IAEA SAFETY STANDARDS

for protecting people and the environment

Draft ~~M~~ N

Step 1~~0~~1

~~Addressing~~ Member States**'** **and NUSSC** ~~for~~ comments **addressed**.

Reviewed in NS-SSCS (Asfaw)

Design of Instrumentation and Control Systems for Nuclear Power Plants

DS-431

DRAFT SAFETY GUIDE

New Safety Guide

Supersedes NS-G-1.1 and NS-G-1.3

IAEA

International Atomic Energy Agency

~~TABLE OF~~ CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. This Safety gGuide gives provides recommendations on the design of iInstrumentation and cControl (I&C) systems to meet the requirements established in the Specific Safety Requirements publication on Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR 2/1, Ref. [1].

1.2. This publication is a revision and combination of two previous Safety Guides, namely —IAEA Safety Standards Series Nos. NS-G-1.1 [1], Ref. [2], and No. NS-G-1.3 [2], Ref. [3], which itare supersedesd by this Safety Guide. The revision takes into account of developments in I&C systems since the publication of the predecessor earlier Safety gGuides in 2000 and 2002, respectively. The main changes are duerelate to the continuinged development of computer applications and the evolution of the methods necessary for their safe, secure and practical use. In addition, account is taken of developments in human factors engineering and the need for computer security. It This Safety Guide references and takes into account other IAEA Safety Standards and Nuclear Security Series documents publications that have givenprovide guidance that affectsrelating to I&C design. Most notable among these are the Safety Requirements for on the Management System for Facilities and Activitiess, IAEA Safety Standards Series No. GS-R-3, Ref. [42], and its supporting Guides IAEA Safety Standards Series No. GS-G-3.1, Ref. [53] and IAEA Safety Standards Series No. GS-G-3.5, Ref. [64], and the General Safety Requirements on Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GS-R Part -4, Ref.[75].

1.3. The main topical areas for which this Safety Guide gives provides new or updated guidance are the following:

- Considerations specific to I&C for achieving compliance with GS R 3,the requirements established in Ref. [42];.;

- Design inputs to be considered when developing the design basis for I&C systems design bases;.;

- The interdependent set nature of life cycles the development processes associated with needed for the design and implementation of I&C systems, and in particular the life cycle for the overall I&C for the facility as a whole, for individual I&C systems and for, software, and the need for the

---

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standard Series No. NS-G-1.1, IAEA, Vienna (2000).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Guide Series No. NS-G-1.3, IAEA, Vienna (2002).

integration of human factors engineering inputs and computer security inputs into those life cycles;.

- The use of computers, devices programmed with hardware description languages (HDL), and industrial devices of limited functionality, and recommendations means offor gaining assurance of their correct performance;.

- The overall I&C architecture to in support of the concept of defence in depth concept applied in the design of the nuclear plant systems and mechanical systems and to in establishing defence in depth for the I&C system itself as a protection against common cause failure;.

- Data transport between systems important to safety, with special requirements consideration for cases where the system receiving data is of in a higher safety class than the system sending data;.

- Provisions for ensuring the security of digital safety systemsProvisions for ensuring the security of digital safety systems;.

- Activities relating to the development of Ccomputer software development activities including design, verification and validation, derived from the principles given in this Safety Guide or implicit in the detail of previous Safety Guide NS-G--1.-1, Ref. [2].

1.4. Throughout the documentthis Safety Guide, the term 'I&C system' refers to any I&C system important to safety as defined by the IAEA Safety Glossary, Ref. [86]. The term 'important to safety' is not repeated again except for emphasis. In cases, where recommendations or explanations are applicable to both I&C systems important to safety and I&C systems that are not important to safety, the term 'All I&C systems' is usedthis is explicitly stated.

1.5. This Safety gGuide has a particularly strong relationship withis closely related to DS-430, Ref. [97], (the draft Ssafety Gguide on Design of Electrical Power Systems for Nuclear Power Plants), which gives provides recommendations for power supply, cable systems, protection against electromagnetic interference, equipment and signal grounds, and other topics that are necessary for the satisfactory operation of I&C systems.

1.6. Additional guidance for on the design and development of I&C systems, equipment, and software are is available from Member States and from other organizations that develop sStandards Development Organizations. Their documentsSuch publications give much greater detail than is appropriate for IAEA sSafety sStandards. It is expected that this Safety Guide will be used in conjunction with an appropriate set of more detailed industrial standards.

OBJECTIVE

1.7. The objective of this Safety Guide is to provide guidance on the overall I&C architecture and on the I&C systems important to safety in nuclear power plants for the satisfaction ofmeeting the safety goals of the plant.

1.8. The Safety Guide identifies the input information needed by I&C designers to define the I&C design basis from the mechanical, electrical, nuclear, and civil engineering design of the plant, from the plant layout process, and from safety analysis. The I&C design basis will, for example, give provide the functional requirements to be achieved by the I&C, the extremes of environmental temperature in which equipment is required to operate, the external events that I&C equipment is required to withstand, and the conditions for which an automatic shutdown is required to take place.

SCOPE

1.9. This Safety Guide provides guidance on the design, implementation, qualification, and documentation of I&C systems important to safety in nuclear power plants to achieve compliance with meet IAEA SSR 2/1, the requirements of Ref. [1]. This Safety Guide also discusses describes certain I&C specific issues which are relevant to implementing the recommendations of certain other Safety Guides, such as those which cover the management systems, commissioning, installation, operation, and operating limits and conditions. For such cases, this Safety Guide identifies relevant sections of these other Ssafety Gguides that are being addressed.

1.10. The guidance applies to all I&C equipment, from the sensors to the devices which that actuate and control mechanical equipment. It covers, for example, the following:

- Sensors,;

- Actuator controls,;

- Equipment for automatic and manual control of plant equipment;,

- Operator interfaces.

1.11. The Safety gGuide also applies to the means for implementing I&C equipment such as:

- Computer systems and associated communication systems, :

- Software;,

- Devices that are programed using hHardware dDescription lLanguages (e.g., field programmable gate arrays),; and

- Industrial digital devices of limited functionality.

1.12. This Ssafety Gguide does not give provide recommendations for support features of for I&C systems, such as cooling, lubrication, and energy supply. Recommendations for electrical energy pwoerpower supply are given provided in DS 430, Ref. [97].[3] Recommendations for other support features are to be given in a new safety guide on the topic of auxiliary systems.

---

[3] A draft Safety Guide on the topic of auxiliary systems that will provide recommendations for other support features is currently under development.

1.13. Although this Ssafety Gguide covers certain aspects of human factors and computer security as they relate to I&C, it is does not a provide comprehensive guidance on these domains. The intent in this Safety Gguide is to identify major interfaces with the human factors and computer security activities and to give recommendations on I&C design features that affect these topics. Example of human factors and computer security topics not covered in this guide include: computerised operating procedures, and information technology security. More detailed information on computer security is available in the IAEA Nuclear Security Series documents Ref NSS17provided in Ref. [8].

1.14. The guidance applies to the design of I&C systems for new plants, to modifications of existing plants, and to the modernization of the I&C of existing plants. The IAEA safety guide NS G 2.3, Reference. [109] deals with plant modification, and. Tthe overlap of this Safety Gguide with NS G 2.3Ref. [9] has been kept to a is minimumized.

1.15. The IAEA Safety Glossary defines I&C systems important to safety as those I&C systems that are part of a safety group and also those I&C systems whose malfunction or failure could lead to radiation exposure of site personnel or members of the public. Section 5 of this Safety Guide further discusses the term 'important to safety' and other terminology relating to safety classification terminology. Examples of I&C systems to which this Safety gGuide may apply include:

- Reactor protection systems,;

- Reactor control systems, reactivity control systems, and their monitoring systems;,

- Systems to for monitoring and controlling reactor cooling;,

- Systems to for monitoring and controlling emergency power supplies;,

- Systems to for monitoring and controlling containment isolation;,

- Instrumentation for Aaccident monitoring instrumentation;,

- Systems for monitoring of eEffluents monitoring systems;, and

- I&C systems for fuel handling.

1.16. This Ssafety Gguide also provides recommendations for the development of computer software for use in I&C systems important to safety as well as for digital data communication. This sSafety gGuide also defines measures needed for I&C functions that are programmed into integrated circuits using HDL hardware description languages..

1.17. The IAEA's Technical Reports Series No. 387, Ref. erences [104],. and Nuclear Energy Series NP T 3.12, Ref. [112], present overviews of concepts that underlie this Safety Guide and give examples of systems discussed addressed in it. These references may provide useful background material for some users, although they should not be used directly asdo not provide IAEA guidance.

STRUCTURE

1.18. Section 1, this introduction, provides the scope and objectives of the Guide.

1.189. Section 2 gives provides guidance for the application of the requirements in Ref. [2] and the recommendations of Refs [3, 4] IAEA Management System standards as they relate specifically to the development of I&C systems. It also considers addresses the use of life-cycle models to describe management system processes for the development of I&C, gives provides guidance on the generic processes for I&C design, and gives provides guidance on the implementation conduct of specific I&C development activities.

1.2019. Section 3 identifies the necessary inputs to the design and provides recommendations on the need to provide the design basis of for I&C systems.

1.210. Section 4 gives provides guidance on the architecture of the overall I&C for the plant.

1.212. Section 5 describes the safety classification scheme that is used to grade the application of the recommendations of this Safety gGuide according toin accordance with the safety significance of items to which they apply.

1.223. Section 6 provides general guidance applicable to all I&C systems important to safety.

1.234. Section 7 gives provides recommendations that are specific to certain systems such as the reactor protection system, certain types of equipment such as sensors, and to certain technologies such as digital systems and integrated circuits configured with HDLhardware description languages. The guidance ofrecommendations in Sections 2 to 67 and Sections 89 and 910 also apply to the specific systems discussed in Section 78.[last sentence unclear; check section numbers]

1.245. Section 8 is concerned with addresses the human-machine interface (HMI). It includes guidance on the application of hHuman fFactors pPrinciples to I&C and the characteristics to be achieved bythat the human machine interfaceHMI should have.

1.256. Section 9 gives provides guidance on the development of software for computer based I&C systems important to safety.

1.267. This Safety gGuide should be considered applied as a whole, not as a series of stand-alone sections. For example, the guidance on software given provided in Ssection 9 is to be applied in conjunction with the guidance on the management systems and on development lifecycleprocesses guidance given in Ssection 2.

1.278. Informative aAnnexes include references, a listing of internationallyindustrial used standards that provide more detailed guidance on the topical areas of this Safety gGuide, information and relating this Safety gGuide to the two preceding Safety Gguides it supersedes, and a list of definitions, and a summary of areas where practices of Member States differ. A list of definitions specific to this Safety Guide is also provided.

2. THE MANAGEMENT SYSTEMS FOR I&C DESIGN

2.1. SSR 2/1 Requirement 6 [1] states that:

"The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized."

2.2. SSR 2/1 Requirement 2 [1] states that:

"The design organization shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design."

2.3. IAEA Safety Requirements GS-R-3, Reference. [42] establishes requirements for the management systems of for nuclear facilities and activities.

2.4. GS-R-3 Paragraph 2.1 Reference [2], para. 2.1 states that:

"A management system shall be established, implemented, assessed and continually improved. It shall be aligned with the goals of the organization and shall contribute to their achievement. The main aim of the management system shall be to achieve and enhance safety by:

– Bringing together in a coherent manner all the requirements for managing the organization;

– Describing the planned and systematic actions necessary to provide adequate confidence that all these requirements are satisfied;

– Ensuring that health, environmental, security, quality and economic requirements are not considered separately from safety requirements, to help preclude their possible negative impact on safety."

GS-R-3 Reference [2], Ppara.graph 4.21 further states:

"The iInformation and knowledge of the organization shall be managed as a resource."

2.5.   -In order to ensure safety, design bases documentations on the design basis and related information or records relatinged to I&C systems important to safety must should be controlled by suitable processes, such that they are complete, clear, concise, correct and consistent over the entire lifecycle development process for the I&C system. The management system must should ensure that design basies documents and related or derived information or records are sufficient and adequate, and

are maintained over time to reflect design changes or changing conditions in at the plant. This includes documents and information that may be derived from the design basjes documentation and that may have an impact on safety, such as procedures or manuals relatinged to operation, maintenance, or modification of such systems.

2.56. The Mmanagement systems includes the organizational structure, the organizational culture, policies, processes, including those to identify and allocate resources (e.g., personnel, equipment, infrastructure, the working environment), and processes for developing I&C systems that meets safety requirements.

2.76. Each organization involved in I&C development activities should have a management system which that is consistent with the expectations of the management system of the operating organization management system.

2.87. Safety Guides GS-G-3.1, Ref. References [35] and GS-G-3.5, Ref. [46] give provide guidance on the application of the GS-R-3, Ref. [4] requirements established in Ref. [2] to for facilities and activities and for nuclear power plantsinstallations and other kinds of installations, facilities, and activities.

2.98. The management systems for development of I&C systems should comply meetwith the requirements of GS-R-3, Ref. [24], and be in accordance with the recommendations of Safety Guides GS-G-3.1, provided in Rrefs. [53] and GS-G-3.5, Ref. [46], which apply broadly for the development of all systems, structures and components in a nuclear power plant. This Safety Guide, which addresses the specific development processes needed for I&C systems, should be used in conjunction with these publications.

2.9. The management systems requirements and recommendations of these documents broadly apply to development activities for all NPP systems, structures, and components. Therefore, it is expected that this guide will be used in conjunction with the IAEA management systems guidance. For the most part, the application of the management systems requirements and recommendations to I&C does not need further interpretation in this safety guide. What is unique for I&C systems is the specific development process needed. The GS-R-3, Ref. [4] topics of Ref. [2] that are of particular interest in the development of I&C systems are listed belowin the following:

- The Mmanagement sSystems;

- Safety culture;

- Management commitment;

- Compliance with Sstatutory and regulatory compliancerequirements;

- Organizational policies;

- Planning;

12

- Responsibilities and authority;

- Provision of resources;

- Human resources;

- Development of management system processes;

- Process mManagement;

- Control of documents, products (including tools), and records;

- Purchasing;

- Communication;

- Management of organizational change;

- Monitoring and measurement;

- Self-aAssessment;

- Independent aAssessment;

- Non-conformances and corrective and preventative actions; and

- Improvement.

USE OF LIFE CYCLE MODELS

2.10. GS-R-3Reference [2], para. 5.1 paragraph 5.1 states:

"The processes of the management system that are needed to achieve the goals, provide the means to meet all requirements and deliver the products of the organization shall be identified, and their development shall be planned, implemented, assessed and continually improved."

2.11. Modern nuclear power plant Modern I&C systems in nuclear power plants are complex entities that needfor which different approaches to design and qualification approaches are necessary beyond those that were typically applied to older systems. Often Frequently, the functional characteristics and performance of previous generations of I&C systems could be wellwere characterized by models based upon physics principles and testing that validateds these models.

2.12. Modern I&C systems, in particular digital systems whose functionality depends upon software or a hardware definition language (HDL) descriptions, are fundamentally different from older systems in that their behaviour is determined by logic and is not prescribed by externally by the continuity of physical laws. Consequently, minor errors in design and implementation can cause digital systems to exhibit unexpected behaviour.

2.123. In digital I&C systems, demonstration that the final product is fit for its purpose depends greatly, but not exclusively, on the use of a high-quality development process that provides for disciplined specification and implementation of design requirements. Verification and validation is activities are necessary to for ensuring that the final product is suitable for use. However, correct performance of digital I&C systems performance over the full range of conditions cannot be inferred from the a combination of testing and physics models to the same extent that this can be done for systems that rely only on hardware systems. Consequently, confidence in the correctness of modern systems derives more from the discipline of the development process, than was the case for systems implemented purely with hardware.

2.14. In response to this situation, in the nuclear power community domain as well as in other safety-critical domains such as aerospace, have applied development processes have been applied that are commonly represented as life cycle models, which describe the activities for the development of electronic systems and the relationships between these activities. These commonly accepted practices have been formalized in nuclear standards that provide extensive guidance regarding processes for developing I&C systems. Normally, activities relatinged to a given development step are grouped into the same phase of the development process.

2.15. A well-documented development process will also produces evidence that can allow independent reviewers and the regulatorys body to gain confidence in the fitness for purpose of the final product.

2.16. The recommendations for life cycle processes described provided in this section also apply to life cycle activities described in Ssection 9. The life cycleguidance on developmentlife cycle processes guidance in this section supplements the requirements of of GS R 3, Ref. [24] and the recommendations of GS G 3.1, Refs. [35] and GS G 3.5, Ref. [46] as they apply to the development of I&C systems development.

2.17. Three fundamental levels of life cycles are needed to describe the development of I&C systems:

- An overall I&C architecture life cycle;

- One or more individual I&C system life cycles; and

- One or more individual component life cycles. Component life cycles are typically managed in the framework of a platform development and are independent from the overall architecture level and the individual system level life cycles. Component life cycles for digital systems are typically divided into separate life cycles for the development of hardware and software.

2.18. Other activities sometimes outside of the development of I&C systems development will have an important influence on the requirements for and the design of I&C systems requirements and design. Human factors engineering and computer security are examples of such activities. These Such activities have a broader purpose than the support of I&C system design, but they will have a strong influence on I&C development. Furthermore, it is easier and more cost efficient to take account of

human factors and security features ~~are easier and more cost efficient to implement~~ in the design phase. After~~wards~~ the design phase, changes can be very difficult or even impossible to implement.

2.19. Figure 1 shows an example I&C development life cycle and the main inputs received from the ~~h~~Human ~~f~~Factors ~~e~~Engineering ~~(HFE)~~ and computer security program~~me~~s.

2.20. The 'V-model'~~'~~ shown in Fig.~~ure~~ 2 is a useful alternative view of a~~n~~ ~~example~~ sample development ~~lifecycle~~process. This model illustrates the relationship between requirement~~s~~ specification, design, integration~~,~~ and system validation ~~activities~~ and how ~~V&V~~verification and validation activities relate to development activities. Figure 2 applies to both digital and analogue systems. Of course, if there is no software, the software activities are unnecessary.

