for the Definition of Reliability Program Plans for Nuclear Power Generating Stations [28].

The following definitions were found.

Table 8. IEEE definitions of terms

Concept	Associated Term	Source Document	Definition
Independence	Independence	IEEE Std 308, IEEE Std 384	The state in which there is no mechanism by which any single design basis event, such as a flood, can cause redundant equipment to be inoperable.
Independence	Isolation Device	IEEE Std 384	A device in a circuit that prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits.
Redundancy	Redundant Equipment or System	IEEE Std 603	A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function regardless of the state of operation or failure of the other. Note: Duplication of essential functions can be accomplished by the use of identical equipment, equipment diversity, or functional diversity.
Redundancy	Redundant, Redundancy	IEEE Std 622	The introduction of auxiliary elements and components to a system to perform the same function as other elements in the system for the purpose of improving reliability. Redundant electric heat tracing systems consist of two heaters and two controllers, each with its own sensor, supplied from two power systems and two alarms, each system independent of the other but all applied to the same mechanical piping, valves, tanks, *etc.* Redundant electric heat tracing systems are referred to as primary and backup in this recommended practice.
Reliability	Availability	IEEE Std 577	The characteristic of an item expressed by the probability that it will be operational at a randomly selected future instant in time.

Concept	Associated Term	Source Document	Definition
Reliability	Availability	IEEE Std 352	The probability that an item or system will be operational on demand. 1) Steady-state availability is the expected fraction of the time in the long run that an item (or system) operates satisfactorily. 2) Transient availability (or instantaneous availability) is the probability that an item (or system) will be operational at a given instant in time. For repairable items, this will converge to steady-state availability in the long term.
Reliability	Operational Availability	IEEE Std 338	The measured characteristic of an item expressed by the probability that it will be operable when needed as determined by periodic test and resultant analysis
Reliability	Reliability Targets	IEEE Std 933	The reliability goals to be achieved by the plant systems.
Reliability	Reliability	IEEE Std 577	The characteristic of an item expressed by the probability that it will perform a required function under stated conditions for a stated time.
Reliability	Operational Reliability	IEEE Std 933-1999	The assessed reliability of an item based on operational data.
Reliability	System Reliability	IEEE Std 577	The probability that a system, including all hardware and software subsystems, will perform a required task or mission for a specified time in a specified environment.
Separation	Separation	IEEE Std 690	Physical independence of redundant circuits, components, and equipment. (Physical independence may be achieved by space, barriers, shields, *etc.*)
Separation	Separation Distance	IEEE Std 384	Space that has no interposing structures, equipment, or materials that could aid in the propagation of fire or that could otherwise disable Class 1E systems or equipment.

Note: NSSC also uses definitions from IEEE Computer Society Standard IEEE Std 729. These are not included here because they are not developed by the IEEE Nuclear Power Engineering Committee (NPEC).

A.7 International Atomic Energy Agency (IAEA)

The 2007 IAEA Safety Glossary [29] gives definitions of terms that should be used consistently across all IAEA safety standards. Where a term of interest was not given in the Safety Glossary, associated terms from the glossary of *Design of Instrumentation and Control Systems for Nuclear Power Plants*, IAEA SSG-39 [30], were also considered. Definitions from SSG-39 were also included if they differed from those in the Safety Glossary.

As this edition of the report was going to print the 2018 IAEA Safety Glossary became available. The 2018 Glossary made a number of small changes to the IAEA terms and definitions of in the 2007 version. The differences between the 2007 terms used in this report and the terms given in the 2018 version were examined and it was concluded that updating the report to include the current IAEA terminology would not substantively change the conclusions of this report.

The following definitions were found.

Table 9. IAEA definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Defence-in-Depth	Safety Glossary	A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions. The objectives of defence-in-depth are: (a) To compensate for potential human and component failures; (b) To maintain the effectiveness of the barriers by averting damage to the facility and to the barriers themselves; (c) To protect workers, members of the public and the environment from harm in accident conditions in the event that these barriers are not fully effective. INSAG defines five levels of in depth: (a) Level 1: Prevention of abnormal operation and failures. (b) Level 2: Control of abnormal operation and detection of failures. (c) Level 3: Control of accidents within the design basis. (d) Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents. (e) Level 5: Mitigation of radiological consequences of significant releases of radioactive material.
Defence-in-Depth and Diversity	Defence-in-Depth	Safety Glossary	The application of more than one protective measure for a given safety objective, such that the objective is achieved even if one of the protective measures fails.
Defence-in-Depth and Diversity	Diversity	Safety Glossary	The presence of two or more redundant *systems* or *components* to perform an identified function, where the different *systems* or *components* have different attributes so as to reduce the possibility of *common cause failure*, including *common mode failure*.
Defence-in-Depth and Diversity	Diversity	SSG-39	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure. Note 1: When the term 'Diversity' is used with an additional attribute, the term diversity indicates the general meaning "existence of two or more different ways or means of achieving a specified objective", where while the attribute indicates the characteristics of the different ways applied, *e.g.* functional diversity, equipment diversity, signal diversity. Note 2: See also the entry for Functional Diversity in the IAEA Safety Glossary.
Defence-in-Depth and Diversity	Functional Diversity	Safety Glossary	Examples of such attributes are: different operating conditions, different working principles or different design teams (which provide functional diversity).
Defence-in-Depth and Diversity	Physical Diversity	Safety Glossary	Examples of such attributes are: different sizes of equipment, different manufacturers, and types of equipment that use different physical methods (which provide physical diversity).

Concept	Associated Term	Source Document	Definition
Separation	Physical Separation	Safety Glossary	Separation by geometry (distance, orientation, *etc.*) by appropriate barriers, or by a combination thereof.
Redundancy	Redundancy	Safety Glossary	Provision of alternative (identical or diverse) SSC, so that anyone can perform the required function regardless of the state of operation or failure of the other.
Reliability	Availability	Safety Glossary	The fraction of time for which a system is capable of fulfilling its intended purpose.
Reliability	Availability	SSG-39	The ability of an item 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, with the assumption that the necessary external resources are provided.
Reliability	Dependability	Safety Glossary	A general term describing the overall trustworthiness of a system, *i.e.* the extent to which reliance can be justifiably placed on this system. Reliability, Availability, and Safety are attributes of dependability.
Reliability	Reliability	Safety Glossary	The probability that a system or component will meet its minimum performance requirements when called upon to do so.
Independence	Functional Isolation	Safety Glossary	Prevention of influences from the mode of operation or failure of one circuit or system on another.
Independence	Independent Equipment	Safety Glossary	Equipment that possesses both of the following characteristics: (a) The ability to perform its required function is unaffected by the operation or failure of other equipment; (b) The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function.

A.8 International Electrotechnical Commission (IEC)

Definitions were taken from the IEC glossary [31], which lists the definitions given in every IEC standard. Only definitions given in the standards of IEC Subcommittee 45A (IEC SC45A), Instrumentation, Control and Electrical Systems of Nuclear Facilities, were considered. IEC SC45A has ensured any defined term has the same definition in any standard that includes the term in its definitions section. Also, there is a stated policy to use the definitions of the IAEA Safety Glossary wherever possible.

The following definitions were found.

Table 10. IEC definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Diversity	IEC Glossary	Presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure. Note 1: When Diversity is used with an additional attribute, the term Diversity indicates the general meaning 'existence of two or more different ways or means of achieving a specified objective', where the attribute indicates the characteristics of the different ways applied, *e.g.* functional diversity, equipment diversity, signal diversity. Note 2: See also Functional Diversity.
Defence-in-Depth and Diversity	Functional Diversity	IEC Glossary	Application of diversity at the level of process engineering application functions (for example, to have trip activation on both pressure and temperature limit). Note: IAEA Safety Glossary, edition 2007, does not give a definition for functional diversity but gives examples of means to achieve it. This IEC SC45A definition is compatible with the means indicated in the IAEA safety glossary to achieve functional diversity.
Redundancy	Redundancy	IEC Glossary	Provision of alternative (identical or diverse) SSC, so that any one can perform the required function regardless of the state of operation or failure of the other.
Reliability	Availability	IEC Glossary	The property of being accessible and usable upon demand by an authorized entity. Note 1 to entry: This definition is different from the one used in the other IEC standards in the field of instrumentation and control of nuclear facilities which is 'ability of an item 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, assuming that the required external resources are provided'. [Source: IAEA Nuclear Security Series No. 17:2011]
Reliability	Availability	SSG-39	The ability of an item 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, with the assumption that the necessary external resources are provided.
Reliability	Reliability	IEC Glossary	Probability that a device, system or facility will meet its minimum performance requirements when called upon to do so for a specified time under stated operating conditions Note 1: The reliability of a computer-based system includes the reliability of its hardware which is usually quantified and the reliability of its software which is usually a qualitative measure because there are no generally recognised means to quantify the reliability of software. Note 2: This definition differs from 2007 edition of the IAEA Safety Glossary one which is "The probability that a system or component will meet its minimum performance requirements when called upon to do so." IEC SC45A experts indicated that this IAEA definition is not consistent with general practice in that it does not include the idea of mission time.

Concept	Associated Term	Source Document	Definition
Independence	Independent Equipment	IEC Glossary	An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public. Items important to safety include: a) Those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public. b) Those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions c) Those features which are provided to mitigate the consequences of malfunction or failure of structures, systems or components.

A.9 Japan – Nuclear Regulatory Authority (NRA)

The *Outline of New Regulatory Requirements (Design Basis)* [32] was examined. The status of this document is unknown. There may be other applicable documents, but we would need a Japanese participant to find and interpret any such documents.

The following definitions were found.

Table 11. NRA definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Diversity	Outline of New Requirements	The existence of two or more systems or components with different attributes to perform an identical function. In this case, "different attributes" means that the operating principle and others are different, so that the functions will not be impaired simultaneously due to common or subordinate causes. Furthermore, 'common cause' refers to a cause that simultaneously affects two or more systems or components; such as influential factors induced by environmental temperature, humidity, pressure, radiation, *etc.* or those induced by electric power, air, oil, cooling water, *etc.* supplied to systems and components, or influences caused by earthquake, flooding and fires, *etc.*
Redundancy	Redundancy	Outline of New Requirements	The existence of two or more systems or components with identical attributes to perform an identical function.
Independence	Independence	Outline of New Requirements	Two or more systems or components are free from simultaneous functional impediment due to common or subordinate causes under environmental or operational conditions considered in design.

A.10 Republic of Korea – Nuclear Safety and Security Commission (NSSC)

No relevant English language documents were located. A set of definitions was obtained from the staff of their Technical Support Organization (TSO), the Korean Institute of Nuclear Safety (KINS). This list should be reviewed with members of the Korean industry to confirm that the definitions given are relevant to the purpose of this report.

- IEEE Std 338-2012, IEEE Standard for Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems [21].
- IEEE Std 384-2008, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits [23].
- ANSI/IEEE Std 352-1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems [22].
- IEEE Std 577-2012, IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations [24].
- IEEE Std 690-1984-2004, IEEE Standard for the Design and Installation of Cable Systems for Class 1E Circuits in Nuclear Power Generating Stations [27].
- IEEE Std 729- 1983, IEEE Standard Glossary of Software Engineering Terminology [33].
- IEEE Std 933-1999, IEEE Guide for the Definition of Reliability Program Plans for Nuclear Power Generating Stations [28].

Table 12. NSSC definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Defence-in-Depth	US NRC Glossary	An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defence to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defence-in-Depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.
Defence-in-Depth and Diversity	Functional Diversity	NUREG-CR-6303	Two systems are functionally diverse if they perform different physical functions through they may have overlapping safety effects.
Defence-in-Depth and Diversity	Signal Diversity	NUREG-CR-6303	The use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly.
Defence-in-Depth and Diversity	Diverse Protection System (DPS)		The DPS is a part of Diverse Instrumentation and Control Systems and provides a diverse method to trip the reactor to satisfy concerns relative to Anticipated Transient Without Scram (ATWS) as well as Defence-in-Depth and Diversity issues. The DPS is designed to comply with the requirements of 10 CFR 50.62 to reduce the risk of ATWS.
Defence-in-Depth and Diversity	Diverse Indication Systems (DIS)		The DIS a part of diverse instrumentation and control systems and provides indications to satisfy the NRC Defence-in-Depth and Diversity Position 4 requirements. This system receives isolated safety inputs from Channel A only and provides a flat panel display on the Safety Console. This display is neither a safety platform nor a DCS based system.
Defence-in-Depth and Diversity	Diverse Manual ESF Actuation Switches (DMAS)		The DMAS a part of Diverse Instrumentation and Control Systems and provides input signals by the operator to actuate various ESF equipment in conformance with the NRC Defence-in-Depth and Diversity Position 4 requirements. The DMAS is wired to control panel multiplexers located in the Safety Console.

Concept	Associated Term	Source Document	Definition
Separation	Separation	IEEE Std 690-1984	Physical independence of redundant circuits, components, and equipment. (Physical independence may be achieved by space, barriers, shields, *etc.*)
Separation	Separation Distance	IEEE Std 384-1992	Space that has no interposing structures, equipment, or materials that could aid in the propagation of fire or that could otherwise disable Class 1E systems or equipment.
Independence	Independence	IEEE Std 384-1992	The state in which there is no mechanism by which any single design basis event, such as a flood, can cause redundant equipment to be inoperable.
Redundancy	Redundancy		Duplication of essential function can be accomplished by the use of identical equipment, equipment diversity, or functional diversity. Redundancy can be accomplished by use of identical equipment, equipment diversity, or functional diversity. Synonym: redundant system.
Redundancy	Redundant Equipment or System	IEEE Std 384-1992	Equipment or system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function regardless of the state of operation or failure of the other.
Redundancy	Standby Redundancy		(Software) In fault tolerance, the use of redundant elements that are left inoperative until a failure occurs in a primary element. Contrast: active redundancy. (IEEE Std 610.12-1990) That redundancy wherein the alternative means for performing a given function are inoperative until needed.
Reliability	Reliability	IEEE Std 352-1987	The characteristic of an item or system expressed by the probability that it will perform a required mission under stated conditions for a stated mission time.
Reliability	Reliability Targets	IEEE Std 933-1999	The reliability goals to be achieved by the plant systems.
Reliability	Availability	IEEE Std 933-1999	The characteristic of an item expressed by the probability that it will be operational at a randomly selected future instant in time.
Reliability	Operational Availability	IEEE Std 338-2006	The measured or observed characteristic of an item expressed by the probability that it will be operable when needed as determined by periodic test and resultant analysis.
Reliability	Operational Reliability	IEEE Std 729-1983	(software) The reliability of a system or software subsystem in its actual use environment. Operational reliability may differ considerably from reliability in the specified or test environment. See also: System; Reliability.
Reliability	Operational Reliability	IEEE Std 933-1999	The assessed reliability of an item based on operational data.
Reliability	System Reliability	IEEE Std 729-1983	The probability that a system, including all hardware and software subsystems, will perform a required task or mission for a specified time in a specified environment.
Independence	Isolation Device	IEEE Std 384-1992	A device in a circuit that prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits
Spurious Activation	Spurious Initiation		Attempts to establish a communication connection or association, using a false identity or through the replay of a previous, legitimate initiation sequence. Spurious initiation includes spoofing or masquerading attempts in the communication system, and coupled with other attacks, could result in unauthorized disclosure or modification of information, unauthorized receipt of services, or denial of service to legitimate users or critical functions.