2.21. At any time in the development process, ~~lessons learned~~experience gained might result in a need to revise work done in a previous phase. These changes will then flow through and affect work from the intervening phases. For simplicity, ~~figures~~ Figs 1 and 2 do not show ~~the~~ such iteration paths.
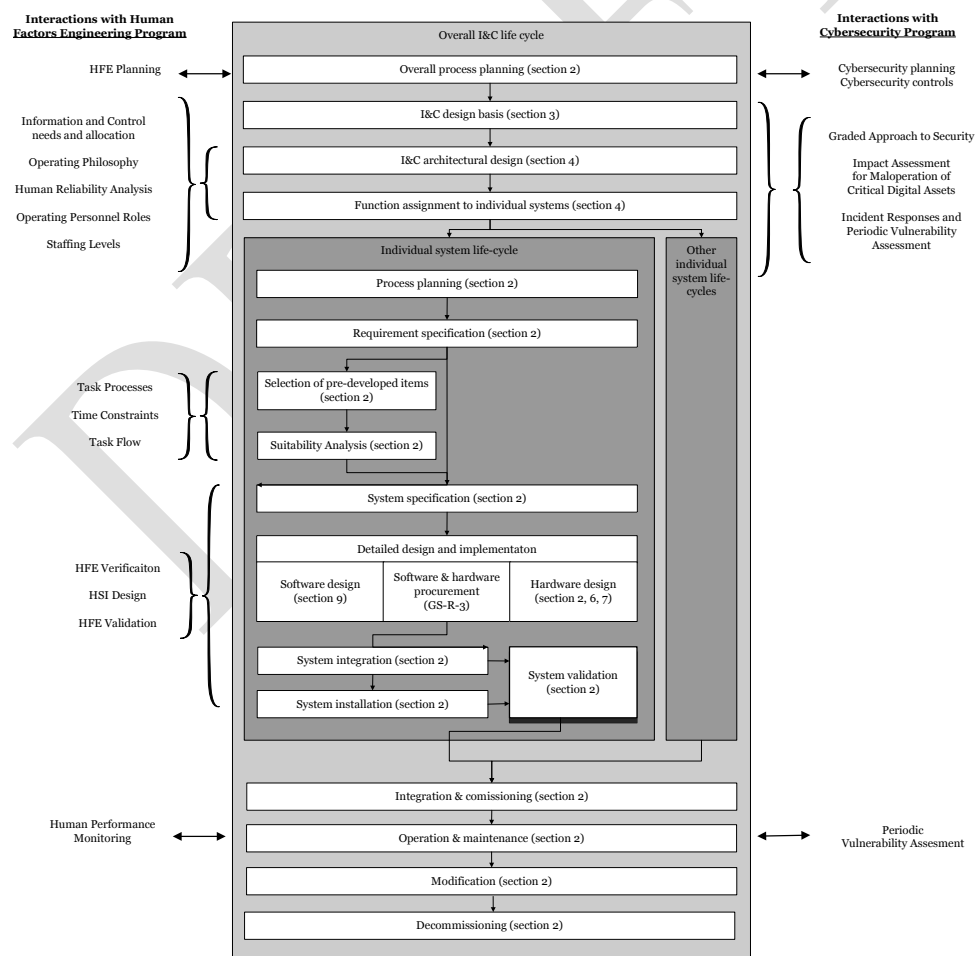
FIG. 1. Typical I&C life cycle activities and interfaces with HFE and Computer Security programs

2.22. All activities associated with development, implementation, and operation of the overall I&C architecture, individual I&C systems, and I&C components[4] (including hardware, software, and HDL descriptions) should be carried out in the framework of a documented development life cycle.

2.23. The life cycle of each I&C system and component should cover the a period that starts with derivationing their requirements and finishes ends when they the I&C system or component isare no longer required for the safety of the plant.

Process planning

2.24. Before the initiation of any technical activity, a plan identifying the necessary inputs, and the products, and processes, of that activity, and the relationship of the activity with other activities, should be prepared and approved in accordance with the requirements for the management system.
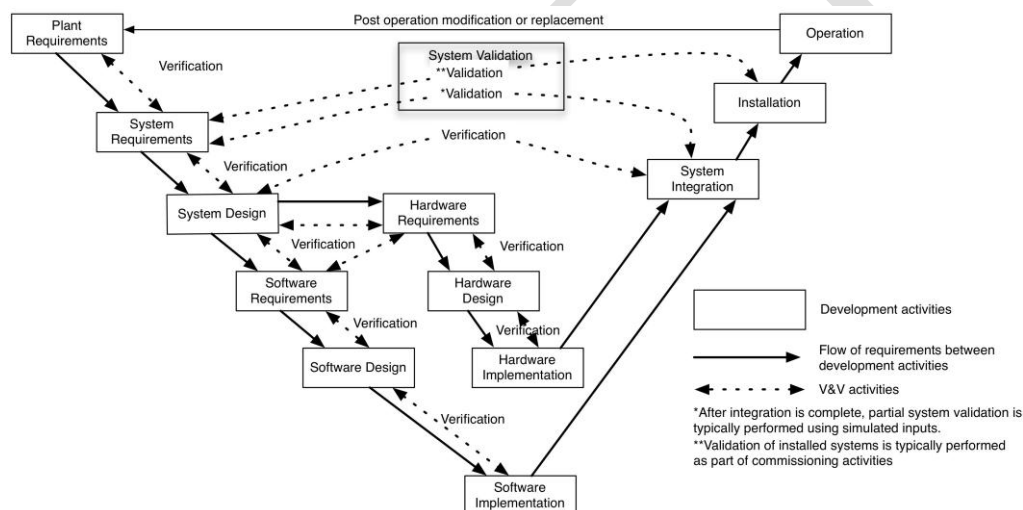
FIG. 2 Typical relationship Between I&C life cycle processes and V&Vverification and validation activities

2.25. Plans for the development of I&C systems deal with the topics that are specific to I&C and with topics where I&C development may need a specialized treatment. Typically, plans specific to I&C development will be prepared to deal with the topics given belowin the following:.

- Life cycle models;

- Configuration management;

- Identification, control, and resolution of non non-conformances;

---

[4] I&C components includes hardware, software such as application software and firmware, and hardware description language.

- I&C system hazard analysis;

- Verification and validation;

- Use of insights from probabilistic safety assessment;

- Safety analysis specific to I&C safety analysissystems;

- Requirements engineering;

- Architectural design;

- Selection and acceptance of pre-developed items;

- Design;

- Implementation, e.g., hardware manufacture and coding of software or coding and synthesis of HDL a hardware description languages;

- Integration;

- System validation;

- Installation;

- Commissioning;

- Equipment qualification;

- Qualification and use of tools;

- Maintainability;

- Mitigation of Oobsolescence mitigation;

- Operations;

- Training;

- Software maintenance/recovery.

2.26. Plans for Sseveral of these topics may be combined into a single plan.

2.27. The development of I&C systems also depends upon plans for activities that are not specific to I&C development, such as:

- Quality assurance;

- Classification of items important to safety;

- Purchasing;

- Manufacturing; and

- Production and maintenance of documentation.

2.28. All I&C development activities should be performed in accordance with the applicable approved plans.

Coordination with human factors engineering activities and computer security activities

2.29. Al~~T~~though development processes relating to ~~HFE~~ human factors engineering and c~~C~~omputer s~~S~~ecurity ~~life cycle processes~~ are not covered by this Safety ~~g~~Guide, ~~these~~ such processes provide information that is required for the I&C development. Figure 1 illustrates the relationships and interfaces between these processes. These include: activities that produce ~~HFE specific~~ requirements specific to human factors engineering, outputs of ~~the HFE V&V~~ verification and validation activities relating to human factors engineering, technical security measures and computer security requirements.

2.30. The development of I&C ~~development~~ systems should be coordinated with human factors engineering activities ~~HFE~~ and computer security activities.

2.31. In the development of I&C ~~development~~ systems~~should implement~~ requirements ~~developed by~~arising out of the h~~H~~uman f~~F~~actors e~~E~~ngineering program~~me should be taken into account~~, including:

   a. The ~~identification~~ specification of roles and responsibilities of operating personnel ~~roles and responsibilities~~ and other staffing requirements;

   b. Safety classification of the elements of the h~~H~~uman-~~M~~machine i~~I~~nterface;

   c. The ~~identification~~ specification of information needs, including considerations for defining a subset of indications and controls required to address accident conditions and post-accident conditions;

   d. The ~~identification~~ specification of control needs, automatic and manual control functionality and the allocation of controls to suitable locations;

   e. Requirement relating to ~~T~~task process~~es~~, time constraints and the~~,~~ flow of operating personnel and information as identified by analyses (i.e. task analysis, see para.~~graph~~ 8.78);

   f. Strategies for C~~c~~ontext based annunciation ~~strategies; C~~ context based annunciation avoids flooding of messages~~which might occur~~, for example, during start-up~~s~~ and during transients;

   g. Requirements for the reporting of I&C system fault~~s reporting~~;

   h. Provisions ~~to~~ in support of I&C maintainability;~~, and~~

   i. Insights resulting from consideration of the potential for human error in safety analysis (i.e. h~~H~~uman r~~R~~eliability a~~A~~nalysis).

2.32. Verification and validation activities relating to H~~h~~uman F~~f~~actors e~~E~~ngineering ~~Verification and validation activities~~ should:

   a. Verify the resolution ~~to~~ of ~~HFE~~ recommendations relating to human factors engineering and deficiencies identified during analyses of the ~~HMI~~ design of the human-machine interface;

    b.   Verify that the I&C systems conform to applicable HFE design guidelines relating to human factors engineering;

    c.   Verify that the design provides I&C systems, other equipment, and operator aids that are adequate to for supporting operating personnel in the performance of their assigned tasks;

    d.   Verify that the HFE human factors design elicits proper operator response to annunciation messages, including allowing time adequatecy time for credited operator actions ; and

    e.   Validate, using performance based measures, that operating personnel can carry out their functions using the I&C system under all conditions under in which the system is expected to function, including when some parts of the I&C system are out of service for authorizsed reasons (for example, for purposes of maintenance or testing purposes).

2.33. The development of HFE human factors engineering requirements and V&Vthe verification and validation of human factors engineering HFE activities are normally performed within as part of the hHuman fFactors eEngineering programme. The human factors engineering HFE programme is not described in any further detail within this Safety gGuide, with the exception of the interfaces to the I&C life cycledevelopment process.

2.34. The overall I&C for the plant should implement the security measures that are assigned to it by the computer security plan.

2.35. The computer security plan should be updated as necessary to take into account the overall I&C architecture and individual I&C systems.

2.36. Development of I&C should be conducted through dialogue between personnel responsible for safety and for nuclear security or by a mixed team of safety and nuclear security personnel in a development environment that meets the technical, procedural and administrative requirements of the computer security planDevelopment of I&C development should be conducted in a development environment that meets the technical, procedural, and administrative requirements of the computer security plan.

2.37. Additional information on the implementation of computer security at nuclear facilities is given provided in IAEA Nuclear Security Series No. 17, Ref. [138].

ACTIVITIES COMMON TO ALL LIFE-CYCLE PHASES

Configuration Management

2.38. GS-R-3Reference [2], paragraphs 5.12 through to 5.19 states:

    "Documents shall be controlled. …It shall be ensured that document users are aware of and use appropriate and correct documents. …

    "Changes to documents shall be reviewed and recorded and shall be subject to the same level of approval as the documents themselves. …

    "Controls shall be used to ensure that products do not bypass the required verification activities. …

"Products shall be identified to ensure their proper use. Where traceability is a requirement, the organization shall control and record the unique identification of the product."

2.39. In GS-R-3, Ref. [24] these topics are discussed addressed under the heading of control of documents, control of products, and control of records. For engineering activities the control of documents and of products is more commonly grouped under the heading of configuration management. The GS-R-3 requirements of Ref. [2] for control of records also apply to documents under configuration management, although some records may be controlled separately from the configuration management systems, e.g., by a separate records management system. GS-G-3.1, References. [53] and GS-G-3.5, Ref. [64] provide additional recommendations on the four topics identified indicated in para. paragraph 2.38.

2.40. The Oobjectives of configuration management during the life cycle development processes for of I&C systems include the following:

- To identify Identification of all items under for which configuration management is required, i.e. documents, I&C products and associated records;.

- To provide Provision for secure storage and retrieval of configuration items;.

- To identify Identification of dependencies and relationships between items under configuration management;.

- To identify Identification of all changes of items under configuration management;.

- To prevent Prevention of the inadvertent and unauthorized modifications of items under configuration management;.

- To ensure Ensuring continued conformance with the design basies;.

- To define Specification of baselines for configuration baselines, i.e. the configuration of mutually compatible and consistent components of for an item in at every hierarchical level of configuration under configuration management.[5]

    Items for which a configuration baseline is established may include, for example, individual components, systems, or the overall I&C system. The baseline for any item will include all of the systems, and components that comprise the item.

- To ensure Ensuring consistency between the physical plant and the technical documentation;. and

---

[5] Items for which a configuration baseline is established may include, for example, individual components, systems or the overall I&C system. The baseline for any item will cover all of the systems and components that comprise the item.

Formatted: Font: 10 pt

Formatted: Font: 10 pt

- ~~To specify~~Specification of the current status of items under configuration management, e.g. their review or approval, or validation status.

2.41. Configuration management should include techniques and procedures for: analysing the effects of changes, approving changes, ensuring versions are combined correctly, releasing design documents and software for use, and establishing and maintaining a chronological record (e.g.~~,~~ what versions of tools are to be used at a particular point in design).

2.42. All I&C items and their associated documents should be designated, given a unique identification~~,~~ and placed under configuration management.

2.43. I&C items ~~are~~ include the deliverable delivered I&C system, any~~and~~ separately installed items ~~of a system~~that support the system or are necessary for the system to operate as intended, the documents and files that define all these items, and the software tools that might affect their quality ~~of the installed items~~.

2.44. I&C items typically include, for example:

- Procured items, reused items~~,~~ and newly developed items;

- Software components, such as source code and executable code, ~~HDL~~ hardware description languages, field programmable gate array (FPGA~~)~~ configuration data (known as 'bit stream') and software that is installed in plant equipment, including applications software, operating systems~~,~~ and support software;

- Hardware components~~,~~ and replaceable elements of such components;

- Firmware;

- Development documents such as: specifications, design documents, fabrication drawings and instructions, installation drawings and instructions, software and ~~HDL~~ hardware description languages;

- Equipment configuration data and configuration files, e.g.~~.~~ safe operating limits~~,~~; warning or alert limits~~,~~; setpoints and calibration constants; ~~and~~

- Physical tools and software tools that are used to produce, control, configure, verify or validate I&C components, including parameter settings used when employing ~~these~~ such tools.

2.45. Configuration management data should be used to verify that I&C items are assembled correctly and installed in the correct physical and topological location and that the intended software version is installed correctly.

2.46. ~~GS-R-3~~Reference [2], para.~~graph~~ 5.21 ~~requires~~states that:

"Records shall be specified in the process documentation and shall be controlled. All records shall be readable, complete, identifiable and easily retrievable."

2.47. Life cycle process records should be placed under configuration management.

2.48. The configuration management programme for life cycle records may be different from that used for I&C products.

2.49. Life cycle records to be placed under configuration control include any information on which the system safety analysis depends or which could affect safety during operation or maintenance, for example:

- Plans and procedures for life cycle activities;

- Safety demonstration plan;

- Analysis documents;

- Artefacts ~~Rr~~ecords that ~~documenting~~ the ~~system~~ safety demonstration and its supporting evidence, e.g. artefacts or records of: Assurance~~.;~~ ~~v~~Verification (including analysis and testing), ~~v~~Validation (including validation of requirements)~~.;~~ ~~p~~Process assessment and audit~~.;~~ ~~a~~Authenticity~~.;~~ ~~i~~Integrity, and ~~t~~Traceability;

- Records of verification and validation activities;

- Test specifications, procedures, plans, and results;

- Limiting settings of safety systems ~~settings~~ and the methodology for establishing limiting settings of safety systems ~~settings~~;

- ~~System integration~~ Pprocedures, plans and results relating to system integration;

- ~~Process~~ Documents relating to review and audit ~~documents~~of processes;

- Matrices for supporting ~~Requirements~~ traceability ~~matrices~~of requirements;

- Maintenance and operating procedures;

- Technical aspects of purchasing specifications for equipment and spares;

- Qualification records; ~~and~~

- Documentation ~~on~~of I&C systems and components ~~documentation, (~~see para.~~graph~~ 2.910).

2.50. The identification of items under configuration management should include the revision ~~level~~number.

2.51. Configuration control ~~applies~~ should be applied to the ~~original~~ initial development of I&C systems, changes made during development and ~~the~~ modifications after ~~it has~~they have been placed in service.

2.52. The configuration management process should maintain relevant information for each item under configuration management.

2.53. Information ~~to~~ that ~~should~~might be recorded ~~might~~ includes, for example, when the item was first considered to be completed, what changes were incorporated in the various versions including difference reports where appropriate, the dependencies on other items under configuration management, the item's current approval status, and the persons responsible for creating, reviewing and approving it.

2.54. The identity of software installed in I&C equipment and the values of configuration data should be retrievable from the I&C equipment itself.

2.55. The ability to retrieve the identity of installed items and the values of configuration data will support verification that the devices are properly configured. The installation of ~~A~~automatic checking features or software tools may assist in this verification.

I&C systems hazard analysis

2.56. For the overall I&C architecture, a hazard analysis should be performed to identify conditions that might compromise the defence -in -depth or the strategy for diversity ~~strategy~~ of the plant design.

2.57. For each safety system~~s~~, a hazard~~s~~ analys~~ie~~is should be performed to identify conditions that might degrade the performance of ~~their~~ its safety function.

2.58. Hazards ~~to~~ that should be considered include internal hazards and external hazards, failures of plant equipment~~,~~ and I&C failures or spurious operation due to hardware failure or to software errors. ~~Also included are c~~Contributory hazards due to unwanted interactions should also be considered.

2.59. The hazard analysis for I&C system~~s~~ ~~hazard analysis~~ should consider all plant states and operating modes, including transitions between different operating modes. Degraded states should also be included.

2.60. The initial results of the I&C system hazard analysis should be available before the design basis for the overall I&C is completed.~~The design basis for the overall I&C should not be completed until T~~the initial results of the I&C system hazard analysis ~~should be~~are available before the design basis for the overall I&C is completed.

2.61. The hazard analysis should be updated at every phase of the development lifecycle, including (but not limited to) the design of the overall I&C architecture, and the specification of requirements, design, implementation, installation and modification of safety systems.

2.62. The intent of updating the hazard analysis is to identify hazards that may be caused by specific characteristics of I&C safety systems, by interaction between I&C safety systems and the plant, and by interaction of I&C safety systems with other I&C systems, regardless irrespective of their safety classification.

2.63. Measures should be taken to eliminate, avoid, or mitigate the consequences of identified hazards that can could degrade the performance of system functions.

2.64. Measures to eliminate, avoid, or mitigate the consequences effects of hazards might, for example, take the form of changes to the I&C requirements, design, or implementation of I&C systems or of changes to the plant design.

2.65. The methods selected for hazard analysis methods should be appropriate for the item being analysed.

Verification and validation

2.66. Each phase of an I&C the development process of an I&C system uses information developed in earlier phases, and provides results to be used as the input for later phases.

2.67. The results of each life cycle phase in the development process should be verified against the requirements set by the previous phases.

2.68. A rRequirements tTraceability mMatrix can be used to document confirmation that requirements are satisfactorily met in each life cycle phase of the development process and or that appropriate action was taken where requirements were not satisfactorily met.

2.69. The overall I&C, each I&C system, and each I&C component should be verified to confirm it that implements all of theirthe requirements (both functional requirements and non-functional requirements) have been met, and to investigate determine whether anyfor the existence of undesirable behaviour that is not requiredexists (see paragraphs 2.129 to 2.143). The requirements defining the overall I&C, each I&C system, and each I&C component should be validated to confirm that they are fulfilled as intended. 2.70. Note that the term component includes hardware, software such as application software and firmware, and HDL descriptions.

2.701. Verification and validation should be carried out by individuals, teams, or organizational groups that are independent of the designers and developers.

2.712. Establishmenting of independence of verification and validation normally involves ensuring that the V&V teams, individuals, or organizational groups carrying out verification and validation:

- Have adequate technical competence and knowledge:;

- Can set their own scope:;

- Are not subject to pressure from the developers,;

- Are not subject to reductions in budget or to constraints in schedules constraints that would prevent them from completing their full scope of their review;, and

- Are allowed to submit their findings to programme management without adverse pressure from the development group.

2.72 3. The amount extent and type of independence of the verification and validation V&V should be suitable for the safety class of the system or component involved. 2.74. Verification and validation V&V may occur in parallel at different levels of independence (for example, verification and validation V&V carried out by testers independent from developers in the original development organis zation, plus and additional independent verification and validation V&V carried out by a separate organiz sation).

2.75 73. Verification and validation activities, including records of detected anomalies and their disposition, should be documented. If anomalies are detected in at the verification and validation V&V stage, the resulting design modifications and their implementation should be subject to the same verification and validation V&V process performed previously.

2.76 74. Technical communications between the verification and validation V&V teams, system integration teams, commissioning teams and the system designers and developers should be documented.