A.11 Russian Federation – Rostechnadzor (RTN)

The following documents were considered:

- Law on Use of Atomic Energy (170-FZ) [34].
- General Regulations on Ensuring Safety of Nuclear Power Plants (OPB-88/97) [35].
- Nuclear Safety rules for Reactor Installations of Nuclear Power Plants (NP-082-07) [36].

The following definitions were found.

Table 13. RTN definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Diversity principle	NP-082-2007	The principle of reliability improvement through application in different systems (or within one system in different channels) of different means and/or similar means based on diverse functional principles.
Redundancy	Redundancy Principle	NP-082-2007	The principle of the system reliability improvement through application of structural, functional and information redundancy in the scope that is maximum necessary and sufficient for the systems to perform the designated functions.
Independence	Independence Principle	NP-082-2007	Principle of the system reliability improvement through application of functional and/or physical separation of trains (elements) where, if implemented, a failure of one train (element) does not lead to a failure of another train (element).
Independence	Independent Systems (elements)	OPB-88/97	Systems (elements) for which failure of one system (element) does not lead to failure of another system (element)

A.12 Republic of South Africa – National Nuclear Regulator (NNR)

The following documents were considered:

- Basic Licensing Requirements for the Pebble Bed Modular Reactor (RD-0018) [37].
- Guidance for Licensing Submissions Involving Computer Software and Evaluation Models for Safety Calculations (LG-1045) [38].
- Licensing Guide on Safety Assessments of Nuclear Power Reactors (LG-1041) [39].
- Design and Implementation of Digital Instrumentation and Control for Nuclear Installations (PP-0017) [40].

The following definitions were found.

Table 14. NNR definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Defence-in-depth	LG-1041	The principle of defence-in-depth, as applied to all safety activities, where organizational behavioural or design related, ensures that they are subject to overlapping provisions, so that if a failure were to occur it would be detected and compensated for or corrected by appropriate measures. Application of this principle throughout design and operation provides a graded protection against a wide variety of transients, anticipated operational occurrences, and accidents, including those resulting from equipment failure or human actions within the plants, and events that originate outside of the plant.
Defence-in-Depth and Diversity	Defence-in-depth	LG-1045	…a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between a radiation source or radioactive materials and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

A.13 Sweden – Swedish Radiation Safety Authority (SSM)

The following documents were considered:

- The Swedish Radiation Safety Authority's Regulations and General Advice Concerning the Design and Construction of Nuclear Power Reactors .
- (SSMFS 2008:17) [41].
- Swedish Radiation Safety Authority Regulatory Code (SSMFS 2008:1) [42].

The following definitions were found.

Table 15. SSM definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Defence-in-Depth	SSMFS-2008-1	Application of several, overlapping levels of technical equipment, operational measures and administrative procedures to protect the facility's barriers and to maintain their effectiveness as well as to protect the surroundings if the barriers should not function as intended.
Defence-in-Depth and Diversity	Diversification	SSMFS-2008-17	Two or more alternative systems or components that independently of each other perform the same safety task, but in essentially different ways or by having different characteristics.
Independence	Functional Separation	SSMFS-2008-17	Systems or components that do not affect each other's function unintentionally.
Separation	Physical Separation	SSMFS-2008-17	Systems or components that are physically separated through distance or barriers or a combination of these
Redundancy	Redundancy	SSMFS-2008-17	Two or more alternative identical or different systems or components that independently of each other perform the same safety task

A.14 Turkey – Turkish Atomic Energy Authority (TAEK)

The following documents were considered:

- Guide on Specific Design Principles [43]
- Regulation on Design Principles for Safety of Nuclear Power Plants [44]
- Regulation on Specific Principles for Safety of Nuclear Power Plants [45]

The following definitions were found.

Table 16. TAEK search terms definitions

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Diversity	Design Principles	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure.
Separation	Physical Separation	Design Principles	Separation by geometry (distance, orientation, *etc.*), by appropriate barriers, or by a combination thereof.

A.15 United Arab Emirates – Federal Authority for Nuclear Regulation (FANR)

The following documents were considered:

- Regulation for the Design of Nuclear Power Plants (FANR-REG-03) [46].
- Guidelines for the Design, Construction, and Operation of Nuclear Power Plants (FANR-RG-005) [47].

The following definitions were found.

Table 17. FANR definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Defence-in-Depth	FANR REG-03	A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.
Defence-in-Depth and Diversity	Diversity	FANR-REG-03	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure.
Separation	Functional Isolation	FANR-REG-03	Prevention of influences from the mode of operation or failure of one circuit or system on another.
Separation	Physical Separation	FANR-REG-03	Separation by geometry (distance, orientation, *etc.*), by appropriate barriers, or by a combination thereof.
Redundancy	Redundancy	FANR-REG-03	Provision of alternative (identical or diverse) SSCs, so that anyone can perform the required function regardless of the state of operation or failure of any other.

A.16 United Kingdom – Office of Nuclear Regulation (ONR)

The following documents were considered:

- Safety Assessment Principles for Nuclear Facilities [48].
- ONR Guide – Safety Related Instrumentation (NS-TAST-GD-031) [49].
- ONR Guide – Diversity, Redundancy, Segregation and Layout of Mechanical Plant (NS-TAST-GD-036) [50].
- ONR Guide – Computer Based Safety Systems (NS-TAST-GD-046) [51].
- ONR Guide – Design Safety Assurance (NS-TAST-GD-057) [52].

The following definitions were found.

Table 18. ONR definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Diversity	Safety Assessment Principles	The presence of two or more systems or components to perform an identified function, where the systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure (IAEA Safety Glossary).
Defence-in-Depth and Diversity	Diversity [Software]	TAST-GD-46	The introduction of diversity in any aspect of a system or its manufacture/production will reduce the likelihood of common mode failures. Systems can be considered as having varying degrees of diversity according to the number of these different aspects which have been achieved by dissimilar means. Diversity in software covers the computer instruction set but also the programming language, support software, design, and all staff involved in the life cycle.
Defence-in-Depth and Diversity	Engineering Diversity	TAST-GD-036	The provision of dissimilar means of achieving the same objective; *e.g.* the use of features which differ in the physical means of achieving a specific objective or use of different equipment made by different manufacturers.
Separation	Segregation	Safety Assessment Principles	The physical separation of structures, systems or components by distance or by some form of barrier that reduces the likelihood of common cause failures.
Separation	Segregation	TAST-GD-036	The separation of components by distance or physical barriers, a particular example being provision of principal fire barriers to delineate individual fire zones; such barriers may also serve as barriers to other hazards.
Redundancy	Engineering Redundancy	TAST-GD-036	The provision of more than the minimum number of nominally identical equipment items required to perform a specific safety function. Such redundant provisions allow a safety function to be satisfied when one or more items (but not all) are unavailable, due to a variety of unspecified potential failure mechanisms or maintenance (*e.g.* identified faults or hazards).
Redundancy	Redundancy	Safety Assessment Principles	Provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other (IAEA Safety Glossary).
Reliability	Reliability	Safety Assessment Principles	The probability that a system or component will meet its minimum performance requirements when called upon to do so (IAEA Safety Glossary).

A.17 United States – Nuclear Regulatory Commission (NRC)

The following documents were considered:

- Code of Federal Regulations: Domestic Licensing of Production and Utilization Facilities (10 CFR Part 50) [53].
- IEEE Std 603-2009 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations [25].
- USNRC Glossary (NRC Website) [54].
- Standard Review Plan for Light Water Cooled Nuclear Reactors, Rev. 7, Appendix 7-B (NUREG-0800) [55].

Within the NRC regulatory environment only the definitions given in the Code of Regulations have real weight. IEEE Std 603-1991 is incorporated by reference into the 10 CFR Part 50 so in the below table IEEE Std 603 definitions are associated with10 Part CFR 50.

The NRC Glossary seems to be targeted at members of the public more than the staff.

The following definitions were found.

Table 19. NRC definitions of terms

Concept	Associated Term	Source Document	Definition
Defence-in-Depth and Diversity	Defence-in-Depth	NRC Glossary	An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defence to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defence-in-Depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.
Defence-in-Depth and Diversity	Diverse Instrumentation and Control Systems	SRP Chapter 7 Rev. 7	Those systems provided expressly for diverse backup of the reactor trip system and engineered safety features actuation systems. Diverse I&C systems account for the possibility of common-mode failures in the protection systems. Diverse I&C systems include the anticipated transient without scram (ATWS) mitigation system as required by 10 CFR 50.62. For plants with digital computer-based instrumentation and controls, diverse I&C systems may also include hardwired manual controls, diverse displays, and any other systems specifically installed to meet the guidance of the Staff Requirements Memorandum on SECY-93-087, *Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs*.
Redundancy	Redundant Equipment or System	10 CFR Part 50 (IEEE Std 603)	A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function regardless of the state of operation or failure of the other. Note: Duplication of essential functions can be accomplished by the use of identical equipment, equipment diversity, or functional diversity.

Appendix B | Analysis of Terms Related to the Key Concepts

This Chapter considers the definitions associated with each original key concept, noting similarities, differences, and possible strategies for overcoming differences.

B.1 Defence-in-Depth and Diversity

No definition was located for the concept of Defence-in-Depth and Diversity, but the individual terms are defined.

B.1.1 Defence-in-Depth

Table on next page.

B.1.1 Defence-in-Depth

Terms	Source Document	Definition	Comments
Defence-in-Depth	IAEA Safety Glossary	A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.	These definitions are the same. They do not include statements about independence between levels but the do require diversity.
Defence-in-Depth	FANR REG-03	A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of Anticipated Operational Occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.	
Defence-in-Depth	NNR LG-1045	A hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between a radiation source or radioactive materials and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.	
Defence-in-Depth	SSM SSMFS-2008-1	Application of several, overlapping levels of technical equipment, operational measures and administrative procedures to protect the facility's barriers and to maintain their effectiveness as well as to protect the surroundings if the barriers should not function as intended.	These definitions do not require diversity of levels and they become progressively less detailed.
Defence-in-Depth	ASN Nuclear Facilities Order	The operator applies the Defence-in-depth principle, consisting in the implementation of successive, and sufficiently independent, levels of defence, aiming, as far as operation is concerned, at: • Preventing AOOs ; • Detecting AOOs and implementing those actions allowing, firstly, to, prevent them from leading to an accident, and, secondly, to come back to normal operation, or, at least, to reach and maintain a safe state. • Controlling the accidents, should they occur, or, at least, limiting their degradation, by having the situation under control, in order to reach and maintain a safe state. Managing the accident conditions which have not been controlled, in order to limit the consequences, in particular for the people and the environment.	
Defence-in-Depth	IAEA Safety Glossary	The application of more than one protective measure for a given safety objective, such that the objective is achieved even if one of the protective measures fails.	
Defence-in-Depth	AERB SC-D1	Provision of multiple levels of protection for ensuring safety of workers, the public, or the environment.	
Defence-in-Depth	NSSC NRC Glossary	An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defence to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defence-in-Depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.	These statements are more descriptions than definitions.
Defence-in-Depth	NRC Glossary	An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defence to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defence-in-Depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.	
Defence-in-Depth	NNR LG-1041	The principle of Defence-in-Depth, as applied to all safety activities, where organizational behavioural or design related, ensures that they are subject to overlapping provisions, so that if a failure were to occur it would be detected and compensated for or corrected by appropriate measures. Application of this principle throughout design and operation provides a graded protection against a wide variety of transients, anticipated operational occurrences, and accidents, including those resulting from equipment failure or human actions within the plants, and events that originate outside of the plant.	

The IAEA provides a definition that is sufficiently general to apply to organizations that adopt the defence-in-depth model of INSAG-10 and those that do not. IAEA lists describe the INSAG-10 approach as one model for implementing defence-in-depth. The ASN definition is the most consistent with the application of the Defence-in-Depth concept as it is described by IAEA SSR 2-1. The NRC and NRR definitions are more discussion than a description, but unlike the other definitions the NRR LG-1041 definition makes it very clear that the concept applies to all activities, not just plant design.

B.1.2 Diversity

Terms	Source Document	Definition	Comments
Diversity	IAEA Safety Glossary	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure.	These definitions are essentially the same. Some have more detail and explanation. Note that for definitions that are worded to specify redundancy the organization either includes diversity in the definition of redundancy or does not have a definition of redundancy. Hence, the term redundancy in these definitions do not appear to exclude the possibility that the diverse system may be of a different kind or may achieve the fundamental function in a different way.
Diversity	TAEK Design Principles	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure.	
Diversity	ONR Safety Assessment Principles	The presence of two or more systems or components to perform an identified function, where the systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure.	
Diversity	IAEA SSG-39	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure. Note 1: When the term Diversity is used with an additional attribute, the term diversity indicates the general meaning 'existence of two or more different ways or means of achieving a specified objective', where while the attribute indicates the characteristics of the different ways applied, *e.g.* functional diversity, equipment diversity, signal diversity. Note 2: See also the entry for Functional diversity in the IAEA Safety Glossary.	
Diversity	IEC TC45A IEC Glossary	Presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure. Note 1: When Diversity is used with an additional attribute, the term diversity indicates the general meaning 'existence of two or more different ways or means of achieving a specified objective', where the attribute indicates the characteristics of the different ways applied, *e.g.* functional diversity, equipment diversity, signal diversity. Note 2: See also Functional Diversity.	
Diversity principle	STUK Decree 717/2013	Ensuring of functions through systems or components having different operating principles or differing from each other in some other manner, with all systems or components able to implement a function separately.	
Diversity	ASN EPR Safety Report	The existence of redundant components or systems performing a given function, with those components or systems, considered as a whole, having one or several characteristics which differ from one to another.	
Diversity	AERB SG/D-25	The presence of two or more different components or systems to perform an identified function, where the different components or systems have different attributes, so as to reduce the possibility of common cause failure.	
Diversity	FANR FANR-REG-03	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure.	
Diversity	CNSC REGDOC 2.5.2	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure.	