Use of insights from probabilistic safety analysis

2.77 75. SSR 2/1 Reference [1], para. graph 5.76 states:

"The design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and for all plant states, including shutdown, with particular reference to:

(a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;

(b) Providing assurance that small deviation in plant parameters that could give rise to large variations in plant conditions (cliff edge effects) will be prevented…..;

(c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified."

2.78 6. Insights gained from probabilistic safety assessments (PSAs) should be considered in the design of I&C systems.

2.7977. Detailed information on probabilistic safety assessment PSAs and the use of PSA results from probabilistic safety assessment during design can be found in SSG-3, Ref.s [124] and SSG-4, Ref. [135].

Safety assessment

2.8078. Safety assessment of I&C should be conducted in accordanceing withto the requirements of GS-R-4, Ref. [57] and the recommendations of SSG-2, Ref. [162], and SSG-3, Ref. [14].

2.8179. Design analyses and verification and validation, should be performed to confirm that all design basis requirements of the overall I&C architecture and each individual I&C system are met.

2.8280. Paragraph 3.14 recommends topics to be considered in the design basis requirements for the overall I&C architecture and all I&C systems. Paragraph 3.16 recommends additional topics to be considered in the design basis requirements for safety systems.

2.8381. Typical design analysis, verification and validation techniques include, for example, the following:

- Traceability analysis. Traceability analysis is typically used to confirm implementation and validation of requirements.

- Failure mMode and eEffects aAnalysis (FMEA). Failure mode and effects analysis FMEA is often used to confirm compliance with the single failure criterion and that all known failure modes are either self-revealing or detectable by planned testing.

- Analysis of Ddefence -in -dDepth and Ddiversity aAnalysis. Analysis of Ddefence -in -Ddepth and dDiversity Analysis is one of the means of investigating vulnerability of safety systems to common cause failure. See NP-T-3.12, Ref. [112], which gives provides additional information on this topic.

- Reliability analysis. Reliability analysis uses statistical methods to predict the reliability of systems or components. Commonly used reliability analysis techniques include parts count analysis, parts stress analysis, life data analysis, reliability block diagrams, and fault tree analysis.

- Validation. Validation testing involves deterministic techniques and may include statistical techniques.

- Security testing. Security testing usually involves requires input from a vulnerability assessment and should is used to confirm the use of security good practice in security.

- Analysis to confirm that items have been designed for reliability. Such analysis is used to confirms that a design incorporates features that are known to promote high reliability such as, for example,

redundancy, compliance with the single failure criterion, testability, fail-safe design~~,~~ and rig~~ou~~rous qualification.[6]

~~For I&C systems a combination of qualitative analysis, quantitative analysis, and testing is usually needed to verify compliance with reliability requirements.~~

> **Formatted:** Indent: Left: 0.63 cm

- Confirmation of functional requirements for various operating modes of the I&C system ~~operating modes~~. This includes analysis of correct system behaviour during and after power interruptions, restart or reboot, and other transition points. Calendar time changes (e.g. daylight saving time, leap years~~, etc.~~) are examples of other transition points.

2.84~~82~~. Each assumption ~~of~~ used in an analysis should be stated~~,~~ and use of the assumption should justified ~~in that analysis~~.

2.85~~3~~. The methodology for any analysis conducted should be thoroughly defined and documented together with ~~analysis~~ inputs into the analysis, results from the analysis~~,~~ and the analysis itself.

2.86~~84~~. Given the current state of the art, for an individual system ~~which~~ that is specified and designed in accordance with the highest quality criteria, a figure of the order of 10^{-4} to 10^{-5} failure/demand may be an appropriate overall limit to place on the reliability that may be claimed in the probabilistic safety analysis, when all of the potential sources of failure (excluding cyber security related ~~ones~~sources of failure) ~~due to~~associated with the specification, design, manufacture, installation, operating environment~~,~~ and maintenance practices~~,~~ are taken into account. This figure may need to include the risk of common mode failure in the redundant channels of the system, and applies to the whole of the system, from sensors~~,~~ through processing~~,~~ to the outputs to the actuated equipment. Claims for better reliabilities than this are not precluded, but will need special justification, with account tak~~ening into account~~ all of the factors mentioned.

2.87~~85~~. Any reliability claims for I&C systems should be substantiated and should be within justifiable limits (Annex III describes limits accepted ~~by~~ in some ~~Member~~ States).

2.88~~86~~. During the design and implementation process, the interaction of each I&C system with the plant should be reviewed regularly against the plant safety requirements and against the requirements of ~~SSR2/1,~~ Ref. [1].

2.89~~87~~. Where any conflict with these requirements is found, the design and implementation should be corrected appropriately.

Documentation

2.90~~88~~. I&C documentation ~~should~~:

---

[6] For I&C systems, a combination of qualitative analysis, quantitative analysis and testing is usually needed to verify compliance with reliability requirements.

> **Formatted:** Font: 10 pt

a. Should Pprovide the a means of communicating information between the various phases of and the various parties involved in the design process;

b. Should Pprovide a record showing that all requirements have been correctly interpreted and fulfilled in the installed system;

c. Should Ccommunicate information that is essential to the operationally essential and safety design related information to the plant operating personnel;

d. Should Pprovide a foundation for maintenance of the plant and I&C systems maintenance and for potential future revisions to the design;

e. Should Bbe traceable throughout the I&C life cycle phases;

f. Should Bbe controlled under a configuration management system, and;

g. Should Bbe unambiguous, complete, consistent, well structured, readable, understandable to their target audience (e.g., domain experts, safety engineers, software designers), verifiable, and maintainable.

2.9189. Adequate documentation will facilitate operation, surveillance, troubleshooting, maintenance, future modification or modernization of the system, as well as training of plant and technical support staff.

2.9290. The operating organization should establish or be provided with documentation for I&C systems and components that, as a minimum, cover the following topics:

a. Design requirements;

b. Functions and functional design;

c. Principles of operation;

d. The role of the system role in the overall plant concept;

e. Design features, including identification of features that are important to safety;

f. As-built design and configuration documentation;

g. As-built location of systems and their main components, including sensors and actuators;

h. Interfaces with and dependencies on other plant systems;

i. Facilities and requirements for surveillance, testing, diagnostics, maintenance, and operation;

j. Documentation of tTest procedures and results;

k. Equipment qualification;

l. The design and development process and quality requirements followed in the design;

m. Strategies for all phases of testing, including commissioning;

n. Design and development verification and validation methods and results;

o. Operating instructionsprocedures all normal operation states and modes;

p. Emergency operating procedures, and severe accident guidelines, to cover all normal operation modes and postulated accident scenarios and design extension conditions;

q. Recommendations and purchasing specifications for provision of spare parts and components.

r.   Security design features and their application.[7]

~~If the design makes use of assumptions about the operating organization's, operational security policies and practices (including computer security), these are to be communicated to the user. It might be appropriate to include elements of such descriptions in separate documents so that their distribution can be more restricted than other system information.~~

2.9391. Documentation of ~~acquisition and supply~~ processes and requirements for acquisition and supply, design, fabrication activities, software code, and verification and validation should be available for assessment by the operating organization, regulatory ~~authorities~~body, or independent third parties acting for these organizations (see para~~graph~~s 9.995 to 9.10298).

LIFE CYCLE ACTIVITIES

Requirement specification

2.9442. The requirements for the overall I&C, each individual I&C system~~,~~ and I&C components should ~~have~~ be documented ~~requirements~~ in an appropriate form.

2.9593. The combination of ~~the~~ requirements of the full set of individual I&C systems should fulfil the design basis established for the overall I&C.

2.9694. The Rrequirements ~~specifications~~ for the overall I&C and each individual I&C system should be derived from the I&C design basis.

2.9795. Section 3 discusses the derivation and content of the overall I&C design basis.

2.9896. The system and component requirements should specify, as applicable, the following:

a.   What each individual I&C system or component is to do:~~;~~

b.   The relations between inputs and outputs for each function in each plant state and each plant operating mode;

c.   The minimum precision and~~,~~ accuracy~~,~~ and the maximum time response for measurements, control functions, and displays;

d.   The system interfaces (e.g.~~,~~ between the system and the operator, and with other systems);

e.   Self-supervision features including their required timing performance (including fault detection times and recovery times);

f.   The actions to be taken by the I&C system upon detection of faults by means of self-supervision;

---

[7] If the design makes use of assumptions about the operating organization's operational security policies and practices (including policies and practices relating to computer security), these are to be communicated to the user. It might be appropriate to include elements of such descriptions in separate documents so that their distribution can be more restricted than other system information.

g. Security features (such as validity checks, specific computer security controls, and features that allow systems to inherit the security controls in their environments and to inherit access privileges);

h. The level of reliability and availability to be achieved and any supporting requirements necessary to ensure that this is achieved;[8]

The level of reliability and availability might be defined quantitatively, or qualitatively for example in terms of the supporting requirements referred to above, e.g., requirements to implement specific reliability strategies, requirements on development process characteristics or requirements to comply with specified standards.

i. Facilities and features required for maintenance;

j. Design constraints.[9]

Examples of design constraints include constraints to support independence or diversity requirements.

k. Safe response to particular failure modes.;

l. Robustness to the full range of operating environments associated with normal and accident plant conditions on the plant and foreseeable internal and external hazards.

2.9997. Where design constraints are necessary, they should be specified, justified and traceable.

2.10098. Security design requirements for digital systems should take account of the results of a security risk assessment and should be consistent with the characteristics of the operating organization's security policies.

2.10199. Specific processes should be used to manage requirements throughout the life cycle and to ensure that all requirements are fulfilled, verified, validated and implemented.

2.102100. Requirements engineering is a specific process for enassuring that the safety goals of I&C systems are included addressed byin the design.

2.103101. Requirements should be documented established and documented using a predetermined combination of techniques commensurate with the system's importance to safety.

2.104102. Techniques for establishing and documenting requirements might, for example, include the use of specification languages with that have well-defined syntax and semantics, models, analysis, and review.

---

[8] The level of reliability and availability might be defined quantitatively, or qualitatively, for example in terms of the supporting requirements referred to above, e.g. requirements for implementation of specific reliability strategies, requirements on characteristics of the development process or requirements for compliance with specified standards.

[9] Examples of design constraints include constraints to support independence or diversity requirements.

2.~~105~~103. As far as possible, requirements should be written in terms of what needs to be achieved rather than how they are to be designed and implemented.

2.~~106~~104. Requirements should be described in terms understandable to all parties concerned (e.g.~~,~~ the licensee, suppliers~~,~~ and designers).

2.~~107~~105. Documentation of ~~R~~requirements ~~documentation~~ should refer to, include~~,~~ or be complemented by additional information, e.g.~~,~~ background information for specific requirements, risk considerations, recommendations for the design of functions or safety features, to the extent necessary to ensure ~~it~~ the ~~documentation~~requirements are fully understood by their ~~is understandable by to its~~ target audience.

2.~~108~~106. Requirements that have a potential impact on safety should be identified as such.

2.~~109~~107. The origin of and rationale for every requirement should be defined, to facilitate verification, validation, traceability to higher level documents and demonstration that all relevant design basis requirements have been taken into account~~ed for~~.

Selection of pre-developed items

2.~~110~~108. Pre-developed items should be appropriately qualified in accordance with the guidance given in para~~graphs~~ 6.79~~8~~ ~~through~~ to 6.135~~4~~.

2.~~111~~109. Pre-developed items ~~might be~~include hardware devices, pre-developed software ~~(PDS)~~, commercial off the shelf ~~(COTS)~~ devices, digital devices composed of both hardware and software, hardware devices configured with hardware definition language or pre-developed functional blocks usable in ~~a HDL~~ hardware description language.

2.~~112~~110. ~~NP-T-3.12,~~ Ref~~.~~erence [1~~2~~1]~~,~~ ~~gives~~ provides more detail about the use of commercial off the shelf ~~COTS~~ devices.

2.~~113~~111. Any functions of a pre-developed item that are not used in implementing an I&C safety system should be shown not to interfere unacceptably with the system's safety functions.

2.~~114~~112. Where feasible, pre-developed items should be configured such that unused functions are disabled.

2.~~115~~113. Often~~,~~ ~~the~~ pre-developed items selected are commercial off the shelf ~~(COTS)~~ devices. Use of commercial off the shelf ~~COTS~~ devices might reduce costs and design effort. Furthermore, there may be no ~~nuclear specific~~ device specific for nuclear power plants available and use of a well-proven commercial product could be more effective or more safe than development of a new item.

2.~~116~~114. Commercial off the shelf ~~COTS~~ devices tend to be more complex, may have unintended functionalities and often become obsolete in a shorter time. They will often have functions that are not needed in the nuclear power plant application. Qualification of a commercial off the shelf ~~COTS~~ device could be more difficult because commercial development processes may be less transparent

and controlled than those described in this Safety gGuide. Often qualification is impossible without cooperation from the vendor. The difficulty with associated with acceptanceing of a commercial off the shelf COTS device may often be lie with the unavailability of the information to demonstrate quality and reliability.

2.117115. In the process of deciding whether to use commercial off the shelf COTS devices or not, the licensee should pay attentionconsider to the maintenance of their qualification during the lifetime of the plant lifetime.

2.118116. There might, fFor example, there might be frequent design changes of the product line, such as, changes to subcomponents, new firmware versions, new manufacturing processes, or new software versions. This may cause challenges to the vendor as well as the plant configuration management in order to properly identifying such modifications, especially with regard to I&C maintenance and management of spare parts management. In some cases, operating organizations have purchased a '"lifetime supply'" of spares of a specific version to avoid the possibility that a specific component or version may becomes unavailable for purchase.

2.119117. Pre-developed items should have documentation that gives the information necessary for their use in the I&C system.

Design and implementation of I&C systems design and implementation

2.120118. The design of the overall I&C architecture and the individual I&C systems should result from a systematic, step-wise decomposition of required functionality plus other requirements.

2.121119. The system requirements that are to be satisfied by an I&C system should be allocated to an appropriate combination of hardware, devices configured with HDLhardware description language, and software (if present).

2.122120. Hardware might include application specific integrated circuits specific to certain applications. Software might include pre-existing software and firmware, such as the operating system, software to be developed or software to be produced by configuring pre-developed software. The refined requirements might also have to take into account for lower level design decisions made for in respect of parts outside the I&C system, e.g. the type and performance of actuated devices.

2.123121. The implementation of requirements that are not important to safety should be shown not to interfere with functions important to safety.

2.124122. Design rules should be established to ensure that the internal logic of each I&C system is amenable to verification and validation.

2.125123. The design should take into account for I&C parameters that need to be configurable or verified and validated during operation and should provide the means to do so (e.g., trip settings for the reactor protection system trip settings, calibration constants and software configuration settings).

System integration

2.126124. System integration should:

a. Address all interfaces between the components being integrated, such as between the hardware and software or between software modulesChallenge all integration interfaces such as hardware software or software module to module;

b. Confirm that the requirements onfor the interfaces requirements between the various components of the system are satisfiedmet; and

c. Confirm that the components, subassemblies and subsystems operate as designed in the integrated system to enable the system to meet its specified requirements, including requirements covering out-of-range values, exception handling, and timing related requirements.

2.12775. A consistent configuration of verified modules (hardware and software) should be available prior to the beginning of system integration.

2.12688. Software tools are typically used to control the issue of modules for assembly into system components and to control the software build used for system validation. Software tools are also used and for on-site use in operation to facilitate configuration control and traceability between installed components and validated components.

2.12997. A documented traceability analysis should be used to demonstrate that the system integration is complete with respect to the system design specification and that the objectives of para.graph 2.12645 have been met.

System validation

2.130128. System validation should be performed for each individual I&C system and for the integrated set of I&C systems.

2.131129. For the purpose of this Safety Gguide, system validation ends when installation of the system into the plant is complete. However, If sSome additional elements of system validation may need to be performed after the system is installed in the plant. These may need to be included in commissioning tests provided that the results are included into validation test records and that independence, as defined in paras 2.71 70 and 2.7271, is maintained between the design team and the validation team.

2.132130. The system that is subjected to testing for the purposes of validation testing should be representative of the final configuration of the I&C system at the site.

2.13331. The software that is subjected to system validation should be identical to the software that will be used in operation.

2.134132. System validation should be used to demonstrate that the system meets all requirements under all possible interface conditions and all possible load conditions.

2.135133. Modes of operation and interactions between I&C systems and the plant that could not be readily tested during system validation should be tested during commissioning, or should be validated through supplementary analysis.

2.136134. System validation should cover the following:

   a. All parts of the system;

   b. The full ranges of interface signals[10] including out-of-range values;. Interface signals include, for example, inputs and outputs to or from other systems, sensors, actuators, and operator interfaces.

   c. Exceptions handling;

   d. Setpoint accuracy and hysteresis;

   e. All modes of plant and system operation including transitions between modes;

   f. Recovery after power failure;

   g. Timing; and

   h. Robustness and fault tolerance.

2.13775. The system validation tests should involve variation of all inputs, i.e., dynamic testing should be used.

2.138136. The dynamic tests should use realistic scenarios that are representative of plant parameter variations that would place demands on the I&C system and that are based on an analysis of the possible plant scenarios.

2.139 137 The functional tests should be designed to cover all behaviours allowed by the functional requirements. The structural coverage of functional tests structural coverage, resulting from analysis of these functional requirements, should be justified taking account of the functional requirements.

2.140138. Validation testing using statistical techniques should be considered.

2.141139. The use of simulators for system validation should be considered.

2.142140. The system operation manuals and appropriate parts of the maintenance manuals should be validated during system validation as far asto the maximum extent possible, during system validation.

2.143141. A documented traceability analysis should demonstrate that the system validation is complete with respect to the specification of system requirements specification and that the objectives of paragraphs 2.134 132 and 2.136 134 have been met.

2.144142. The complete set of test documentation should be sufficient to enable the testing process to be repeated with confidence that consistent satisfactory results will be achieved for any repeated and previously satisfactory test.

---

[10] Interface signals include, for example, inputs and outputs to or from other systems, sensors, actuators, and operator interfaces.

Installation, overall I&C integration, and commissioning

2.145143. The I&C system should be installed in the plant in accordance with the approved design.

2.146144. Equipment should be inspected on receipt inspection, or commissioning tests should be carried out to verify that the systems and components have not suffered damage during transportation.

2.147145. The following paragraphs discuss set out considerations in implementing the guidance of IAEA NS-G-2.9, Ref. [157] for I&C systems.

2.148146. Commissioning should progressively integrate the I&C system with the other components and other plant items, and should verify that they are in accordance with design assumptions and that they meet the functional criteria and performance criteria.

2.149147. Testing within the plant environment is an important part of commissioning.

2.150148. Commissioning should give particular attention to verification of interfaces with external systems interfaces and to the confirmation of the correct performance with the interfacing equipment.

2.151149. During In the commissioning period all I&C systems should be operated for an extended time under operating, testing and maintenance conditions that are as representative of the in-service conditions as possible.

2.152150. The validation of operation manuals and appropriate parts of the maintenance manuals should be completed before commissioning is completed.

2.153151. Before I&C systems are declared operable, relevant life cycle planned activities should be completed, traceability should be established from requirements to installed systems and their build and design documentation should be complete and reflect the as-built configuration.

Operation and maintenance

2.154152. Maintenance and surveillance of I&C systems should be performed in accordance with the guidance of IAEA NS-G-2.6, Ref. [168], which provides guidance on planning, organizsational aspects, and implementation of maintenance and surveillance, including calibration, of I&C systems.

2.155153. The following paragraphs discuss set out considerations in implementing the guidance of NS-G-2.6, Ref. [168] for I&C systems.

2.156154. Changes to I&C system parameters should be undertaken using appropriate means and facilities.

2.157155. Human performance monitoring of the operation and maintenance of the I&C system should be performed monitored to document operating experience that may indicate a need of for modifications to reduce human error.