Terms	Source Document	Definition	Comments
Diversity	NRA Outline of New Requirements	The existence of two or more systems or components with different attributes to perform an identical function. In this case, 'different attributes' means that the operating principle and others are different, so that the functions will not be impaired simultaneously due to common or subordinate causes. Furthermore, 'common cause' refers to a cause that simultaneously affects two or more systems or components; such as influential factors induced by environmental temperature, humidity, pressure, radiation, etc. or those induced by electric power, air, oil, cooling water, etc. supplied to systems and components, or influences caused by earthquake, flooding and fires, *etc*.	
Diversification	SSM SSMFS-2008-17	Two or more alternative systems or components that independently of each other perform the same safety task, but in essentially different ways or by having different characteristics.	
Diversity principle	RTN NP-082-2007	The principle of reliability improvement through application in different systems (or within one system in different channels) of different means and/or similar means based on diverse functional principles.	
The following definitions deal with specific types of Diversity			
Functional Diversity	IEC TC45A IEC Glossary	Application of diversity at the level of process engineering application functions (for example, to have trip activation on both pressure and temperature limit).	
Functional Diversity	IAEA Safety Glossary	Examples of such attributes are: different operating conditions, different working principles or different design teams (which provide functional diversity) .	Not a definition, but an example.
Functional Diversity	NSSC NUREG-CR-6303	Two systems are functionally diverse if they perform different physical functions through they may have overlapping safety effects.	
Engineering Diversity	ONR TAST-GD-036	The provision of dissimilar means of achieving the same objective; *e.g.* the use of features which differ in the physical means of achieving a specific objective or use of different equipment made by different manufacturers.	Similar to the IAEA example of Physical Diversity.
Diversity [Software]	ONR TAST-GD-46	The introduction of diversity in any aspect of a system or its manufacture/production will reduce the likelihood of common mode failures. Systems can be considered as having varying degrees of diversity according to the number of these different aspects which have been achieved by dissimilar means. Diversity in software covers the computer instruction set but also the programming language, support software, design, and all staff involved in the life cycle.	
Physical Diversity	IAEA Safety Glossary	Examples of such attributes are: different sizes of equipment, different manufacturers, and types of equipment that use different physical methods (which provide physical diversity).	Not a definition, but an example.
Signal Diversity	NSSC NUREG-CR-6303	The use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly.	
Diverse Instrumentation and Control Systems	NRC SRP Chapter 7 Rev. 4	Those systems provided expressly for diverse backup of the reactor trip system and engineered safety features actuation systems. Diverse I&C systems account for the possibility of common-mode failures in the protection systems. Diverse I&C systems include the anticipated transient without scram (ATWS) mitigation system as required by 10 CFR 50.62. For plants with digital computer-based instrumentation and controls, diverse I&C systems may also include hardwired manual controls, diverse displays, and any other systems specifically installed to meet the guidance of the Staff Requirements Memorandum on SECY-93-087, *Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs*.	Not a definition of Diversity but an application of Diversity.
Diverse Protection System (DPS)	NSSC	The DPS is a part of diverse instrumentation and control systems and provides a diverse method to trip the reactor to satisfy concerns relative to Anticipated Transient Without Scram (ATWS) as well as Defence-in-Depth and Diversity issues. The DPS is designed to comply with the requirements of 10 CFR 50.62 to reduce the risk of ATWS.	
Diverse Indication Systems (DIS)	NSSC	The DIS a part of diverse instrumentation and control systems and provides indications to satisfy the NRC Defence-in-Depth and Diversity Position 4 requirements. This system receives isolated safety inputs from Channel A only and provides a flat panel display on the Safety Console. This display is neither a safety platform nor a DCS based system.	
Diverse Manual ESF Actuation Switches (DMAS)	NSSC	The DMAS a part of diverse instrumentation and control systems and provides input signals by the operator to actuate various ESF equipment in conformance with the NRC Defence-in-Depth and Diversity Position 4 requirements. The DMAS is wired to control panel multiplexers located in the Safety Console.	

There is good agreement about the definition of Diversity, with some outliers that do indicate that the intent of diversity is to cope with common cause failure. The terms Diversification and Diversity Principle are also used with the same meaning as the term Diversity. Some ambiguity is introduced by the term identical function. Does this mean that the diverse systems must accomplish the same specific function, *e.g.* high-pressure injection or does it mean to accomplish the same fundamental safety function? In the latter case depressurization of the reactor pressure vessel and low-pressure injection might be considered diverse from high-pressure injection.

There are a few definitions for specific kinds of Diversity. They do not seem to contribute much given that a complete taxonomy of diversity types is not defined.

It appears that use of the first IAEA definition of Diversity would encompass all of the other definitions for the term Diversity.

B.2 Independence

Terms	Source Document	Definition	Comments
Independent Equipment	IAEA Safety Glossary	Equipment that possesses both of the following characteristics: (a) The ability to perform its required function is unaffected by the operation or failure of other equipment; (b) The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function.	These definitions are similar.
Independent Equipment	IEC Glossary	Equipment that possesses both of the following characteristics: (a) The ability to perform its required function is unaffected by the operation or failure of other equipment; (b) The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function.	
Independence	ASN EPR Safety Report	A system or equipment is said to be independent if it respects both following conditions: • Its capacity to perform its function is not affected by the operation or the failure of other systems or equipment. • Its capacity to perform its function is not affected by the consequences of the initiating event for which its operation is required.	
Independence	NRA Outline of New Requirements	Two or more systems or components are free from simultaneous functional impediment due to common or subordinate causes under environmental or operational conditions considered in design.	This definitions may be intended to be that same as those above
Independent Systems	CNSC RD-337	Systems that do not share any components.	This definition does not address interdependencies between systems except as caused by common components. Communications and common data for example.
Independence	IEEE NPEC IEEE Std 384, IEEE Std 308-2012	The state in which there is no mechanism by which any single design basis event, such as a flood, can cause redundant equipment to be inoperable.	This definition is limited to independence between redundant systems and does not include design dependencies within systems.
Independence	NSSC IEEE Std 384	The state in which there is no mechanism by which any single design basis event, such as a flood, can cause redundant equipment to be inoperable.	

Terms	Source Document	Definition	Comments
The following definitions deals with specific means of achieving an aspect of Independence			
Isolation Device	IEEE NPEC IEEE Std 384	A device in a circuit that prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits.	
Isolation Device	NSSC IEEE Std 384	A device in a circuit that prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits.	
Independence	AERB SC-D1	The ability of equipment, channel or system to perform its function irrespective of the normal or abnormal functioning of any other equipment, channel or system. Independence is achieved by functional isolation and physical separation.	
Separation Principle	STUK Decree 717/2013	Physical separation and functional isolation	
Functional Isolation	STUK Decree 717/2013	The isolation of systems from one another so that the operation or failure of one system does not adversely affect another system; functional isolation also covers electrical isolation and isolation of the processing of information between systems	
Independence	FANR	Prevention of influences from the mode of operation or failure of one circuit or system on another.	These definitions deal with just one aspect for achieving independence.
Functional Isolation	AERB SC-D-20	Prevention of influences from the mode of operation or failure of one circuit or system on another.	
Functional Isolation	IAEA Safety Glossary	Prevention of influences from the mode of operation or failure of one circuit or system on another.	
Functional Separation	SSMFS-2008-17	Systems or components that do not affect each other's function unintentionally.	
Independent Systems	CNSC REGDOC 2.5.2	Systems that are each capable of performing a required function while remaining unaffected by the operation or failure of the other system.	
Independent Systems (elements)	RTN OPB-88/97	Systems (elements) for which failure of one system (element) does not lead to failure of another system (element).	
Independence Principle	RTN NP-082-2007	Principle of the system reliability improvement through application of functional and/or physical separation of trains (elements) where, if implemented, a failure of one train (element) does not lead to a failure of another train (element).	

While there are differences the IAEA definition seems to encompass all of the other definitions.

B.3 Redundancy

Terms	Source Document	Definition	Comments
Redundancy	IAEA Safety Glossary	Provision of alternative (identical or diverse) SSC, so that any one can perform the required function regardless of the state of operation or failure of the other.	
Redundancy	IEC TC45A IEC Glossary	Provision of alternative (identical or diverse) SSC, so that any one can perform the required function regardless of the state of operation or failure of the other.	
Redundancy	FANR FANR-REG-03	Provision of alternative (identical or diverse) SSCs, so that any one can perform the required function regardless of the state of operation or failure of any other.	
Redundancy	ONR Safety Assessment Principles	Provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other.	
Redundancy	STUK YVL B.1	The use of alternative (identical or diverse) structures, systems or system components, so that any one of them can perform the required function regardless of the state of operation or failure of any other.	
Redundancy principle	STUK Decree 717/2013	The use of several parallel subsystems, so that the system can perform the required function even though individual subsystems are out of operation e.g. due to maintenance or failures	These definitions are essentially the same.
Redundant Equipment or System	IEEE NPEC IEEE Std 603	A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function regardless of the state of operation or failure of the other. Note: Duplication of essential functions can be accomplished by the use of identical equipment, equipment diversity, or functional diversity.	
Redundant Equipment or System	NSSC IEEE Std 603	A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function regardless of the state of operation or failure of the other. Note: Duplication of essential functions can be accomplished by the use of identical equipment, equipment diversity, or functional diversity.	
Redundant Equipment or System	NRC 10 CFR Part 50 (IEEE Std 603)	A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function regardless of the state of operation or failure of the other. Note: Duplication of essential functions can be accomplished by the use of identical equipment, equipment diversity, or functional diversity.	
Engineering Redundancy	ONR TAST-GD-036	The provision of more than the minimum number of nominally identical equipment items required to perform a specific safety function. Such redundant provisions allow a safety function to be satisfied when one or more items (but not all) are unavailable, due to a variety of unspecified potential failure mechanisms or maintenance (*e.g.* identified faults or hazards).	This term is similar to the above but quite differently stated. The difference between Engineering Redundancy given here and the definition of redundancy given in the ONR Safety Assessment Principles is unclear.
Redundancy	NSSC	Duplication of essential function can be accomplished by the use of identical equipment, equipment diversity, or functional diversity. Redundancy can be accomplished by use of identical equipment, equipment diversity, or functional diversity. Synonym: redundant system.	These definitions do not discuss the use of redundancy to account for equipment or system unavailability for reasons other than failure.
Redundancy	ASN EPR Safety Report	The implementation of a number of systems or equipment (identical or different) which is higher than the necessary number, so that the failure of one of them does not lead to the loss of the function that they perform.	

Terms	Source Document	Definition	Comments
Redundancy	SSM SSMFS-2008-17	Two or more alternative identical or different systems or components that independently of each other perform the same safety task	This definition is similar to the above but it limits the application of the term redundancy only to items that perform safety tasks.
Redundancy	AERB SC-D1	Provision of alternative structures, systems, components of identical attributes, so that any one can perform the required function, regardless of the state of operation or failure of the other.	These definitions exclude the possibility that redundant channels can also be diverse.
Redundancy	NRA Outline of New Requirements	The existence of two or more systems or components with identical attributes to perform an identical function.	
Redundancy Principle	RTN NP-082-2007	The principle of the system reliability improvement through application of structural, functional and information redundancy in the scope that is maximum necessary and sufficient for the systems to perform the designated functions.	This definition extends the concept of redundancy to functions and information.
Redundant, Redundancy	IEEE NPEC IEEE Std 622	The introduction of auxiliary elements and components to a system to perform the same function as other elements in the system for the purpose of improving reliability. Redundant electric heat tracing systems consist of two heaters and two controllers, each with its own sensor, supplied from two power systems and two alarms, each system independent of the other but all applied to the same mechanical piping, valves, tanks, *etc.* Redundant electric heat tracing systems are referred to as primary and backup in this recommended practice.	This definition is specific to heat trace systems
Standby Redundancy	NSSC	(Software) In fault tolerance, the use of redundant elements that are left inoperative until a failure occurs in a primary element. Contrast: active redundancy. (IEEE Std 610.12-1990) That redundancy wherein the alternative means for performing a given function are inoperative until needed.	This term is specific to software.

There are some differences that may be important:

- The RTN definition extends the concept beyond equipment to information and functions as well.
- The AERB and NRA definitions exclude the possibility that redundant systems may be also diverse.
- One of the two STUK definitions limits the use of the term to systems that perform safety functions.
- The Korean and French definitions do not specifically address the use of redundancy to deal with equipment or system unavailability for reasons other than failure.

None of the definitions above fully embraces all of the ideas given in the other definitions; therefore, users will need to be aware of the differences particular to the organization that will review their applications. Nevertheless, these differences are relatively small thus it should be possible to work out any confusion by discussion between applicants and regulators. It is also possible that the differences are errors introduced during translation.