2.158156. Adequate quantities of spare parts should be available for operation and maintenance throughout the intended service lifetime (e.g. based on I&C design, component reliability and future availability of replacement components and vendor support).

Modifications

2.159157. The following paragraphs discuss set out considerations in implementing the guidance of NS-G-2.3, Ref. [910] for I&C systems.

2.160158. The design of I&C upgrades and modifications to I&C should consider:

a. The lLimitations due toresulting from the physical characteristics of the installed plant, which that effectively restrict the design options for I&C systems;

b. The possible need to maintain consistency between the design of replacement equipment and existing I&C equipment in order to, for example, reduce the complexity of the overall operator interface and maintenance tasks of the plant;

c. Practical considerations with respect to the equipment or technology that is commercially available and the prospects for securing support of such equipment and technology by manufacturers or third parties for the installed lifetime of the equipment;, and

d. The need to update existing design documentation.[11] The design documentation for older systems might be incomplete or inaccurate. Consequently major modifications to or replacement of such systems might require some degree of 'reverse engineering' to recreate the original design bases and specifications.

2.161159. When an I&C system is modified or is part of an upgrade, the level of rigour to be applied in justifying and executing the change should be established beforehand.

2.162160. The level of rigour should be based upon the role and function of the affected systems' role and function in ensuring the safety of the nuclear power plant, in association with the existing systems that will remain in operation after the work. This also applies to changes to software tools.

2.163161. Development of the modification or upgrade of I&C systems should follow a defined specified life cycle.

2.164162. The complexity of the life cycle process needed for modifications is related to the complexity and safety significance of the modification.

2.165163. The life cycle for even the simplest changes should include at least the phases of the individual system life cycle shown in Fig.ure 2, including verification and validation V&V after each I&C modification.

2.166164. Interim configurations of the hHuman-mMachine iInterface configurations that represent a transition between new and existing I&C might need further HFE analysis from a human factors

---

[11] The design documentation for older systems might be incomplete or inaccurate. Consequently major modifications to or replacement of such systems might require some degree of 'reverse engineering' to recreate the original design bases and specifications.

engineering perspective to accommodate the use of temporary equipment or procedures. Enhancements to the interface with the operator interface might lead to an increase in errors by operations personnel and maintenance personnel for some time after the change. In some cases incremental training might be necessary.

2.167165. When an I&C system is replaced, consideration should be given to running the new I&C system in parallel with the old system for a probationary period, i.e., until sufficient confidence has been gained in the adequacy of the new system should be considered. The equivalent of parallel operation might be possible by installing new redundant equipment in one train at a time.

2.168166. When considering the parallel operation of I&C systems, the disadvantages of operational problems and complexity should be weighed against the gain of in confidence, and the risks should be evaluated.

2.169167. The consequences of an update or change in software tools update or change between the time of initial development and the modification may be significant and should be made subject to impact assessmentassessed for its impact (for example, a compiler upgrade could invalidate previous results of analysis or verification results concerning the adequacy of the compiler).

3. DESIGN BASIS FOR I&C DESIGN BASESSYSTEMS

IDENTIFICATION OF I&C FUNCTIONS

3.1. SSR 2/1 Rrequirement 4 [1] states:

> "Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases."

3.2. SSR 2/1 para. paragraph 4.1 [1] states:

> "A systematic approach shall be taken to identifying those items important to safety that are necessary to fulfil the fundamental safety functions and to identifying the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions for all plant states."

3.3. SSR 2/1 para. paragraph 4.2 [1] states:

> "Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled."

3.4. Required safety functions are derived from the nuclear power plant design process (see section 4 of SSR 2/1Ref. [1]) and a systematic approach is required to be followed to allocate these functions to plant structures, systems and components.

3.5. The required functions (and corresponding non-functional requirements for properties such as safety, security, and timing constraints) of the I&C systems should be determined as part of the design process for the nuclear power plant design process.

3.6. The functions allocated to the I&C systems include those functions that provide information and control capabilities relevant to operating operation of the plant in the various modes of operational states and in accident conditions. The objectives of these functions, corresponding to the concept of defence in depth, are to:

- Prevent deviations from normal operation;.

- Detect failures and control abnormal operations;.

- Control accidents that are within the plant design basis;.

- Control the consequences of design extension conditions;. and

- Mitigate the radiological consequences of significant releases of radiationaccidents.

CONTENT OF I&C DESIGN BASIES FOR I&C SYSTEMS

3.7. SSR 2/1 Requirement 14 [1] states:

"The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant."

3.8. SSR 2/1 para. paragraph 5.3 [1] states:

"The design basis for each item important to safety shall be systematically justified and documented. The documentation shall provide the necessary information for the operating organization to operate the plant safely."

3.9. The overall I&C architecture and each I&C system should have a documented design basis.

3.10. The overall I&C architecture is the organizational structure of the plant I&C systems. The overall I&C architecture of a nuclear power plant includes multiple I&C systems, each playing specific roles.

3.11. The design basis identifies functions, conditions and requirements for the overall I&C and each individual I&C system. This information will is then be used to categorize the functions and assign them to systems of the appropriate safety class [17].

3.12. Note that in some instances, I&C system requirements will be identified as the nuclear power plant design and design basis for the nuclear power plant are developed. Thus, the complete content of the I&C design basies might not be available at the beginning of the project.

3.13. The development of the I&C design basis should be derived from the plant safety design basis documents, ~~which~~ and should provide the following information:

    a.   The defence-in-depth concepts of the plant;~~,~~

    b.   The safety functions to be provided (see para.~~graph~~ 3.11);~~,~~

    c.   The safety categorization, and the functional and performance requirements of the plant functions important to safety;~~,~~

    d.   The ~~priority~~ principles concerning priority between automatically and manually initiated actions; and between automatic actions where more than one system can ~~activate~~ actuate a device or function;~~,~~

    e.   ~~Member State~~National requirements for licensing of I&C ~~licensing~~systems;~~,~~

    f.   ~~Member state~~National requirements for safety classification of I&C;~~ safety classification,~~

    g.   ~~Member State~~National requirements with respect to operational requirements;~~,~~

    h.   The analysis and identification of digital I&C systems critical to facility safety and security functions~~Identification of critical digital assets for computer security~~,

    i.   ~~Computer security v~~Vulnerability~~Risk~~ assessments and impact analyses for computer security;~~,~~

    j.   Information and control needs and allocation;~~,~~

    k.   The ~~o~~Operating philosophy at the plant;~~,~~

    l.   Human reliability analysis;~~,~~

    m.   Roles of ~~O~~operating personnel;~~ roles, and~~

    n.   Staffing levels.

3.14. In addition to the recommendations given in para.~~graph~~ 3.15, the design basis for the safety systems should specify the following:

    a.   The limiting values of parameters required to actuate safety systems (analytical limits, see para.~~graph~~ 6.209 and Fig.~~ure~~ 3);

    b.   Variables and states that are to be displayed so that ~~the~~ operators can confirm the operation of protective ~~system~~ functions of the systems;

    c.   The justification for any safety actions that are not automatically initiated, including:

        ~~1.~~i.   The occasions, incidents, time durations and plant conditions for which manual control is allowed;

        ~~2.~~ii.   The justification for permitting initiation, or control after initiation, solely by manual means;

        ~~3.~~iii.   The range of environmental conditions of the operators' environment when they are expected to take manual action ~~during plant~~in operational states and in accident conditions;

4.iv.   Confirmation that information the operators are to take into account when performing manual actions will be displayed in appropriate locations and will have performance characteristics necessary to support the operator actions;

i.v.   The conditions under which bypass of I&C safety functions are to be permitted;

ii.vi.   The conditions which that must be satisfied before an actuated protective system can be reset; and

iii.vii.   The requirements for diverse functions to mitigate the consequences of common cause failure.

3.15. The design basies for I&C systems should specify the necessary capability, reliability and functionality for the overall I&C and for each individual I&C system, including the following:

   a.   All functional requirements, for example:

      1.i.   The plant operational states in which each I&C system is required;

      2.ii.   The various plant configurations for which each I&C system is to be operational;

      i.iii.   The functional requirements[12] for each plant state, for each plant operational mode and during for extended shutdown;Note: Functional requirements define, for example, the transformations of inputs to outputs and the actions taken.

      3.iv.   The safety significance of each required I&C function;

      4.v.   The postulated initiating events (PIE) to which the system is to respond;

      5.vi.   The role of each individual I&C system role in the concept of defence -in -depth concept of the overall I&C architecture;

      6.vii.   The variables, or combination of variables, to be monitored;

      7.viii.   The control and protection functions required, including identification specification of actions that are to be performed automatically, manually, or both, and the location for the controls;

      8.ix.   The required ranges, rates of change, accuracy, quantization of digital representations, precision in calculation precision, and required response times for each I&C safety function;

   b.   All requirements imposed to achieve the needed necessary level of reliability and availability, for example:

      1.i.   The requirements for independence of safety functions;

---

[12] Functional requirements define, for example, the transformations of inputs to outputs and the actions to be taken.

2. ii.   The requirements for periodic testing, self-diagnostics, and maintenance;

i. iii.   The qualitative or quantitative reliability and availability goals;[13] ~~System and component reliability and availability limits may be specified using probabilistic criteria, deterministic criteria (e.g., compliance with single failure criterion or specific procedures and verification methods for software), or both.~~

3. iv.   The ~~failure~~ behavioural requirements on failure ~~from~~ of the process and the plant safety analysis;

c.   All requirements imposed to achieve the ~~needed~~ necessary level of security, for example:

1. i.   The security and operational constraints that are to be observed in the design; ~~and~~

2. ii.   The security measures to be implemented.

d.   All requirements that are ~~needed~~ necessary to ensure equipment is appropriately qualified, for example:

1. i.   The design criteria including ~~identification~~ specification of standards with which the I&C systems should comply;

2. ii.   The plant conditions with the potential to ~~functionally~~ degrade the performance of systems in carrying out their functions and the provisions to be made to retain the necessary capability;

3. iii.   The range of internal and external hazards (including natural phenomena) under which the system is required to perform functions important to safety;

i. iv.   The range of plant environmental conditions[14] under which the system is required to perform functions important to safety; ~~Plant environmental conditions of concern include the normal conditions, abnormal conditions, and the extreme conditions that I&C equipment might experience during design basis accidents, internal events, or external events. Any interactions across I&C systems, and particularly between components qualified to different degrees, may compromise defence-in-depth requirements if not fully accounted for.~~

4. v.   The limitations on materials to be used;

---

[13] ~~System and component~~ R̲eliability and availability limits for systems and components may be specified using probabilistic criteria, deterministic criteria (e.g.~~,~~ compliance with the single failure criterion or specific procedures and verification methods for software), or both.

[14] Plant environmental conditions of concern include the normal conditions, abnormal conditions, and the extreme conditions that I&C equipment might experience during design basis accidents, internal events, or external events. Any interactions across I&C systems, and particularly between components qualified to different degrees, may compromise the requirements for defence -in -depth ~~requirements~~ if not fully taken into account~~ed for~~.

    5.vi.   The constraints imposed by the physical plant design and layout, with including constraints those on equipment location, cable access and power sources; and

    6.vii.   The physical location of and interfaces between equipment.

3.16. The items above may be specified in either the overall I&C design basis or the design baseis for individual systems design bases. For some items it might be appropriate to specify generic requirements in the overall I&C design basis and to provide more detail in the design basis for individual systems design bases. In any case. it is essential that the design bases for the overall I&C and for the individual systems should be consistent with each other and that the relationship and interfaces between the different design bases should be readily understandable.

4. ~~GUIDANCE FOR~~ I&C ARCHITECTURE

ARCHITECTURAL DESIGN

4.1. The architectural design for the overall I&C architectural design establishes:

- The I&C systems that comprise the overall architectureThe high level definition of the I&C systems;

- The tiered structureorganization of these systems;

- The assignment allocation of I&C functions to these systems:, and

- The communications betweeninterconnections across the I&C systems and the topology ofrespective interactions allocated and prohibited communication links;

- The design constraints (including prohibited interactions and behaviours) allocated to the overall architecture;

- The definition of the boundaries among the various I&C systems.

4.2. The architectural design for Iindividual I&C systems architectural design establishes:

- The composition-decomposition relationships through all levels of integration down to the indivisible, individual itemThe subsystems that will compose make up the I&C system

- The individual I&C items that will compose make up these subsystems;

- The hierarchical structure of subsystems and the hierarchical structure of individual I&C items within subsystems;

- The assignment allocation of I&C functions to individual I&C items, behaviours, constraints, and (derived) quality requirements to each item at each level of integration;

- Rules of composability and composition to assure that the composition of behaviours at one level of integration satisfies the behaviours required at the next higher level of integration and does not introduce other behaviours;

- The interconnections across items at each level of integration and across levels of integration and the respective interactions allocated and prohibited~~The layout of communications between items and subsystems within the individual I&C system; and~~

- The partitioning to avoid unnecessary ~~complexity of systems~~ complexity and unnecessary interactions between individual ~~elements of each I&C system~~ elements;

- The design constraints (including prohibited interactions and behaviours) allocated to each individual I&C system.

4.3. Modern I&C systems are more interconnected and more difficult-to-analy~~z~~se (and thus safety assurance is more difficult ~~to assure~~ than ~~were the~~ was the case for earlier generations of I&C systems). A well designed I&C system architecture will ensure defence-in-depth and diversity and will localize and contain difficult to analyse features in systems so that ~~where it can be assured that~~ these features ~~will~~ do not make assurance ~~render negatively influence~~ of plant safety too difficult ~~unassurable~~.

4.4. The overall I&C architecture and the individual I&C system architectures should satisfy the plant requirements, including requirements for system interfaces and requirements for properties such as safety, security, verifiability, analy~~z~~sability and timing constraints.

4.5. SSR 2/1 Requirement 7 [1] states:

"The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable."

4.6. ~~INSAG 10,~~ Ref~~erences.~~ [18~~9~~] and ~~INSAG 12, Ref.~~ [20~~19~~] explain the concept of defence-in-depth and describe the levels of defence-in-depth.

4.7. The overall I&C architecture should not compromise the concept of defence-in-depth and the diversity strategies of the design of the plant ~~design~~.

4.8. The overall I&C architecture should define the concept of defence-in-depth and the diversity strateg~~ies~~ to be ~~implemented~~ applied within the overall I&C.

4.9. The overall I&C architectural design also establishes the level of independence between the I&C systems that support the different levels of the plant's concepts of defence in depth and diversity ~~concepts~~.

4.10. Defence-in-depth within the overall I&C architecture is achieved by means of independent lines of defenc~~s~~e so that the failure of one line of defence is ~~mastered~~ compensated for by the following one.

CONTENT OF THE OVERALL I&C ARCHITECTURE

4.11. The overall I&C architecture ~~should~~:

a. Should Iinclude all I&C functions needed necessary to fulfil the plant design basis;

b. Should Iidentify topics that are to be dealt with consistently across all I&C systems;[15]

b. ~~Topics to be considered consistently across all I&C systems include, for example: implementation of the plant operational concept, application of human interface design standards, constraints on cable routing, grounding practices and alarm management philosophy.~~

> **Formatted:** List Number, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.27 cm

c. Should Iidentify the individual I&C systems that will be included in the overall I&C architecture in order to:

1.i. Support the plant concepts of defence -in -depth and diversity conceptsapplied at the plant;

2.ii. Support the overall I&C design basis requirements for independence for the overall I&C; and

> **Formatted:** Outline numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Right + Aligned at: 1.02 cm + Tab after: 1.52 cm + Indent at: 1.52 cm

3.iii. Adequately separate systems of different safety classes and functions of different safety classescategories.

d. Should Ddefine the interfaces and means of communications between the individual I&C systems;

e. Should Eestablish the design strategies to be applied to fulfil the reliability requirements of each safety function allocated to the overall I&C architecture;[16]

e. ~~Strategies for achieving reliability requirements might include, for example, compliance with the single failure criterion, redundancy, independence between redundant functions, fail-safe design, diversity, testability and maintainability. Section 7 discusses considerations in implementing strategies to achieve reliability.~~

> **Formatted:** List Number, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.27 cm

f. Should support the compliance of safety groups with the single failure criterion;

g. Should Pprovide necessary information that is necessary in the main control room, the supplementary control room, and other areas where information is needed for operation or for managing the an accident;

h. Should Pprovide the necessary operator controls in the main control room, the supplementary control room, and other areas where controls are needed for operation or for managing the an accident; and

---

[15] Topics to be considered consistently across all I&C systems include, for example: implementationapplication of the plant operational concept of the plant, application of design standards for the human machine interface design standards, constraints on cable routing, grounding practices and the philosophy of alarm management philosophy.

> **Formatted:** Body Text First Indent

[16] Strategies for achievingdetermining reliability requirements might include, for example, compliance with the single failure criterion, redundancy, independence between redundant functions, fail-safe design, diversity, verifiability (including analyzability and testability)testability and maintainability. Section 7 discussesdescribes considerations in implementing strategies to achieve reliability.

    i.   <u>Should P</u>provide <u>the</u> automatic controls necessary to maintain and limit the process variables within the specified operational ranges and to limit the consequences of failures and deviations from normal operation so that they do not exceed the capability of safety systems.

4.12. The characteristics of I&C platforms used to implement I&C systems may interact with the design of the overall I&C architecture, and the overall I&C architecture will impose functional and qualification requirements on ~~the~~ <u>I&C</u> platforms. Therefore, it is generally advisable that the I&C platforms be selected in conjunction with the definition of the overall I&C architecture. The functional and qualification requirements for safety systems usually differ from those of control systems. Because of this and for reasons of diversity, the overall I&C will normally involve two or more platforms.

CONTENT OF INDIVIDUAL I&C SYSTEM ARCHITECTURES

4.13. The architectural design of each I&C system ~~should~~:

    a.   <u>Should P</u>provide all I&C functions ~~needed~~ <u>necessary</u> to fulfil the role assigned to it in the overall I&C architectural design;

    b.   Where appropriate, <u>should</u> partition the system into redundant divisions and <u>should</u> specify the required degree of independence between <u>such</u> divisions;[17] ~~Typically safety systems will be organized into redundant divisions in order to comply with the single failure criterion. Systems of lower safety class might not need to have redundant elements for reasons of nuclear safety, but might be redundant to improve the reliability of normal operation.~~

    c.   ~~Identify~~ <u>Should specify</u> the I&C items to be included in each <u>redundant</u> division;

    d.   <u>Should d</u>Describe the allocation of I&C functions and other system requirements to each I&C item;

    e.   <u>Should D</u>define the interfaces and means of communications between the I&C items within the system; ~~and~~

    f.   <u>Should D</u>define the main design features to be applied to the main items and the data links.

INDEPENDENCE

4.14. Independence within the overall I&C architecture is intended to prevent the propagation of failures between systems, and to avoid, where practical, exposure of multiple systems to the same ~~CCF~~ sources <u>of common cause failure</u>. Examples of such ~~CCF~~ sources <u>of common cause failure</u> include internal events, external events~~,~~ and failure of common support service systems.

4.15. The overall I&C architecture should neither compromise the independence of safety system divisions, nor the independence ~~implemented at~~<u>of</u> the different levels of the ~~plant~~ <u>concept of</u> defence-in-depth ~~concept~~<u>applied at the plant</u>.

---

[17] <u>Typically, safety systems will be organized into redundant divisions in order to comply with the single failure criterion. Systems ~~of~~<u>in</u> a lower safety class might not need to have redundant elements for reasons of ~~nuclear~~ safety, but might be redundant to improve the~~ir~~ reliability ~~of~~<u>in</u> normal operation.</u>

4.16. I&C functions that should are required to be fully independent should be assigned to independent hardware systems or items.

4.17. Safety systems should be independent from systems of a lower safety classification.

4.18. Redundant divisions within safety systems should be independent of each other to the extent necessary to ensure that all safety functions can be accomplished when required. Where communication between redundant divisions is necessary, for example for the purpose of voting or to enable partial trip, there should be sufficient measures to ensure electrical isolation,and physical separation and informationindependence of communication separation. Communication for the purpose of voting can limit spurious actuation caused by random failure, which could jeopardize safety.

4.19. Operator interfaces should not suppress the safety function of more than one redundant division at the same time.

4.20. A Ssafety control stations may operate an item of safety equipment outside its own division by way of a priority function that complies with the recommendations of paragraph para. 6.556.

4.21. Safety systems or components may also be operated from operator controls of in a lower safety classification only if demands by the safety system have priority to operate the device.

4.22. Information from safety systems may be presented on control stations of in a lower safety classification if the recommendations of paragraphs 6.256 to 6.567 are met.

4.23. Safety systems and components should remain capable of performing their safety functions when exposed to the effects of the accident conditions or conditions arising from, internal hazards or external hazards in which their response is necessary.

4.24. Failure or spurious operation of a support feature for an I&C safety system support feature should not compromise the independence between redundant portions of safety systems, between safety systems and systems of in a lower safety classification, or between different levels of the concept of plant defence in depth conceptapplied at the plant.

CONSIDERATION OF COMMON CAUSE FAILURE

4.25. SSR 2/1, Requirement 24 [1] states:

> "The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability."

4.26. The IAEA Safety Glossary, Ref. [68], defines a common cause failure as "fFailure of two or more structures, systems and components due to a single specific event or cause."

4.27. Common cause failure might happen, for example, because of human errors, errors in the development or manufacturing process, errors in maintenance, errors in software tools used in development tools, propagation of failures propagation between systems or components, or inadequate specification of, qualification for, or protection against, internal or external hazards.

4.28. The overall I&C architecture should define the architectural concepts to be employed in order to make the levels of the plant defence -in -depth at the plant as independent as is practical.

4.29. In order to preserve the independence between levels of the plant defence -in -depth at the plant, I&C is should be designed with defences against common cause failure CCF within and between systems. To Aachieveing this, involves making a well considered the allocation of functions to the various systems and system elements should be well considered, providing appropriate levels of independence between systems should be provided, and identifying the strategies to protect against common cause failure CCF within in the safety systems should be specified.

4.30. The potential that of common cause failure CCF within the overall I&C might to compromise one or more fundamental safety functions should be assessed.

4.31. Justification should be provided for any identified common cause failures CCF that are not considered in this assessment.

4.32. An analysis should be done of the consequences of each PIE postulated initiating event within the scope of safety analysis in combination with the common cause failures CCF that will would prevent a protection system from performing the needed necessary safety functions.

4.33. A analysis of the concepts of defence -in -depth and diversity analysis is one method of performing the analysis described in para.graph 4.32. See para.graph 2.83279.

	Formatted: Highlight

4.34. If the analysis described in para.graph 4.32 determines that a PIE postulated initiating event in combination with a common cause failure CCF of a protection system results in unacceptable consequences, the design should be modified.

4.35. Complete elimination of all vulnerabilities of I&C systems and architecture to common cause failure CCF is not achievable, but justification should be provided for the acceptance of any accepting identified vulnerabilities identified.

Diversity

4.36. The IAEA Safety Glossary, Ref. [68], defines diversity as "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."

4.37. Diversity is a way to of reducinge CCF vulnerability to common cause failures resulting from errors in requirements, design, manufacturinge or maintenance error, and to includeof including conservatism to compensate for the difficulty of demonstrating the specified level of reliability.

4.38. Where diversity is credited as mitigating the effects of common cause failure in the protection system, justification should be provided that the diverse features actually achieve the mitigation of the effects of the common cause mitigation failure that is claimed.

4.39. When diverse I&C systems are provided, it should be ensured that the diverse systems should not beare not subject to the same errors in specification, design, fabrication, or maintenance.

4.40. Probabilistic studies[18] should not treat I&C items important to safety as fully independent[19] unless they are diverse, and meet the guidance recommendations for functional independence, electrical isolation, communications independence, environmental qualification, seismic qualification, electromagnetic qualification, physical separation, and protection against internal events given in this documentprovided in this Safety Guide.

4.41. Probabilistic studies include, for example, reliability analysis and probabilistic safety assessment. In probabilistic studies, systems are treated as fully independent by simply taking the product of their individual failure probabilities.

5. SAFETY CLASSIFICATION OF I&C FUNCTIONS, SYSTEMS, AND EQUIPMENT

5.1. SSR 2/1 Requirements 18 [1] states:

> "The engineering design rules for items important to safety at a nuclear facility power plant shall be specified and shall comply with the relevant national or international codes and standards and with proven engineering practices, with due account taken of their relevance to nuclear power technology."

5.2. SSR 2/1 Requirement 22 [1] states:

> "All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance."

5.3. SSR 2/1 para.graph 5.34 [1] states:

> "The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:
>
> (a) The safety function(s) to be performed by the item;

---

[18] Probabilistic studies include, for example, reliability analysis and probabilistic safety assessment.

[19] In probabilistic studies, systems are treated as fully independent by simply taking the product of their individual failure probabilities.

(b) The consequences of failure to perform a safety function;

(c) The frequency with which the item will be called upon to perform a safety function;

(d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function."

5.4. SSR 2/1 ~~paragraph~~ para. 5.36 [1] states:

"Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment."

5.5. ~~The draft Safety Guide DS 367 Safety Classification of Structures, Systems and components in Nuclear Power Plants,~~ Reference. [21 17] provides recommendations and guidance on how to meet the requirements established in Refs [1] and [57] for the identification of SSCs important to safety and for their classification on the basis of their function and safety significance.

5.6. The safety classification process recommended in Ref. [17 21] is consistent with the concept of defence in depth set out in Ref. [1]. The functions performed at the different levels of defence in depth are considered.

5.7. For a specific nuclear ~~facility~~ power plant, the classification process should primarily consider:

- The design basis ~~of~~ for the plant and its inherent safety features;

- The list of all postulated initiating events, as required in Ref. [1], Requirement 16. The frequency of occurrence of the postulated initiating events, as considered in the design basis ~~of~~ for the ~~facility~~ plant, should be taken into account.

5.8. The possibility that the failure or spurious operation of an item important to safety may directly cause a ~~PIE~~ postulated initiating event, or that the failure on demand of an item important to safety may make the consequences of a postulated initiating event ~~PIE~~ worse, should be considered when the list of postulated initiating events ~~PIE~~ is established.

5.9. All I&C system functions and design provisions necessary to achieve the main safety functions, as defined in Ref. [1], Requirement 4, for the different plant states, including all modes of normal operation, should be identified.

5.10. All I&C system functions should then be categorized on the basis of their safety significance, with account taken of the three following factors:

1) The consequences of failure to perform the function;

2) The frequency of occurrence of the postulated initiating event for which the function will be called upon;

3) The time following a postulated initiating event at which, or the period of time during which, the function will be required to be performed.

5.11. The I&C systems and components performing each function assigned in a safety category should be identified and classified. They should be primarily classified according to the category assigned to the function that they perform.

5.12. When assigning the safety classification, the timeliness and reliability with which alternative actions can be taken and the timeliness and reliability with which any failure in the I&C system can be detected and remedied should be considered.

5.13. In the Safety Guide DS 367Ref. [17], three safety categories for functions and three safety classes for SSCs are recommended, based on the experience of the Member States. However, a larger or smaller number of categories and classes may be used, provided that they are aligned with the guidance provided in paras 2.12 and 2.15 of Ref. [17] if desired.

6. GENERAL RECOMMENDATIONS FOR ALL I&C SYSTEMS IMPORTANT TO SAFETY

GENERAL

6.1. I&C systems should fully implement meet the requirements of their design basis.

6.2. Unnecessary complexity should be avoided in the design of I&C safety systems.

6.3. All features of I&C safety systems should be beneficial to their safety functions.

6.4. Complexity in the design of I&C safety systems should not lead to violation of other design principles, e.g., independence, redundancy or diversity.

6.5. The intent of avoiding complexity is to keep the I&C system as simple as possible but still fully implement meet its safety requirements. Examples of complexity to be avoided are the inclusion of functions that do not contribute to the its safety functionsality or do not contribute to its reliability, the use of design and implementation features not amenable to sufficient analysis or verification, and the use of implementation platforms for implementation that are too complex to facilitate an adequate demonstration of safety demonstration. Therefore, the aArchitecture employed should have with simple interactions and simple communication links is, therefore, needed. Careful documentation and review of the rationale for each requirement is one effective means for avoiding inessential unnecessary complexity.

DESIGN FOR RELIABILITY

6.6. SSR 2/1 Requirement 23 [1] states:

"The reliability of items important to safety shall be commensurate with their safety significance."

6.7. SSR 2/1 Requirement 62 [1] states:

"Instrumentation and control systems for items important to safety at the nuclear power plant shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed."

6.8. SSR 2/1 para. paragraph 6.34 [1] states:

"Design techniques such as testability, including a self-checking capability where necessary, fail-safe characteristics, functional diversity and diversity in component design and in concepts of operation shall be used to the extent practicable to prevent loss of a safety function."

6.9. In the design of I&C systems, examples of features used to provide functional reliability include: the ability to tolerate random failure, independence of equipment and systems, redundancy, diversity, tolerance of common cause failures, testability and maintainability, fail-safe design, and selection of high quality equipment.

Single failure criterion

6.10. SSR 2/1 Requirement 25 [1] states:

"The single failure criterion shall be applied to each safety group incorporated in the plant design."

6.11. SSR 2/1 para.graph 56.39 [1] states:

"Spurious action shall be considered to be one mode of failure when applying the concept to a safety group or safety system."

6.12. Normally, concepts such as redundancy, independence, testability, continuous monitoring, environmental qualification, and maintainability are employed to achieve compliance with the single failure criterion.

6.13. Each safety group should perform all actions required to respond to a postulated initiating event PIE in the presence of any single detectable failure within the safety system, in combination with the following:

a. Any undetectable failures, i.e., any failure that cannot be detected by periodic testing, alarm or anomalous indication;

b. All failures caused by the single detectable failure and the undetectable failures;

c. All failures and spurious system actions that cause, or are caused by, the design basis postulated initiating event requiring that could affect the safety group;. and

d. The removal from service or the bypassing of part of the safety system for testing or maintenance that is allowed by plant operating limits and conditions.

6.14. Failures resulting from errors in design, maintenance, operations, or manufacturing are not included in analysis of compliance with the single failure criterion. Known errors should be properly

addressed by means of the Mmanagement systems are expected to result in properly addressing known errors. The effects of unknown errors cannot be predicted, and thus the single failure criterion is not a useful tool for understanding the effects of such errors on a safety group. Analysis to assess the potential consequences of common cause failure CCF due to such errors is discussed in sSection 4.

6.15. Non-compliance with the single failure criterion should be in exceptional cases only, and should be identified in design documents and clearly justified in the safety analysis.

6.16. Great care is needed necessary in the analysis ofwhen analysing low frequency events, such as external hazards, to justify non-compliance with the single failure criterion. It is advisable to pay Pparticular attention consideration should be given to ensuring the long-term availability of the electrical systems and other support systems that are necessary for the operation and monitoring of safety systems.

6.17. Reliability analysis, probabilistic assessment, operating experience, engineering judgment or a combination of these may be used to establish a basis for excluding a particular failure from consideration when applying the single failure criterion.

6.18. Maintenance, repair and testing activities should be consistent with plant the operating limits and conditions at the plant, even in situations in which the single failure criterion is not met..

6.19. Where compliance with the single failure criterion is not sufficient to meet reliability requirements, additional design features should be provided or modifications to the design should be made to ensure that the system meets reliability requirements.

Redundancy

6.20. I&C systems should be redundant to the degree needed necessary to meet the requirements for I&C reliability requirements and the single failure criterion.

6.21. Redundancy is commonly used in I&C systems to achieve system reliability goals for systems, including conformity with the single failure criterion. Redundancy is not fully effective unless the redundant elements are also independent. In general, redundancy increases the reliability, but it also increases the probability of spurious operation. Coincidence of redundant signals ("voting logic") or a rejection scheme for spurious signals is commonly used to obtain an appropriate balance of reliability and freedom from spurious operation.

Independence

6.22. SSR 2/1 Requirement 21 [1] states:

"Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate."

6.23. SSR 2/1 pPara.graph 5.35 [1] states:

"The design shall be such as to ensure that any interference between items important to safety will be prevented, and in particular that any failure of items important to safety in a system in a lower safety class will not propagate to a system in a higher safety class."

6.24. The IAEA Safety Glossary, Ref. [68], defines independent equipment as "Eequipment 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."

6.25. Independence is provided established to prevent a failure, an internal hazard or an external hazard from affecting redundant elements of safety systems. It is also provided established to prevent a failure or hazard from affecting systems that provide different levels of defence in depth. Failure processes to that should be considered include the following: failures resulting from design basis eventsaccidents, exposure to the same hazards, electrical connections between systems or between redundant divisions, data exchange between systems or between redundant divisions, and common errors in design, manufacturinge, operations, or maintenance.

6.26. Means for providing independence include the following features: physical separation, electrical isolation, functional independence, independence from the effects of communications errors (see Ssection 7). Equipment qualification and diversity may also support independence. These topics are discussed later in this section. Generally, combinations of these features are should be employed to achieve independence goals.

6.27. When isolation devices for ensuring isolation are used between systems of different safety importanceclasses , they should be a part of the system of the higher importancesafety class.

6.28. Measures provided for isolation from various physical effects, electrical faults, and communications errors do not necessarily need to be incorporated within the devices being protected. Features for isolating systems from the various different kinds of threats do not need to be incorporated within the same physical device or be positioned at the same location in a circuit. Isolation functions for a single effect may also be shared by more than one device. For example, isolation against errors in data communications errors might be provided by a buffer memory to prevent data from being directly written by one division to another, with validity checking provided by a processor in a different device, to ensure that data is not read from the buffer unless it meets criteria for validity, correctness, and authenticity.

6.29. The adequacy of design features provided to meet independence requirements should be justified.

Physical separation

6.30. Uses of pPhysical separation are listed in the following:

- Physical separation pProtects against common cause failure due to the effects of internal hazards. Internal hazards of concern include fire, missiles, steam jets, pipe whip, chemical explosions, flooding, and failure of adjacent equipment;

- Physical separation mMay be used to protect against common cause failure due toin normal, abnormal, or accident environmentsconditions, the effects of accidents (including all design basis accidents), or the effects of internal and external hazards.[20] Examples include: space to attenuate effect of EMI; separation between systems and components qualified to different levels.

- Environmental, seismic, and electromagnetic qualification may also be used by themselves, or in conjunction with physical separation, to protect against the effects of accidents, internal hazards, or external hazards;

- Physical separation mMay reduce the likelihood of common cause failure CCF as a result of external events that have localized effects (e.g., aircraft crash, tornado, or tsunami); and

- Physical separation rReduces the likelihood of inadvertent errors during operation of or maintenance on redundant equipment.

6.31. Items that are part of safety systems should be physically separated from items of in systems of a lower safety classification.

6.32. Redundant portions of safety groups should be physically separated from each other.

6.33. Complete physical separation between redundant items may be impractical when sensors or actuators are placed close together, such as may be the case for control rod drives or in-vessel instrumentation.

6.34. Some areas that might present difficulties due to convergence of equipment or wiring are the following:

- Containment penetrations,

- Motor control centres;

- Switchgear areas;

- Cable spreading rooms;

- Equipment rooms;

- The main control room and other control rooms; and

---

[20] Examples include: space to attenuate the effects of electromagnetic interference and separation between systems and components qualified to different levels. Environmental qualification, seismic qualification and electromagnetic qualification may also be used by themselves, or in conjunction with physical separation, to protect against the effects of accidents, internal hazards or external hazards;

- The plant process computer.

6.35. Where adequate physical separation is not possible, separation should be provided as far as is practically achievable and the exceptions should be justified (see paragraph para. 6.43).

6.36. Physical separation is achieved by distance, barriers, or a combination of the two.

6.37. NS-G-1.7, References. [202] and NS-G-1.11, Ref. [231] give provide additional guidance on protection against fires and other internal hazards.

Electrical isolation

6.38. Electrical isolation is used to prevent electrical failures in one system from affecting connected systems, or redundant elements within a system.

6.39. Safety systems and components should be electrically isolated from systems and components of in a lower safety classification.

6.40. Redundant portions of safety groups should be electrically isolated from each other.

6.41. Devices providing Eelectrical isolation devices should prevent maximum credible voltage or current transients, grounds, open circuits, and short circuits applied to one side of the device from unacceptably degrading the operation of the connected safety circuits.

6.42. Examples of provisions for electrical isolation include the following: the absence of electronic connections, devices providing electronic devices providing isolationg devices, devices providing optical isolationg devices (including optical fibres), relays, a separation distance, internal mechanical structures, or combinations of these features.

Associated circuits

6.43. When it is impractical to provide adequate physical separation or electrical isolation between a safety circuit and a circuit of a lower safety class function, the lower class circuit of the lower safety class (called here an associated circuit) should be:

a. Should be Aanalysed or tested to demonstrate that the association does not unacceptably degrade the safety class circuits with which it is associated;[21]
   ~~For example, the analysis or test may consider the maximum voltages within the associated circuit, in comparison with the voltages that the safety circuit can tolerate.~~

b. Identified Should be specified as being part of the safety division with which it is associated; and

c. Should be Pphysically separated from other components to the same extent as the circuits of the safety division with which it is associated.

---

[21] For example, the analysis or test may consider the maximum voltages within the associated circuit, in comparison with the voltages that the safety circuit can tolerate.

Functional iIndependence

6.44. Functional independence is a condition that exists when successful completion of a system's required functions is not dependent upon any behaviour including failures ~~and~~ or normal operation of another system, or upon any signals, data~~,~~ or information derived from the other system. Functional independence is a means of achieving isolation of a system from another system. Functional independence can also be used as a means of achieving isolation between redundan~~cies~~teies equipment.

6.45. Functional independence is supported by the architectural design and careful treatment of data that are shared between functions. The architectural considerations are described in ~~S~~section 4. The treatment of shared data is discussed ~~below~~in the following.

6.46. Inputs from I&C systems of a lower safety class~~ification~~ should not adversely affect the ability of safety systems to perform their safety functions.

6.47. Safety systems may, however, depend upon inputs from ~~non safety~~ maintenance systems that are not safety classified, for example, ~~to~~ systems for perform~~ing~~ maintenance, software updates, testing~~,~~ or ~~to~~ for sett~~ing~~ configuration data. Such inputs are typically made with the affected division off line and are verified after data are entered.

6.48. Monitoring systems of a lower safety class~~ification~~ may be connected to safety systems provid~~ing~~ed that it is demonstrated that the~~y~~ monitoring systems cannot disturb the safety systems~~m~~. When safety systems ~~may be~~are to be connected to maintenance systems of a lower safety class~~ification~~, the connection should be made only~~:~~ when the affected division or channel is offline, the use of data from the maintenance system is restricted to a specific purpose, and the connection of the maintenance system complies with the computer security program~~mes~~.

6.49. In circumstances where maintenance ~~can~~ is to be allowed at the channel level, sufficient isolation should be provided between channels that are common to a single division.

6.50. The plant operational modes in which the maintenance system may be connected should be ~~defined~~specified.

6.51. The transfer of data between safety systems and systems of a lower safety class~~ification~~ should be designed so that no credible failures in the systems ~~in~~of the lower safety class ~~systems~~ will prevent any connected safety system from accomplishing its safety functions.