B.4 Reliability

B.4.1 Availability

Terms	Source Document	Definition	Comments
Availability	IEEE NPEC IEEE Std 577	The characteristic of an item expressed by the probability that it will be operational at a randomly selected future instant in time.	These definitions define availability as a system characteristic and indicate that the characteristic can be expressed as a probability.
Availability	NSSC IEEE Std 577	The characteristic of an item expressed by the probability that it will be operational at a randomly selected future instant in time.	
Operational Availability	IEEE NPEC IEEE Std 338	The measured characteristic of an item expressed by the probability that it will be operable when needed as determined by periodic test and resultant analysis.	
Operational Availability	NSSC IEEE Std 338	The measured characteristic of an item expressed by the probability that it will be operable when needed as determined by periodic test and resultant analysis.	
Availability	IEC SC45A	The ability of an item 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, with the assumption that the necessary external resources are provided.	This definition deals with availability only as a characteristic without giving the commonly accepted quantitative measure.
Availability	IAEA SSG-39	The ability of an item 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, with the assumption that the necessary external resources are provided.	
Availability	AERB SG/D-20	The fraction of time that an entity is capable of performing its intended purpose.	These definitions describe only the measurement of availability.
Availability	CNSC REGDOC 2.5.2	The fraction of time that a component or system is able to function. Availability can also mean the probability that a component or system will be able to function at any given time.	
Availability	IEEE NPEC IEEE Std 352	The probability that an item or system will be operational on demand. 1) Steady-state availability is the expected fraction of the time in the long run that an item (or system) operates satisfactorily. 2) Transient availability (or instantaneous availability) is the probability that an item (or system) will be operational at a given instant in time. For repairable items, this will converge to steady-state availability in the long term.	
Availability	NSSC IEEE Std 352	The probability that an item or system will be operational on demand. 1) Steady-state availability is the expected fraction of the time in the long run that an item (or system) operates satisfactorily. 2) Transient availability (or instantaneous availability) is the probability that an item (or system) will be operational at a given instant in time. For repairable items, this will converge to steady-state availability in the long term.	
Availability	IAEA Safety Glossary	The fraction of time for which a system is capable of fulfilling its intended purpose.	This definition is similar to those above but it limits the term to use on systems. In practice the term is used also for channels and components. One might also argue that components or channels are in themselves systems.
Availability	IEC SC45A	The property of being accessible and usable upon demand by an authorized entity. Note 1 to entry: This definition is different from the one used in the other IEC standards in the field of instrumentation and control of nuclear facilities which is ‘ability of an item 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, assuming that the required external resources are provided’. [SOURCE: IAEA Nuclear Security Series No. 17:2011]”	This definition is specific to cyber security.

There are several different definitions here. The IEEE Std 577 is the broadest and seems to encompass all others. That said, there seems to be little opportunity for confusion even with the variety of definitions.

B.4.2 Dependability

Only one definition was found.

Terms	Source Document	Definition	Comments
Dependability	IAEA Safety Glossary	A general term describing the overall trustworthiness of a system; *i.e.* the extent to which reliance can be justifiably placed on this system. Reliability, availability, and safety are attributes of Dependability.	While this term is in the glossary, it is not widely used in IAEA documents.

B.4.3 Reliability

Terms	Source Document	Definition	Comments
Reliability	IEEE NPEC IEEE Std 577	The characteristic of an item expressed by the probability that it will perform a required mission under stated conditions for a stated time.	This definition defines availability as a system characteristic and indicate that the characteristic can be expressed as a probability.
Reliability	IEEE NPEC IEEE Std 577	The characteristic of an item expressed by the probability that it will perform a required mission under stated conditions for a stated time.	
Reliability	IEC SC45A	"Probability that a device, system or facility will meet its minimum performance requirements when called upon to do so for a specified time under stated operating conditions Note 1: The reliability of a computer-based system includes the reliability of its hardware which is usually quantified and the reliability of its software which is usually a qualitative measure because there are no generally recognized means to quantify the reliability of software. Note 2: This definition differs from 2007 edition of the IAEA Safety Glossary one which is: 'The probability that a system or component will meet its minimum performance requirements when called upon to do so.' IEC SC45A experts indicated that this IAEA definition is not consistent with general practice in that it does not include the idea of mission time.'	These definitions describe only the measurement of availability.
Reliability	AERB SC-D1	The probability that a structure, system, component or facility will perform its intended (specified) function satisfactorily for a specified period under specified conditions.	
Reliability	IAEA Safety Glossary	The probability that a system or component will meet its minimum performance requirements when called upon to do so.	
Reliability	ONR Safety Assessment Principles	The probability that a system or component will meet its minimum performance requirements when called upon to do so.	
System Reliability	NSSC IEEE Std 729-1983	The probability that a system, including all hardware and software subsystems, will perform a required task or mission for a specified time in a specified environment.	While similar to the above this definition only applies to systems.
Reliability Targets	IEEE NPEC IEEE Std 933	The reliability goals to be achieved by the plant systems.	
Reliability Targets	NSSC NPEC IEEE Std 933	The reliability goals to be achieved by the plant systems.	
Operational Reliability	IEEE NPEC IEEE Std 933	The assessed reliability of an item based on operational data.	
Operational Reliability	NSSC IEEE Std 933	The assessed reliability of an item based on operational data.	
Operational Reliability	NSSC IEEE Std 729-1983	(software) The reliability of a system or software subsystem in its actual use environment. Operational Reliability may differ considerably from reliability in the specified or test environment. See also: system; reliability.	

The IEEE Std 577 definition seems to encompass all others. The definitions of reliability are fairly similar, but there has been a lot of 'wordsmithing'. That said, there seems to be little opportunity for confusion even with the wide variety of definitions.

The IEEE Std 577 definition is succinct and seems to encompass all others when they are stripped of explanatory text. It also has the advantage of noting that reliability is a characteristic of an item and that probability is simply a means to measure the characteristic.

B.5 Separation

Terms	Source Document	Definition	Comments
Physical Separation	IAEA Safety Glossary	Separation by geometry (distance, orientation, *etc.*) by appropriate barriers, or by a combination thereof.	These definitions are basically the same.
Physical Separation	AERB SC-D1	A means of ensuring independence of equipment by separation by geometry (distance, orientation, *etc.*), appropriate barriers or combination of both.	
Physical Separation	FANR	Separation by geometry (distance, orientation, *etc.*), by appropriate barriers, or by a combination thereof.	
Physical Separation	TAEK Design Principles of NPP	Separation by geometry (distance, orientation, *etc.*), by appropriate barriers, or by a combination thereof.	
Physical Separation	SSM SSMFS-2008-17	Systems or components that are physically separated through distance or barriers or a combination of these.	
Segregation	ONR Safety Assessment Principles	The physical separation of structures, systems or components by distance or by some form of barrier that reduces the likelihood of common cause failures.	
Segregation	ONR TAST-GD-036	The separation of components by distance or physical barriers, a particular example being provision of principal fire barriers to delineate individual fire zones; such barriers may also serve as barriers to other hazards.	
Separation	IEEE Std 690-1984	Physical independence of redundant circuits, components, and equipment. (Physical independence may be achieved by space, barriers, shields, *etc.*)	
Separation	NSSC IEEE Std 690-1984	Physical independence of redundant circuits, components, and equipment. (Physical independence may be achieved by space, barriers, shields, *etc.*)	
Physical Separation	STUK Decree 717/2013	The separation of systems or components from one another by means of adequate barriers, distance or placement, or combinations thereof.	
Physical Separation	ASN EPR Safety Report	The physical separation of two equipment consists in separating them with an appropriate barrier (*e.g.* a wall).	This definition limits physical separation to separation by barriers. Separation by distance is considered to be a different kind of separation. See Geographical Separation below.
Geographical Separation	ASN EPR Safety Report	The geographical separation of two equipment consists in arranging them at a sufficient distance or in orientating them in sufficiently different manners, in order to prevent their simultaneous failure in case of hazard or initiating event. The sufficient distance depends on the considered hazard or initiating event.	This definition considers separation by distance to be different from physical separation.