6.52. The communications of data between redundant elements of a safety group should be designed so that no credible failures in the sending element will prevent the connected elements from meeting their requirements.

6.53. In computer systems, one-directional, broadcast data communication is often used where computer based systems of a higher safety class~~ification~~ provide data to systems of a lower safety class~~ification~~. Hardware characteristics that enforce the one-directional feature should be considered

as a means of ensuring such one-directional communication, e.g., the use of a link that is connected only to a transmitter in the system inof a higher safety classified system and only to a receiver in the system inof the lower safety classified system, are a favoured means of ensuring one-directional communication.

6.54. In justified cases, signals may be sent from systems of a lower safety class to systems of a higher safety classification via individual analogue or binary signal lines, provided that:

- The recommendation in para. 6.50 51 is still satisfied, ; and

- The potential for failures in the system of the lower safety classification that could cause spurious actuation of safety classified components is assessed and is shown to be acceptable.

6.55. When safety systems actuators act on information from other systems, including those of a lower safety classification, provisions should be made to ensure that incorrect data from the other system cannot inhibit safety functions are used. Often this is achieved through the use of priority logic that gives precedence to data and commands from within the safety system.

6.56. Paragraphs 7.52 to 7.59 provide additional recommendations for cases where systems for protection and for control systems use common signal inputs.

Diversity

6.57. Difficulties might arise in demonstrating the reliability of computer-based systems or systems that use complex hardware functions, complex hardware logic or complex electronic components. If it is not possible to justify confirmdemonstrate the adequate reliability of for a function being performed by I&C, then diverse I&C equipment may be used to increase confidence that the fundamental safety functions will be achieved. There are significant differences in the types of diversity expected by in the different Member States.

6.58. The decision to use diversity or not to use diversity in accomplishing the fundamental safety functions under design basis accident conditions should be justified.

6.59. Where diversity is provided to cope with the potential for common cause failureCCF, the use of more than one type of diversity should be considered.

6.60. Examples of different types of diversity include the following:

- Design diversity: achieved by using the use of different design approaches to solve the same problem or a similar problem;

- Signal diversity: achieved by systems in which a safety action may be initiated based upon the value of different plant parameters;

- Equipment diversity: achieved by hardware that employs different technology (e.g., analogue equipment vs. digital equipment, solid-state equipment vs. electromagnetic equipment, or computer-based equipment vs. FPGA equipment based on field programmable gate arrays);

- Functional diversity: achieved by systems that take different actions to achieve the same safety intentfunctionoutcome;

- Life cycle dDiversity in the development process: achieved by using different design organizations, different management teams, different design and development teams, and different implementation and testing teams.

- Logic diversity: achieved by use of different software or hardware description/HDL languages, different algorithms, different timings of logical functions, and different order sequencing of logical functions.

6.61. Where diversity is provided, it should be confirmeddemonstrated that the choice of the types of diversity used should be justified as achievesing the common cause mitigation that is claimed.

6.62. It is not always necessary to apply Ddiversity need not always be implemented in separate systems. For example, functional diversity and signal diversity might be implemented applied within a single system.

6.63. The provision of diversity also involves avoiding the avoidance of areas of potential commonality in the application of diversity, such as similar materials, similar components, similar manufacturing processes, similar logic, subtle similarities in operating principles, or common support features. For example, different manufacturers might use the same processor or license the same operating system, thereby potentially incorporating common failure modes. It is insufficient to base Cclaims for diversity based only on a difference in manufacturers' names or model numbers are insufficient without consideration of this possibility.

Failure modes

6.64. SSR 2/1 Requirement 26 [1] states:

"The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety."

6.65. A Lloss of power to any I&C component or a failure of an I&C component in any of its known and documented failure modes should place the system in a predetermined condition that has been demonstrated to be acceptable for nuclear safety.

6.66. Methods for ensuring that failures place a system in a safe condition include design such that systems go to a safe condition when de-energized or the use of 'watchdog timers' to detect that equipment is no longer performing its design function and to place the system in a safe condition.

6.67. Where such practices are applied, failures of the fail-safe design features themselves should be considered when applying the guidance of ~~paragraph~~ para. 6.65.

6.68. The non-systematic failure modes of I&C components and systems should be known and documented.

6.69. ~~Knowing~~ Knowledge of the failure modes of components is important in ~~applying~~ application of the fail-safe concept to systems. It is also important in confirming that control system failures do not cause events that are outside of the bounds of the safety analys~~i~~es.

6.70. The failures that might result from software errors are difficult to predict. Nevertheless, it is not necessary to know how the software fails in order to determine the possible failure states as seen at device terminals. Possible failure modes could be identified and ~~classified~~ grouped into a manageable set of possibilities, e.g. wrong output, delayed output, frozen output.

6.71. The failure modes that are most likely to result from systematic causes in the design of hardware or software are essentially unpredictable. Consequently, the concept of fail-safe design is not effective for dealing with failures resulting from such causes. Disciplined development processes (~~s~~See section 2), ~~H~~hazard analysis (para~~graph~~s 2.56 to 2.65), application of the concept of defence in depth (see ~~S~~section 4), and the application of diversity (see para~~graph~~s 6.57 to 6.63) are more effective tools for reducing the number of such causes~~,~~ and for coping with the effects of such causes that remain.

6.72. Failures of I&C components should be detectable by periodic testing or~~,~~ self-diagnostics or should be self-revealed by alarm or anomalous indication.

6.73. It is preferred that failures be self-revealing. The mechanism ~~for~~ by which faults are self-revealing ~~faults~~ should not put the system in an unsafe state or result in spurious activation of safety systems.

6.74. Any identified failures that cannot be detected by periodic testing, alarm~~,~~ or anomalous indication should be assumed to exist in conjunction with single failures when evaluating conformance with the single failure criterion. Failure of self-test features, self-diagnostic features or self-alarm~~, etc.~~ features themselves should be detected and revealed.

6.75. As far as practicable, the failure of a component should not cause spurious actuation of any safety system~~s~~.

6.76. On restart or on restoration of power to I&C safety systems or components. the outputs should be initialized in a predefined safe condition, except in response to valid safety signals.

EQUIPMENT ~~QUALIFICATON~~QUALIFICATION

6.77. SSR 2/1 Requirement 30 [1] states:

> "A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their

intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing."

6.78. I&C systems and components should be qualified for their intended function during their service life.

6.79. The qualification of I&C components should include their software, HDL hardware description languages, and process interfaces, if any.

6.80. The qualification should provide a degree of confidence commensurate with the system or component's importance to safety of the system or component.

6.81. The qualification programmes should address all topics affecting the suitability of each system or component for its intended functions, including:

   a.   Suitability and correctness of functions and performance;
   b.   Environmental qualification;
   c.   Qualification for the effects of internal and external hazards; and
   d.   Electromagnetic qualification.

6.82. Equipment qualification should be based on a selection of the following methods:

   a.   Use of engineering and manufacturing processes in compliance with recognized standards;
   b.   Reliability demonstration;
   c.   Past experience in similar applications;
   d.   Type tests;
   e.   Testing of supplied equipment;
   f.   Analysis to for extrapolatinge test results or operating experience under relevant conditions;
   g.   Evaluation of manufacturer production processes;
   h.   Inspection of components during manufacture.

6.83. It is generally not necessary to apply all of the methods mentioned. The specific combination of methods selected will depend upon the system or component under consideration. For example, in the qualification of pre-existing items, might place more emphasis might be placed on past experience and analysis so as to compensate for a lack of completely documented verification and validation during engineering and manufacturing.

6.84. The method, or combination of methods used for equipment qualification should be justified.

6.85. Where operating experience is used to support equipment qualification, it should be shown to be relevant to the proposed use and environment of the target application.

6.86. For safety systems, evidence of qualification evidence based uponon the basis operating experience is not enoughinsufficient and is should therefore be combined with type testing, and testing

of supplied equipment, as well as with evaluation of ~~manufacturers'~~ the production processes of manufacturers, or inspection of components during manufacture.

6.87. Analysis that is part of the evidence of equipment qualification should include a justification of the methods, theories and assumptions used.

6.88. For example, the validity of the mathematical models used for equipment qualification might be justified on the basis of experimental data, test data, or operating experience.

6.89. Traceability should be established between each installed system and component important to safety and the applicable evidence of qualification.

6.90. This includes traceability not only to the component itself, but traceability between the qualified configuration and the installed configuration.

Suitability and correctness

6.91. The equipment qualification programme should demonstrate that the design of I&C systems, and components meets all functional requirements, performance requirements, and reliability requirements contained in the ~~I&C~~ design bases and equipment specifications of the I&C systems and components.

6.92. Examples of functional requirements include, functionality required by the application, functionality required to support the operability of system-s or equipment ~~operability~~, requirements on the operator interface ~~requirements~~, and requirements relating to input /output ranges ~~requirements~~.

6.93. Examples of performance requirements include requirements on accuracy, resolution, range, sample rate, and response time ~~requirements~~.

6.94. Examples of reliability requirements include, requirements for a minimum mean time between failures, and requirements on fail-safe behaviour, independence, failure detection, testability, maintainability, and service life.

6.95. The equipment qualification programme should demonstrate that ~~the design and]~~ the actual design and the as-built I&C systems and installed components correctly implement the qualified design.

Environmental qualification

6.96. In this Safety gGuide, environmental qualification is qualification for temperature, pressure, humidity, chemical exposure, radiation, submergence, electromagnetic phenomena, and ageing mechanisms that affect the proper functioning of components under those conditions.

6.97. Systems, and components should be designed to accommodate the effects of, and be compatible with, the environmental conditions associated with normal operation, ~~and~~ anticipated operational occurrences ~~or~~ and postulated accidents ~~when~~ during which they are required to function.

6.98. Components should be shown to meet all requirements when subjected to the range of specified environmental conditions.

6.99. Details of equipment qualification requirements, processes and methods are given in IAEA Safety Report Series No. 3 – Equipment Qualification, Ref. [224].

Components exposed only to mild environments

6.100. Environmental qualification of I&C components whose environmental service conditions during accidents are at no time significantly more severe than conditions during normal operations (so called 'mild environments') may be based upon a clear specification of functional requirements for the specific environmental conditions associated with plant operational states of the plant together with supplier certification from suppliers or a separate evaluation that the components will perform their required functions under the stated environmental conditions.

Components exposed to harsh environments

6.101. Environmental qualification of components that are required to function in environmental service conditions that are at any time significantly more severe than the conditions during normal operations (so called 'harsh environments') should show demonstrate that the component is, at the end of its qualified life, capable of performing its safety functions under the full range of specified service conditions.

6.102. Showing Demonstration that components can function as required at their the end of their qualified life involves the addressing of significant ageing effects (e.g., radiation and thermal ageing) to show that the required functionality is maintained at the end of qualified life. Normally, this includes providing the inclusion of further conservatism, where appropriate, to allow for unanticipated ageing mechanisms.

6.103. In defining the specification of the equipment qualification programme, the worst credible combinations of environmental service conditions, including synergistic effects between service conditions, should be addressed.

6.104. If it is necessary to separately test separately for different environmental conditions (e.g., separate tests for radiation effects and temperature effects) the sequence in which these tests are conducted should be justified as one that appropriately simulates the degradation caused by the combined environments.

6.105. The most rigorous methods for environmental qualification methods may need to be applied only to safety classified components.

6.106. The eEnvironmental qualification of safety classified components that are required to operate in harsh environments should include type tests.

6.107. When protective barriers are provided to for isolatinge equipment from possible environmental effects, the barriers themselves should be subject to a qualification programme to validate their adequacy.

Internal and external hazards

6.108. The plant design basis and the plant's safety analysis will identify internal and external hazards, such as fire, flooding and seismic events, which the plant is required to tolerate for operation or which the plant is required to withstand safely, and for which protection or system qualification is needed. The plant design basis and the plant's safety analysis will also identify hazards contributed through systemic causes such as an engineering decision or deficiency that could result in the degradation of a safety function; commensurate system constraints should be identified to prevent the degradation of a safety function. The plant design basis and the plant's safety analysis for the plant will identify lead to the identification internal and external hazards, such as fire, flooding and seismic events, which the plant is required to tolerate for operation or which the plant is required to withstand safely, and for which protection or system qualification is needednecessary.

6.109. I&C systems and components should be protected against the effects of fire and explosion in accordance with the guidance of NS-G-1.7, Ref. [202].

6.110. I&C systems and components should be protected against the effects of other internal hazards in accordance with the guidance of NS-G-1.11 Ref. [231].

6.111. I&C systems and components should be designed and qualified to withstand seismic hazards in accordance with the guidance of NS-G-1.6, Ref. [235].

6.112. I&C systems and components should be protected against or designed and qualified to withstand other external hazards in accordance with the guidance of NS-G-1.5, Ref. [246].

Electromagnetic qualification

6.113. Electromagnetic compatibility (EMC) is the ability of a system or component to function satisfactorily in its electromagnetic environment without introducing the introduction of intolerable electromagnetic disturbances to anything in that environment. An item's The susceptibility of an item to electromagnetic interference (EMI) and its the contribution of electromagnetic interference to the electromagnetic environment (emissions) are both part of EMCelectromagnetic compatibility.

6.114. EMI Electromagnetic interference includes rRadio fFrequency iInterference (RFI) and as used in this Safety Guide includes electrical surges, for example, voltage spikes resulting from switching transients.

6.115. The undisturbed operation of electrical and electronic systems and components depends upon the electromagnetic compatibility of components with their operating environment, i.e. a

component'sthe capability of a component to withstand the disturbances caused by the components around it or connected to it.

6.116. Significant sources of electromagnetic interference include fault current clearance by from the operation of switchgears, circuit breakers or fuses operation; electric fields caused by radio transmitters; natural sources such as lightning strike or solar storms; and other man-made sources internal or external to the plant.

6.117. Electromagnetic qualification of I&C systems and components depends upon a combination of system and component design to minimize the coupling of electromagnetic noise to I&C components, testing to demonstrate that components can withstand the expected levels of electromagnetic radiation, and testing to demonstrate that electromagnetic emissions are within tolerable levels.

6.118. Techniques for minimizing the production generation and coupling of electromagnetic noise include the following:

- Suppression of electromagnetic noise at the source;

- Separation and isolation of instrument and controlI&C signal cables from power cables;

- Shielding of equipment and cables from external sources of magnetic and electromagnetic sourcesradiation;

- Filtering of electromagnetic noise before it can couple to sensitive electronic circuits;

- Neutralization or isolation of electronic equipment from ground potential differences; and

- Proper grounding of electrical and I&C equipment, raceways, cabinets, components, and cable shields.

6.119. Appropriate installation and maintenance practices are essential for the proper implementation application and continued effectiveness of these provisions.

6.120. Detailed EMC requirements for electromagnetic compatibility should be determined for safety systems and components and their compliance with the requirements should be demonstrated.

6.121. International EMC standards for electromagnetic compatibility for industrial environments may serve as the basis for the requirements. provided that they are supplemented, where necessary, to cover the electromagnetic compatibility needs plant-specific EMC to the plant that might be more demanding. Determination of EMC requirements for electromagnetic compatibility involves consideration of the possibility that I&C components will be exposed to possible repetitive transients (e.g. switching -off of inductive loads and ringing of relays) and high-energy surges (e.g. power faults and lightning).

6.122. Establishing the ~~EMC~~ electromagnetic environment of I&C components at each nuclear power plant unit generally involve~~s~~ ~~unit~~-specific analyses of each unit. These analyses are used to judge the adequacy of each I&C component~~'s~~ ~~EMC characteristics~~relating to electromagnetic compatibility.

6.123. Equipment and systems important to safety, including associated cables, should be designed and installed to withstand the electromagnetic environment in which they are located.

6.124. The ~~types~~ aspects of electromagnetic interference to be considered in the design of I&C systems and components include the following:

- Emission of and immunity to electromagnetic disturbances;

- Emission and conduction of electromagnetic disturbances via cables;

- Electrostatic discharge ~~(ESD)~~;

- Switching transients and surges;

- The emission characteristics of wireless systems and devices[22] used at the plant as well as those of repair, maintenance and measuring devices. ~~Wireless systems and devices include, for example, mobile phones, radio transceivers, and wireless data communication networks.~~

6.125. In the vicinity of certain sensitive equipment, ~~it may be appropriate to establish~~ exclusions zones should be established in which~~where~~ operation of wireless devices and other portable ~~EMI~~ sources of electromagnetic interference (e.g.~~,~~ weld~~ing~~ers devices~~)~~ is restricted.

6.126. The equipment qualification programme should ~~show~~ demonstrate that safety classified I&C components are capable of performing their safety functions when exposed to the limits defined by the ~~EMI~~ and ~~Surge Withstand Capacity (SWC)~~ operating envelopes for electromagnetic interference and for surge withstand capacity.

6.127. Limits on radiated and conducted electromagnetic emissions should be established for all plant equipment.

6.128. Any electrical or electronic equipment in the plant will contribute to the electromagnetic environment. Therefore, the need to limit electromagnetic emissions ~~applies~~ should apply to all plant equipment, not just equipment that is classified as important to safety.

6.129. Emission constraints placed on individual components should be such that the resultant emission in the operating environment is within the safe (hazard-free) ~~EMI~~ envelope for electromagnetic interference of every component, in all modes or states of the system and the components, including transitions across modes~~/~~ or states and including degraded conditions.~~.~~

---

[22] Wireless systems and devices include, for example, mobile telephones, radio transceivers, and wireless data communication networks.

6.130. The equipment qualification programme should show demonstrate that electromagnetic emissions of all plant equipment are within the defined limits.

6.131. Equipment and systems, including associated cables and power supplies, should be designed and installed to appropriately limit appropriately the propagation (both by both radiation and conduction) of electromagnetic interference among plant equipment.

6.132. When several I&C systems are connected to the same power supply, the electromagnetic qualification should evaluate interferences interfaces and transmission paths for EMIelectromagnetic interference.

6.133. Instrumentation cables should be twisted pairs and should be shielded to minimize interference from electromagnetic and electrostatic interference.

6.134. DS-430, Reference. [79] gives provides recommendations for grounding, cable selection, and cable routing to reduce production generation and propagation of electromagnetic interference.

DESIGN TO COPE WITH AGEING AND OBSOLESCENCE

6.135. SSR 2/1 Requirement 31 [1] states:

"The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life."

6.136. SSR 2/1 para. Paragraph 5.51 [1] states that

"The design for a nuclear power plant shall take due account of ageing and wear out effects in all operational states for which a component is credited, including testing, maintenance, maintenance outages, plant states during a postulated initiating event and plant states following a postulated initiating event."

6.137. SSR 2/1 para. Paragraph 5.52 [1] states

"Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help identify unanticipated behaviour of the plant or degradation that might occur in service."

6.138. The qualified service life of electrical and electronics systems and components might be considerably less than the lifetime of the plant life.

6.139. Age related degradation that impairs the ability of a component to function under severe harsh environmental conditions might exist arise well before the functional capabilities of the component under normal conditions are noticeably affected.

6.140. Ageing mechanisms that could significantly affect I&C components and the means for following the effects of these mechanisms should be identified during design.

6.141. The Iidentification of the potential impacts of ageing impacts involves first an understanding of the relevant ageing phenomena for the various I&C components.

6.142. Ageing of I&C components most commonly results from exposure to heat or radiation. Nevertheless, the possibility that other phenomena (e.g., electromigration in microcircuits, formation of 'tin whiskers', mechanical vibration, or chemical degradation) might be relevant to a specific component is to be considered when applying the guidance of paragraph para. 6.1402.

6.143. Maintenance programmes should include activities to for the identificationy of any trend towards degradation (ageing), including the detection of precursors that could cause the equipment to become incapable of performing its safety function.

6.144. Examples of monitoring techniques include the following:

- Testing of representative plant components or a unit subject to ageing for degradation of performance, at suitable intervals;

- Visual inspections; and

- Analysis of operating experience.

6.145. Examples of means to address ageing impacts include the following:

- Replacement of Ccomponents replacement before the end of its their qualified life;

- Adjustment of functional characteristics (e.g., recalibration) to account for ageing effects; and

- Changes to maintenance procedures or environmental conditions that have the effect of slowing the ageing process.

6.146. The qualified life of safety classified components that are required to perform their safety function in harsh environments should be determined.

6.147. Safety classified components should be replaced before the end of their qualified life.

6.148. On-going qualification might show that the qualified life of a component is validated or is indicated to be different than from the qualified life that was determined through testing, analysis, or experience. Information from on-going qualification may be used to increase or decrease the qualified life of a component.

6.149. The anticipated service life and the anticipated obsolesceobsolescence of I&C systems and components should be identified during design and should be communicated to the operating organization.

6.150. Estimation of service life and the expected ~~obsolesce~~ date of obsolescence of I&C systems and components provides the operating organization with information that they need to make long term agreements with suppliers, to plan the acquisition of extra spare parts~~s~~, and to plan for timely replacement of obsolete items.

6.151. ~~At the present time~~It is expected that ageing or obsolescence may cause the service life of some I&C systems to be significantly shorter than the ~~plant~~ lifetime of the plant. Therefore, it might be appropriate to provide features that will facilitate the installation of and switchover to replacement systems. Such facilities might include space reserved for the installation of new equipment and associated cables.

6.152. ~~NS-G-2.12,~~ Reference. [2~~5~~7] ~~gives~~ provides additional guidance on ageing management and obsolescence management. It includes a ~~discussion~~ description of the interface between the equipment qualification programme and the ageing management programme.

CONTROL OF ACCESS TO SYSTEMS IMPORTANT TO SAFETY

6.153. SSR 2/1 Requirement 39 [1] states:

"Unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be prevented."

6.154. ~~IAEA Nuclear Security Series No. 4,~~ References. [26, 27, 28]~~, No. 8, Ref. [29] and No. 13, Ref. [30] give~~ provide guidance on security for nuclear power plants and the coordination of ~~nuclear~~ safety and nuclear security.

6.155. Access to equipment in I&C systems should be limited to prevent unauthorized access and to reduce the possibility of error.

6.156. Effective methods include appropriate combinations of administrative measures and physical security, e.g.~~,~~ locked enclosures, locked rooms and~~,~~ alarms on enclosure doors.

6.157. Areas of particular concern ~~for~~ are access to set point adjustments, calibration adjustments~~,~~ and configuration data, because of their importance to preventing degraded performance of systems ~~performance~~ due to ~~potential~~ errors in operation or maintenance.

6.158. Paragraphs 7.103 to 7.130 provide additional guidance for the control of electronic access to digital systems.

TESTING AND TESTABILITY DURING OPERATION

6.159. SSR 2/1 Requirement 29 [1] states:

"Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure

their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis."

6.160. SSR 2/1 Paragraph para. 6.35 [1] states:

"Safety systems shall be designed to permit periodic testing of their functionality when the plant is in operation, including the possibility of testing channels independently for the detection of failures and losses of redundancy. The design shall permit all aspects of functionality testing for the sensor, the input signal, the final actuator and the display."

Test provisions

6.161. I&C systems should include provisions for testing.

6.162. Test provisions that are permanently connected to safety systems are themselves safety systems unless they meet the recommendations relating to independence guidance of provided in paragraphs paras 6.25 to 6.56.

6.163. Testing and calibration of safety system equipment should be possible in all modes of normal operations, including power operation, while retaining the capability of the safety systems to accomplish their safety functions is retained.

6.164. Periodic tests during plant operation will normally be needed necessary to achieve the reliability required of safety systems; however it is sometimes desirable to avoid testing during power operation if it this would puts at risk the plant safety of the plant at risk. The benefits of testing and calibration during power operation shouldmust be balanced with the adverse effects they may cause on the plant safety of the plant.

6.165. Where the ability to test a safety system or component during power operation is not provided, the following should be ensured:

a. The reliability of the functions affected should be shown to be acceptable over the interval between tests;

b. The accuracy and stability of the untested components should be shown to meet requirements over the interval between tests;

c. Consideration should be given to providing the provision of means for comparing measurements of untested instrument channels with other devices (for example, to compare neutron power with thermal power); and

d. The capability to test the untested system or components during shutdown should be provided.

Automatic testing, self-supervision and monitoring

6.166. I&C systems should have features for self-supervision or monitoring features that allow regular confirmation of their continued correct operation.

6.167. ~~These~~ Such features should include means for checking the rationality of inputs ~~rationality checking~~.

6.168. Digital safety systems should include safe-state features such as watchdog timers.

6.169. Design~~ing~~ of systems or components so that their failure would be self-revealing is one means of accomplishing the recommendation of ~~paragraph~~ para. 6.166.

6.170. Test facilities include hardware and software provided to perform testing and the associated test sequences ~~regardless~~ irrespective of whether they are initiated manually or automatically.

6.171. Alarms should be provided for indicating loss of redundancy in safety systems.

6.172. When a fault in a system or equipment is detected by self-supervision, a predefined action should be taken.

Preserving I&C functions during testing

6.173. SSR 2/1 ~~paragraph~~ para. 5.46 [1] states:

> "Where items important to safety are planned to be calibrated, tested or maintained during power operation, the respective systems shall be designed for performing such tasks with no significant reduction in the reliability of performance of the safety functions. Provisions for calibration, testing, maintenance, repair, replacement or inspection of items important to safety during shutdown shall be included in the design so that such tasks can be performed with no significant reduction in the reliability of performance of the safety functions."

6.174. The test provisions for I&C systems (both manual provisions and automatic provisions) should be designed to ensure that testing will not adversely affect the ability of I&C systems to perform their safety functions and to minimize the possibility of spurious initiation of safety actions and other adverse effects of the tests on the availability of the plant.

6.175. Arrangements for testing should neither compromise the independence of safety systems nor introduce the potential for common cause failures.

6.176. Arrangements for testing include procedures, test interfaces, installed test equipment, and built in test facilities.

Test interfaces

6.177. SSR 2/1 para. ~~paragraph~~ 5.45 states:

> "The plant layout shall be such that activities for calibration, testing, maintenance, repair or replacement, inspection and monitoring are facilitated and can be performed to relevant national and international codes and standards. Such activities shall be

commensurate with the importance of the safety functions to be performed, and shall be performed without undue exposure of workers."

6.178. Provisions for testing I&C systems and components should have the following characteristics:

a. They should H̶have appropriate test interfaces[23] and means for status indication;̶

~~For example, test interfaces with the capability to introduce simulated process conditions or electrical signals.~~

b. They should O̶operate such that faults in the equipment are readily detectable;̶

c. H̶ave̶ They should have features to prevent unauthorized access;̶

d. B̶e̶ They should be readily accessible to testing staff and test equipment;̶

e. H̶ave̶ They should have the necessary communications facilities n̶eeded̶ to support the tests;̶

f. They should b̶B̶e located such that neither testing nor access to the testing location expose operating personnel to hazardous environments.;̶[24]

~~Example considerations include:~~

- ~~Location of sensors such that testing and calibration can be performed at their location.~~

- ~~Location of test devices and test equipment in areas convenient to the equipment to be tested.~~

- ~~Plant or administrative features that could make it difficult to bring test equipment to the location of components to be tested, e.g., the necessity to move equipment along narrow paths, or in and out of contaminated areas.~~

- ~~Convenience of component status indication and test connections.~~

6.179. Where equipment to be tested is located in hazardous areas, provisions should be made to allow testing to be controlled from outside the hazardous area.

Test program̶me̶

6.180. The design of I&C systems should include i̶dentification̶ specification of a testing and calibration programme that supports i̶mplementation̶ application of the g̶uidance̶ recommendations providedg̶iven̶ in N̶S-G-2.2,̶ Refs̶. [16, 29, 30, 31];̶ NS-G-2.4, Ref. [32], NS-G-2.6, Ref. [18]; and NS-G-2.14, Ref. [33]̶.

---

[23] For example, test interfaces with the capability to introduce simulated process conditions or electrical signals.

[24] Example considerations in determining the location of provisions for testing include the following:
- Location of sensors such that testing and calibration can be performed at their location;
- Location of test devices and test equipment in areas convenient to the equipment to be tested;
- Plant or administrative features that could make it difficult to bring test equipment to the location of components to be tested, e.g., the necessity to move equipment along narrow paths, or in and out of contaminated areas;
- Convenience of the status indication of components and test connections.

6.181. An I&C test programme will normally include the following:

- A description of programme objectives;

- Identification Specification of systems and channels to be tested;

- The frequency and sequencing of individual tests;

- The reasons and justification for the tests to be conducted and the test intervals;

- A description of required documentation and reports;

- Criteria for passing or failing the test, and a process for handling non-conformance to these criteria;

- A requirement for periodic review of the effectiveness of the testing programme effectiveness; and

- Specification of the individual test procedures that will be used to control the conduct of tests.

6.182. The scope and frequency of testing and calibration should be justified as consistent with functional requirements and availability requirements.

6.183. The tests defined in the test programme should ensure confirm thatthat the following conditions are met, during and after completion of the tests:

a. The overall functional capabilities of the systems are not degraded:, and

b. The I&C safety systems continue to meet their functional requirements and performance requirements.

6.184. In Tthe test programme, should arrangethe tests should be arranged into a sequence such that the overall condition of the system or component undergoing testing can be immediately assessed without further testing of other components or systems.

6.185. The Cconduct of the test programme should not cause deterioration of any plant component beyond that provided for in the design.

6.186. In the Cconduct of the test programme and in reaching a the decision about when the end of qualified life for a component has been reached, it may, for example, need be necessary to consider wear and ageing due to the testing.

6.187. Implementation of theThe test programme should provide for the following:

a. Objective information on the status of the system or component status;

b. Assessment of component degradation;

c. Data on trends to assist in detecting degradation;

d. Indications of incipient failure within the system;, and

e. Requirements for evaluations that are to be conducted before a repetition of the failed test can be credited as establishing operability.[25]

~~Evaluating and documenting the reasons for, root causes of, and actions taken after a failed test is normally needed before the results of a repeated test can be used to demonstrate operability of the system or component involved.~~

~~Corrective actions may, for example, include maintenance or repair of components, or changes to test procedures.~~

~~If corrective actions are determined to be unnecessary the reasons are to be documented.~~

6.188. The test programme should define processes for periodic tests and calibration that:

a. Specify overall checks of safety functions from the sensors to the actuators;

b. Can be performed in-situ;

c. Confirm that functional requirements and performance requirements of ~~safety functions~~ the equipment are met;

d. Test input and output functions, such as alarms, indicators, control actions, and operation of actuation devices to the extent necessary to satisfy requirements on system reliability and functional requirements.

e. Define the expected results of each test;

f. Ensure the safety of the plant during testing;

g. Minimize the possibility of spurious initiation of any safety action and any other adverse effect of the tests on the availability of the plant;

h. Forbid the use of makeshift test set-ups, temporary jumpers, or temporary modification of computer code;[26]

~~Test equipment may be temporarily connected to plant equipment if the equipment to be tested has facilities specifically designed for the connection of this test equipment.~~

~~Where temporary connections are required for periodic testing or calibration, connection and use of such equipment are to be subject to appropriate administrative controls.~~

i. Forbid modification of configuration parameters for plant components ~~configuration parameters~~ unless these have been previously identified as service parameters;

j. Minimize the time interval during which equipment is removed from service; ~~and~~

---

[25] Evaluation and documentation of the reasons for, root causes of, and actions taken after a failed test is normally necessary before the results of a repeated test can be used to demonstrate operability of the system or component involved. Corrective actions may, for example, include maintenance or repair of components, or changes to test procedures. If corrective actions are determined to be unnecessary the reasons are to be documented.

[26] Test equipment may be temporarily connected to plant equipment if the equipment to be tested has facilities specifically designed for the connection of this test equipment. Where temporary connections are required for periodic testing or calibration, connection and use of such equipment are to be subject to appropriate administrative controls.

k. Individually test each sensor, to the extent practicable.

6.189. In addition to the recommendations of para. ~~paragraph~~ 6.188, the processes defined for periodic tests and calibration of safety systems ~~should~~:

a. Should b~~B~~e a single on-line test;[27]

Such an on-line test will be able to identify specific defects directly when initiated, without the need for making test connections or disturbing the on-line equipment or its operation for more than a limited time.

~~When a single on-line test is not practicable, the test program may combine overlapping tests, to achieve the test objectives.~~

b. Should I~~i~~ndependently confirm the functional requirements and performance requirements of each channel of sens~~ing~~e, command, execute~~,~~ and support functions;

c. Should i~~I~~nclude as much of the function under test as practical (including sensors and actuators) without jeopardizing continued normal plant operation;

d. Should, w~~W~~herever possible, be accomplished under actual or simulated operating conditions, including sequence of operations;

e. Should T~~t~~est and calibrate all variables used, where combinations of variables are used to generate a particular signal for a safety system; ~~and~~

f. Should B~~b~~e capable of detecting faults in redundant equipment.[28]

~~Redundant equipment might be equipment in redundant divisions or redundant equipment within a single division.~~

6.190. When a single on-line test is not practicable, the test programme may combine overlapping tests, to achieve the test objectives. Where a single on-line test is not provided for a safety system channel, documented justification should be provided for the use of overlapping tests.

6.191. Typically the justification will demonstrate that the overlapping tests provide complete coverage, that reliability of the equipment is acceptable given the longer test interval, and that any components not tested on-line will be tested during plant shutdown.

MAINTAINABILITY

6.192. The design of I&C systems should include maintenance plans for all systems and components.

6.193. I&C systems and components should be designed, located~~,~~ and erected so as to minimize risks to operating personnel and to facilitate necessary preventive maintenance, troubleshooting~~,~~ and timely repair.

---

[27] Such an on-line test will be able to identify specific defects directly when initiated, without the need for making test connections or disturbing the on-line equipment or its operation for more than a limited time.

[28] Redundant equipment might be equipment in redundant divisions or redundant equipment within a single division.

6.194. Design to facilitate maintenance, troubleshooting and repair includes the following:

- Avoiding locating equipment in areas where conditions of extreme temperature, or humidity are expected during plant normal plant operation;

- Avoiding locating equipment in areas where there is a risk of high radiation levels. (Ssee NS-G-1.13, Ref. [324]);

- Taking into account of human capabilities and limitations in performing maintenance activities;

- Leaving sufficient room around the equipment to ensure that the maintenance staff can perform their tasks under normal working conditions.

6.195. If components are located in inaccessible areas, examples of other strategies for coping with failure include the following:

- Installation of spare redundant devices;.

- Facilities for remote maintenance;. and

- Planning for plant operation at reduced power if the equipment fails and cannot be quickly and easily repaired or replaced.

6.196. Means provided for the maintenance of I&C systems should be designed such that any effects on the safety of the plant are acceptable.

6.197. Typical examples for such means are the disconnection of one division in a system with several redundant divisions, or provisions for carrying out alternative manual actions.

PROVISIONS FOR REMOVAL FROM SERVICE FOR TESTING OR MAINTENANCE

6.198. If use of a facility for testing or maintenance can impair an I&C function, the interfaces should be subject to hardware interlocking to ensure that interaction with the test or maintenance system is not possible without deliberate manual intervention.

6.199. The design should ensure that systems cannot unknowingly be left in a test or maintenance configuration.

6.200. Removal from service of any single component of a safety system component or any redundant division should not result in loss of the required minimum redundancy, unless system operation with acceptable reliability can be adequately demonstrated.

6.201. SSR 2/1 para. Paragraph 6.36 [1] states:

"When a safety system, or part of a safety system, has to be taken out of service for testing, adequate provision shall be made for the clear indication of any protection system bypasses that are necessary for the duration of the testing or maintenance activities."

6.202. Inoperability or bypass of components of a safety system components or of divisions should be indicated in the control room.

6.203. For items that are frequently bypassed or frequently rendered inoperable, these indications should be automatic.

6.204. NS G 2.6, Reference. [168] provides guidance for returning systems and equipment to service after testing and maintenance.

SETPOINTS

6.205. SSR 2/1 para. Paragraph 5.44(b2) [1] states:

> "The requirements and operational limits and conditions established in the design for the nuclear power plant shall include…limiting settings for safety systems…."

6.206. The operational limits and conditions for safe operation include I&C setpoints for safety systems.

6.207. Determination of I&C setpoints for safety systems setpoints usually considers the following values:

- Safety limits – limits on certain operational parameters within which the operation of the reactor plant has been shown to be safe.[29]

     The safety limits are sometimes given in terms of parameters that are not directly measurable by the I&C system.

- Analytical limit (of setpoint) – the limit of a measured or calculated variable established by the safety analysis to ensure that a safety limit is not exceeded. [30]

     The margin between the analytical limit and the safety limit takes into account: the response time of the instrument channel, and the range of transients due to the accident considered.

- The tTrip setpoint – a predetermined value for actuation of the final setpoint device to initiate a protective action.

- Allowable value - tThe limiting value that a setpoint may have when tested periodically, beyond which appropriate action is necessary. Finding a setpoint beyond its allowable value may mean that the channel has not performed within the assumptions of the setpoint analysis. In this case, it

---

[29] The safety limits are sometimes given in terms of parameters that are not directly measurable by the I&C system.

[30] The margin between the analytical limit and the safety limit takes into account: the response time of the instrument channel, and the range of transients due to the accident considered.

is necessary to determine if the operational limits and conditions have been violated and what, if any, action is needed to restore the channel to operability.

- Limiting settings for safety systems – t̶T̶he levels at which protective devices are to be automatically actuated, in the event of anticipated operational occurrences or accident conditions, to prevent safety limits from being exceeded.[31] L̶i̶m̶i̶t̶i̶n̶g̶ ̶s̶e̶t̶t̶i̶n̶g̶s̶ ̶f̶o̶r̶ ̶s̶a̶f̶e̶t̶y̶ ̶s̶y̶s̶t̶e̶m̶s̶,̶ ̶a̶l̶s̶o̶ ̶c̶a̶l̶l̶e̶d̶ ̶s̶a̶f̶e̶t̶y̶ ̶s̶y̶s̶t̶e̶m̶ ̶s̶e̶t̶t̶i̶n̶g̶s̶ ̶o̶r̶ ̶l̶i̶m̶i̶t̶i̶n̶g̶ ̶s̶a̶f̶e̶t̶y̶ ̶s̶y̶s̶t̶e̶m̶ ̶s̶e̶t̶t̶i̶n̶g̶s̶,̶ ̶i̶s̶ ̶a̶ ̶l̶e̶g̶a̶l̶ ̶t̶e̶r̶m̶ ̶i̶n̶ ̶s̶o̶m̶e̶ ̶M̶e̶m̶b̶e̶r̶ ̶S̶t̶a̶t̶e̶s̶.̶ ̶T̶h̶e̶s̶e̶ ̶m̶i̶g̶h̶t̶ ̶b̶e̶ ̶e̶x̶p̶r̶e̶s̶s̶e̶d̶ ̶a̶s̶ ̶t̶r̶i̶p̶ ̶s̶e̶t̶p̶o̶i̶n̶t̶s̶,̶ ̶a̶l̶l̶o̶w̶a̶b̶l̶e̶ ̶v̶a̶l̶u̶e̶s̶,̶ ̶o̶r̶ ̶b̶o̶t̶h̶.̶ ̶N̶S̶ ̶G̶ ̶2̶.̶2̶,̶ ̶R̶e̶f̶.̶ ̶[̶3̶1̶]̶ ̶p̶r̶o̶v̶i̶d̶e̶s̶ ̶a̶d̶d̶i̶t̶i̶o̶n̶a̶l̶ ̶g̶u̶i̶d̶a̶n̶c̶e̶ ̶o̶n̶ ̶e̶s̶t̶a̶b̶l̶i̶s̶h̶i̶n̶g̶ ̶a̶n̶d̶ ̶i̶m̶p̶l̶e̶m̶e̶n̶t̶i̶n̶g̶ ̶s̶a̶f̶e̶t̶y̶ ̶s̶y̶s̶t̶e̶m̶ ̶s̶e̶t̶t̶i̶n̶g̶s̶.̶

6.208. Setpoints measured during periodic testing should be evaluated to confirm that deviation from the previous setting is consistent with expectations used in the uncertainty analysis. Excessive deviation that does not result in violation of the allowable value (for instance, deviation in the conservative direction) might still be indication that the channel is not behaving as expected, and that either the equipment needs to be repaired, or the analysis needs to be revised.