Terms	Source Document	Definition	Comments
Separation Distance	IEEE Std 384-1992	Space that has no interposing structures, equipment, or materials that could aid in the propagation of fire or that could otherwise disable Class 1E systems or equipment.	
Separation Distance	NSSC IEEE Std 384-1992	Space that has no interposing structures, equipment, or materials that could aid in the propagation of fire or that could otherwise disable Class 1E systems or equipment.	

All but the STUK and ASN definitions basically use the IAEA definition.

The STUK definition for Separation of Subsystems seems to require different channels to be located in different rooms. Perhaps this is a problem with the translation from Finnish. The STUK definition of Separation Principle refers to their term Operational Separation and the additional text adds nothing meaningful. Its term Operational Separation describes what all others describe as independence. This definition is weaker than that given by IAEA.

The ASN definition of physical separation limits the term to mean separation by barriers and thus is inconsistent with the IAEA definition. For the French separation by distance is considered Geographical Separation, rather than being just another form of physical separation.

Note also the ONR use of Segregation in place of Separation. Applicants in the UK should be aware of this oddity. An argument could be made that this is more precise English, but given the wide spread use of the term Separation it can also be argued that it gives precision priority over comprehension.

B.6 Spurious Activation

Terms Spurious	Source Document	Definition
Initiation	KINS	Attempts to establish a communication connection or association, using a false identity or through the replay of a previous, legitimate initiation sequence. Spurious initiation includes spoofing or masquerading attempts in the communication system, and coupled with other attacks, could result in unauthorized disclosure or modification of information, unauthorized receipt of services, or denial of service to legitimate users or critical functions.

This definition is specific to cyber-security. The concept of unintended operation due to failures or design errors is more relevant to issues of safety classification. No authoritative definition was found for this concept.

Appendix C | References

[1] CORDEL DICTF 2014-2016 Outlook

[2] Safety Classification for I&C in Nuclear Power Plants – Current status and difficulties

[3] IAEA Specific Safety Requirements SSR-2/1 (Rev.1) – Safety of Nuclear Power Plants: Design, 2016

[4] INSAG-10, Defence in Depth in Nuclear Safety

[5] Defence-in-Depth and Diversity: Challenges Related to I&C Architecture

[6] (Canada) Nuclear Energy Act, RSC, 1985, c A-16

[7] General Nuclear Safety Regulations (SOR/2000-202)

[8] Design of Reactor Facilities: Nuclear Power Plants (REGDOC-2.5.2)

[9] Design of New Nuclear Power Plants (RD-337)

[10] Government Degree [sic] on the Safety of Nuclear Power Plants (717/2013)

[11] Regulatory Oversight of Safety in the Use of Nuclear Energy (YVL A.1)

[12] Safety Design of a Nuclear Power Plant (YVL B.1)

[13] Electrical and I&C Equipment of a Nuclear Facility (YVL E.7).

[14] Nuclear Facilities Order (2012)

[15] EPR Safety Report (Flamanville 3).

[16] Design of Light Water Reactor Based Nuclear Power Plants (AERB/NPP-LWr/SC/D)

[17] Computer Based Systems of Pressurized Heavy Water Reactors (AERB/NPP-[14] PHWR/SG/D-25)

[18] Design of Pressurized Heavy Water Reactor Based Nuclear Power Plants (AERB/NPP-PHWR/SC/D-1)

[19] Safety Classification and Seismic Categorization for Structures Systems and Components of Pressurized Heavy Water Reactors (AERB/NPP-PHWR/SG/D-1)

[20] Safety Related Instrumentation and Control for Pressurised Heavy Water Based Nuclear Power Plants (AERB/NPP-PHWR/SG/D-20)

[21] IEEE Std 338-2012 - IEEE Standard for Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

[22] ANSI/IEEE Std 352-1987 IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems

[23] IEEE Std 384-2008 IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits

[24] IEEE Std 577-2012 IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations

[25] IEEE Std 603-2009 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

[26] ANSI/IEEE Std 622-1987 IEEE Recommended Practice for the Design and Installation of Electric Heat Tracing Systems for Nuclear Power Generating Stations

[27] IEEE Std 690-1984-2004 IEEE Standard for the Design and Installation of Cable Systems for Class 1E Circuits in Nuclear Power Generating Stations

[28] IEEE Std 933-1999 IEEE Guide for the Definition of Reliability Program Plans for Nuclear Power Generating Stations

[29] IAEA Safety Glossary 2007

[30] IAEA SSG-39 - “Design of Instrumentation and Control Systems for Nuclear Power Plants”

[31] IEC Glossaryhttp://std.iec.ch/glossary

[32] NRA Outline of New Regulatory Requirements (Design Basis)

[33] IEEE Std 729-1983 IEEE Standard Glossary of Software Engineering Terminology

[34] Law on Use of Atomic Energy (170-FZ)

[35] General Regulations on Ensuring Safety of Nuclear Power Plants (OPB-88/97)

[36] Nuclear Safety rules for Reactor Installations of Nuclear Power Plants (NP-082-07)

[37] Basic Licensing Requirements for the Pebble Bed Modular Reactor (RD-0018)

[38] Guidance for Licensing Submissions Involving Computer Software and Evaluation Models for Safety Calculations (LG-1045)

[39] Licensing Guide on Safety Assessments of Nuclear Power Reactors (LG-1041)

[40] Design and Implementation of Digital Instrumentation and Control for Nuclear Installations (PP-0017)

[41] The Swedish Radiation Safety Authority's Regulations and General Advice Concerning the Design and Construction of Nuclear Power Reactors (SSMFS 2008:17)

[42] Swedish Radiation Safety Authority Regulatory Code (SSMFS 2008:1)

[43] Guide on Specific Design Principles

[44] Regulation on Design Principles for Safety of Nuclear Power Plants

[45] Regulation on Specific Principles for Safety of Nuclear Power Plants

[46] Regulation for the Design of Nuclear Power Plants (FANR-REG-03)

[47] Guidelines for the Design, Construction, and Operation of Nuclear Power Plants (FANR-RG-005)

[48] Safety Assessment Principles for Nuclear Facilities

[49] ONR Guide – Safety Related Instrumentation (NS-TAST-GD-031)

[50] ONR Guide – Diversity, Redundancy, Segregation and Layout of Mechanical Plant (NS-TAST-GD-036)

[51] ONR Guide – Computer Based Safety Systems (NS-TAST-GD-046)

[52] ONR Guide – Design Safety Assurance (NS-TAST-GD-057)

[53] Code of Federal Regulations: Domestic Licensing of Production and Utilization Facilities (10 CFR Part 50)

[54] USNRC Glossary (NRC Website)

[55] Standard Review Plan for Light Water Cooled Nuclear Reactors, Rev. 7, Appendix 7-B (NUREG-0800)

World Nuclear Association
Tower House
10 Southampton Street
London WC2E 7HA
United Kingdom

+44 (0)20 7451 1520
www.world-nuclear.org
info@world-nuclear.org