6.209. Figure 3 illustrates the relationship between these terms and the types of measurement uncertainties and biases that are normally considered in establishing the basis for trip setpoints and allowable values.

Effects and uncertainties accounted for in safety analysis, e.g., response time

Safety l̶L̶imit

Analytical L̶limit

If the actual setpoint is found in this region, the channel is considered to be inoperable

Allowance for uncertainties, dynamic effects, calibration and installation biases, and safety margin

Allowable v̶V̶alue

Allowance for instrument drift and uncertainties in calibration

Operating margin

Trip s̶S̶etpoint

Normal o̶O̶perations̶

FIG. 3. Setpoint terminology and errors to be considered in *determination of* setpoint*s* *determination*

---

[31] Limiting settings for safety systems, also called safety system settings or limiting safety system settings, is a legal term in some States. These might be expressed as trip setpoints, allowable values, or both. Reference [29] provides additional guidance on establishing and implementing safety system settings.

Formatted: Font: 10 pt

6.210. Setpoints may be either a fixed value or a variable value that depends upon some other plant parameter or condition.

6.211. Trip setpoints used to initiate safety actions should be selected to ensure that required mitigating actions occur before the monitored variable reaches the its analytical limit.

6.212. Limiting settings for safety systems should be calculated using a documented methodology that provides sufficient allowance between the trip setpoint and the analytical limit to take into account for measurement biases,and channel biases, uncertainties and any changes to these values which that occur over time.

MARKING AND IDENTIFICATION OF ITEMS IMPORTANT TO SAFETY

6.213. A consistent, coherent, and easily understood method of naming and identifying all I&C components and for use as descriptive titles for the human-machine interface HMI should be determined and followed throughout the design, installation and operation phases in the lifetime of the plant.

6.214. A suitable identification scheme would should not require frequent reference to drawings, manuals, or other material.

6.215. Coherent and easily understood naming and identification of systems and components is important for engineering staff, maintenance staff, and construction staff as well as for use to label thein labelling controls, displays and indications.

6.216. I&C components in the plant should generally be marked with their identifying information.

6.217. Components or modules mounted in equipment or assemblies do not need their own identification. Configuration management is generally sufficient for maintaining the identification of such components, modules and computer software.

Formatted: Body Text 2

6.2187. The components of different safety divisions should be easily distinguishable from each other and from components of in a lower safety classification.

6.2189. Clear identification of components reduces the likelihood of the inadvertently performanceing of maintenance, tests, repair or calibration on an incorrect channel.

6.119220. Identification may, for example, take the form of tagging or colour coding, for example.

7. DESIGN GUIDELINES FOR SPECIFIC I&C SYSTEMS AND EQUIPMENT SPECIFIC DESIGN GUIDELINES

SENSING DEVICES

7.1. Measurements of plant variables should be consistent with the requirements of the design bases for the I&C systems and the plant design bases.

7.2. Measurement of plant variables includes both measurement of the present value of a variable within a range, and detection of discrete states such as are detected by limit switches, auxiliary relay contacts, and temperature, pressure, flow or level switches.

7.3. Measurement of plant variables may be made by direct measurement, or indirect measurement, such as a calculation based upon multiple measurements, or determination of the value of a variable based upon measurement of other data with a known relationship to the desired variable.

7.4. To the extent practicable, plant conditions should be monitored by direct measurement rather than being inferred from indirect measurements.

7.5. The sensor for each monitored variable and its range should be selected on the basis of the accuracy, response time, operational environment, and range needed necessary to monitor the variable in all plant states during which the information from the sensor is needed. The design of sensors and actuators, should consider design margins.

7.6. The consequences of common cause failure in sensors CCF should be integrated included in the analysis described in paraparagraphs 4.30 to 4.34.

Formatted: Highlight

7.7. No identified CCF vulnerability to common cause failure of sensing devices should have the potential of denying operators the information and parameters that they need to control accidents and mitigate their consequences accident conditions.

7.8. If more than one sensor is necessary to cover the entire range of a monitored variable, a reasonable amount of overlap from one sensor to another should be provided at each transition point to ensure that signal saturation or fold overfoldover effects in the signal response curve do not prevent the required function from being performed.

7.9. If the spatial dependence of in the measurement of a variable (i.e., the measured value of variable depends upon the location of the sensor location) is important to an I&C function, the minimum number and locations of sensors should be identified.

CONTROL SYSTEMS

7.10. SSR 2/1 Requirement 60 [1] states:

"Appropriate and reliable control systems shall be provided at the nuclear power plant to maintain and limit the relevant process variables within the specified operational ranges."

7.11. The automatic control that maintains the main process variables within operational limits is part of the defencse in depth of the plant, and therefore the control systems concerned will normally be important to safety.

7.12. The control systems should provide for bumpless transfer between automatic control mode and manual control modes, and where switchover occurs between an online processor and a standby processor in automatic mode.

7.13. Loss of power to control functions should result in bumpless transfer to standby equipment or a freeze of the actuators with an alarm and transfer to operator manual control.

7.14. The effects of a failure of an automatic control system failures should not create a condition which that exceeds the acceptance criteria or assumptions established for design basis accidents. Failure modes such as multiple spurious actions of a control system actions should also be considered when a the potential for such failures exists for a specified system design. Appropriate design measures such as segmentation can be used as a means to eliminate the plausibility of multiple spurious control system actions or reduce the likelihood of their occurrence to an acceptable level.

PROTECTION SYSTEM

7.15. SSR 2/1 Requirement 61 [1] states:

"A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions."

7.16. The protection system should monitor plant variables and detect deviations from their specified limits so that the protection system will maintain plant parameters within the limits established for each design basis accident.

7.17. The protection system as a whole may include several systems.

Automatic safety actions and manual safety actions

7.18. SSR 2/1 para. Paragraph 6.33(b) [1] states:

"The design [(of the protection system]) … sShall … automate various safety actions to actuate safety systems so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions."

7.19. Means should be provided to automatically initiate and control all safety actions of the protection system safety actions except those for which manual action alone has been justified.

7.20. Typically automatic initiation will be provided for most functions of the protection system functions.

7.21. Examples of situations in which manual action alone might be justified include the following:

- Initiation of certain safety tasks after completion of automatic sequences;.

- Control actions to bring the plant to a safe state in the long term after an accident;, and

- Initiation of safety actions that are not required until a considerable time after the postulated initiating eventPIE.

7.22. In order to justify that manual action alone is acceptable, the following requirements apply and it should be showndemonstrated to have been met that:

a.   Safety systems should provide the operators with information that is clearly presented and sufficient to enable them to make reasoned judgments on the need to initiate the required safety actions;

b.   The operator is should be provided with written procedures and training for the safety tasks;

c.   The operator is should be provided with sufficient means of plant control to perform the required actions;

d.   The communication links between operators carrying out the actions are should be adequate to ensure the correct accomplishment of these actions;

d.e. A suitable human factors engineering analysis should be performed to ensure that plant conditions can be maintained within recommended acceptance criteria for each plant initiating event; and

e.f. The operator is should be allowed sufficient time to evaluate the status of the plant and to complete the required actions.³² The associated timing analysis should take into account the time available and time required for each operator action necessary. The timing analysis determines the safety margin and as the safety margin decreases, the uncertainty in estimating the difference between these times should be appropriately considered.

For new designs or significant modifications, it is advisable to design such that during the first 30 minutes of a design basis event, operator actions are not needed to maintain plant parameters within the established limits.

7.23. Means should be provided to manually initiate the mechanical safety systems and the individual components that are necessary to initiate and control performance of their safety functions.

7.24. The manual signal to initiate the safety function of a mechanical safety system's safety function should be injected as close as practicable to the final actuation device.

7.25. Manual initiation of safety actions provides a form of defence in depth for anticipated operational occurrences and accidentabnormal conditions and supports long-term operation of the plant post following an accident operation.

7.26. Mechanical safety systems are, for example, the individual divisions of control rods the emergency feed water, the emergency core cooling, or containment isolation.

Information display

7.27. SSR 2/1 para. paragraph 6.33(c) [1] states:

---

³² For new designs or significant modifications, it is advisable to design the plant such that during the first 30 minutes of a design basis accident, operator actions are not necessary to maintain plant parameters within the established limits.

"The design [(of the protection system]) … sShall ... make relevant information available to the operator for monitoring the effects of automatic actions."

7.28. The protection system should make available to plant operators the measured value of each input parameter used in functions of the protection system functions, the state of each trip function and actuation function in each division, and the state of actuationinitiation of each system initiation.

Sensors and settings of the Pprotection system sensors and settings

7.29. The sensors that provide signals to the protection system should only feed other systems only through appropriate buffering and isolation devices.

7.30. Design techniques, such as functional diversity, redundancy and signal diversity, should be used to the extent practicable to prevent loss of protection system functions.

7.31. Where multiple setpoints are needed for a protection system function (e.g., to allow for power increase or decrease), the design should ensure that the more restrictive setpoint is used automatically or imposed by administrative means when plant conditions are no longer appropriate for use of the less restrictive setpoint.

7.32. It might sometimes be desirable to provide multiple setpoints to achieve adequate protection for a particular mode of operation or set of operating conditions.

7.33. If the design provides variable setpoints or provides for the ability to change a setpoint when the protection system is required to be operable, the devices used to vary or change the setpoint should be part of the protection system.

7.34. The protection system should provide a means for determining the setpoint values for each channel of the protection system channel.

Operational bypasses

7.35. Operational bypasses or trip-conditioning logic might be necessary to inhibit the actuation of protection system functions during specific plant conditions. For example, it is an operational necessity that the trips that limit reactor power during startup be bypassed at some point to allow power increase past the setpoint for low power trip setpoint.

7.36. Where an operational bypass is necessary, the operator should be provided with suitable warnings or alarms when the plant is approaching a state where it the operational bypass needs to be operated.

7.37. Indication of the states of operational bypasses states should be provided in the control room.

7.38. The protection system should automatically accomplish one of the following actions if the conditions for an activated operational bypass are not met:

    a.   Removale of the activated operational bypass;,

b.   ~~Put~~ Placing of the plant in a condition where the operational bypass is permissible~~,~~ ; or

c.   Initiat~~ione~~ of appropriate protective actions.

Latching of protection system functions

7.39. SSR 2/1 para. ~~paragraph~~ 6.3~~5~~(a) [1] states:

"The design [~~(~~of the protection system~~])~~ … S~~s~~hall prevent operator actions that could compromise the effectiveness of the protection system in operational states and in accident conditions, but not counteract correct operator actions in accident conditions."

7.40. Actions initiated by the protection system should be latched so that once an action is started, it will continue although the initiating state might have ceased to be present.

7.41. Latching of actions initiated by the protection system ~~actions~~ is normally implemented at the level of actuation signals to plant equipment. 'Seal-in' of individual measurement channels is not ~~required~~necessary.

7.42. Once a protection system function ~~is~~ has been initiated, all actions performed by that function should be completed.

7.43. The guidance of para. ~~paragraph~~ 7.42 is not meant to restrict the action of devices that are provided to electrically protect safety equipment activated by the protection system. ~~The electrical power safety guide, DS-430,~~ Ref~~erence~~. [7~~9~~], ~~gives guidance~~provides recommendations on electrical protection of items important to safety.

Formatted: Highlight

7.44. When a protection system function is reset, the actuated equipment should not return to the normal state except by a specific and deliberate operator action.

7.45. Provisions to reset the safety function should be part of the safety system.

Spurious initiation

7.46. The design of the protection system should, to the extent practicable, minimize the potential for spurious initiations or action~~s~~ of the protection system.

7.47. Spurious initiation of protection system functions could lead to the following:

* Unnecessary stress on equipment and reduction of the lifetime of the plant ~~life;~~

* The need for other safety actions;~~,~~

* Erosion of the ~~operators'~~ confidence of operators in equipment, potentially leading to their subsequent disregard~~ing~~ of valid signals;~~, and~~

* Loss of capability for production at the plant.

7.48. Spurious initiation of the protection system should not place the plant in an unsafe condition.

7.49. If spurious initiation or actions of the protection system could result in a plant state in which protective functions are the plant requiresproper functioning of the protection system isstill required, then safe conditions should be maintained through actions that are initiated and carried out by parts of the protection system or by other safety systems that were not responsible for and not affected by the spurious actuation.

Interaction between the protection system and other systems

7.50. SSR 2/1 Rrequirement 64 [1] states:

"Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence."

7.51. SSR 2/1 para. paragraph 6.38 [1] states:

"If signals are used in common by both a protection system and any control system, separation (such as by adequate decoupling) shall be ensured and the signal system shall be classified as part of the protection system."

7.52. The protection system should satisfy all requirements for reliability, redundancy, and independence requirements in the presence of a failure of any component or signal used in common by the protection system and the control system.

7.53. SSR 2/1 para. paragraph 6.32(a) [1] states:

"The protection system shall be designed … tTo be capable of overriding unsafe actions of the control system."

7.54. If a postulated initiating event PIE can cause an action of the control system action that results in a plant condition requiring initiation of a protection system function, then the same postulated initiating event PIE should not prevent proper action of the safety systems providing that the necessaryaction of the protection system function.

7.55. The possibility that a failure in the protection system may be itself a postulated initiating event PIE that triggers an action of control system action for which the protection system is necessary cannot should not be disregarded.

7.56. Examples of measures that have been used to prevent interference between control systems and protection systems causing incorrect operation include the following:

- The Pprovision of separate instrument channels for protection and for control;

- Additional equipment in the safety group to deal with the potential interference;

- The Pprovision of barriers or alternative arrangements in the plant arrangements to limit the damage resulting from the postulated initiating eventPIE; or

- Combinations of these ~~items~~ elements such that the safety group and the plant design are sufficient to maintain the plant conditions within acceptable limits.

7.57. The recommendations provided in paras~~Paragraphs~~ 7.52, 7.54 and 7.55 ~~are meant~~aim to ensure that in the event of such failures the protection system will still fully meet its requirements. The reliability requirements to be satisfied include compliance with the single failure criterion.

7.58. When a device may be actuated by either the protection system or a system of a lower safety class~~ification~~, any ~~protection system~~ demand ~~on~~by the protection system for ~~actuation~~ initiation of its protection of a~~function of the protection system~~ function ~~of the protection system function~~ should have priority to actuate the device.

7.59. For example, actuation signals may be sent from the control system for normal operation or to allow ~~the~~ operating personnel to control normal operation of all system elements from the same interface if any demand on the protection system ~~demand~~ overrides commands from the control system~~commands~~.

POWER SUPPLIES

7.60. Power supplies for I&C systems, ~~regardless~~ irrespective of their type (e.g.~~,~~ electrical power supplies, pneumatic power supplies, hydraulic power supplies), should have requirements on their safety class~~ification~~, reliability provisions, qualification, isolation, testability, maintainability~~,~~ and indication of removal from service that~~,~~ are consistent with the reliability requirements of the I&C systems they serve.

7.61. I&C systems that are required to be available for use at all times in operational states or design basis accident conditions should be connected to non-interruptible power supplies that provide the systems with power within the tolerances specified by the design basis for the I&C ~~design bases~~systems.

7.62. I&C systems may be transferred by ~~operators~~ manual action or by automatic switching action to a stand-by power supply instead of the normal power supply when necessitated by operating circumstances ~~need it~~, provided that the functions of the I&C systems can tolerate the associated interruption in power supply. Normally the transfer system ~~will~~should be treated as part of the power supply system and will be of the same safety ~~category~~class as the I&C system that it supports.

7.63. Some modern I&C systems can be powered directly from DC power sources. This is advantageous for systems that need non-interruptible power because it eliminates the need for inverters, motor-generators~~,~~ or power transfer devices in the electrical power system.

7.64. Power supplies can provide a transmission path for ~~EMI~~ electromagnetic interference ~~which~~that might originate outside the I&C systems or might arise from other I&C systems that are connected directly or indirectly to the same power supply (see para. ~~paragraph~~ 6.1323).

7.65. ~~DS-430,~~ Ref~~erence~~ [~~9~~7] provides recommendations for electrical power supplies and associated distribution systems. Recommendations for other forms of power supply (e.g.~~,~~ pneumatic power supplies, hydraulic power supplies, mechanical power supplies) are ~~currently contained~~provided in ~~the historical document NS-G-1.8,~~ Ref. [3~~3~~4]³³~~, and are to be updated during the preparation of a new safety guide on auxiliary systems.~~

DIGITAL SYSTEMS

7.66. Digital systems include, for example, computer based systems and systems programmed with ~~h~~Hardware ~~d~~Description ~~l~~Languages.

7.67. SSR 2/1 R~~r~~equirement 63 [1] states:

> "If a system important to safety at the nuclear power plant is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system."

Digital system functions

7.68. The use of digital systems for ~~NPP~~ I&C functions provides advantages that include the flexibility to provide complex functions, improved plant monitoring and improved interfaces with operators ~~interfaces~~, capability for self-test and self-diagnostics, a better environment to facilitate ~~lessons learned~~the feedback of operating experience based on tremendous ~~data recording~~ capabiliti~~es~~y for data recording, low physical size and low cabling needs. They can have test and self-check functions that improve reliability.

7.69. I&C functions are implemented differently in digital systems ~~than~~ from how they are implemented in analogue systems. In digital technology~~,~~. functions are combined in one or more processing units. Combined functions in a processing unit could lead to conditions that are very difficult to analyse and the failure of a processing unit will result in the simultaneous failure of several functions. Also, one function may degrade the performance of another (without any identifiable "failure") through unwanted interactions.

7.70. Full verification and validation of such complex components could be very difficult or even practically impossible if they ~~were~~ are not designed correctly. Unidentified errors might exist, and these might be replicated in all redundant components or spread to other systems that based on the same platform, because software modules, programmed devices~~,~~ or libraries could be common to all.

---

³³ A Safety Guide o design of auxiliary and supporting systems in nuclear power plants is also in preparation. [[DS440]]~~.~~

7.71. In digital systems, inputs are sampled at discrete points in time, signals are periodically transmitted between system elements, and outputs are also produced periodically. Consequently changes ~~of~~ in the processing load or communication load of a digital system could affect transmissions speed and response time, if ~~they~~ such systems are not designed correctly. Changes to the processing load or communications load might result from changes in plant parameters, operation in different systems or plant states, or equipment failures.

7.72. ~~Section 3 of~~ Reference. [1~~1~~2]~~, NP-T-3.12: Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants discusses~~ provides further detailed information on the special nature of digital systems ~~in more detail~~.

7.73. The design of digital I&C systems should ensure that the system will perform its safety functions ~~within~~ in accordance with the requirements for~~the~~ response time and accuracy ~~requirements~~ in all specified operating conditions and all possible conditions of data loading.

7.74. I&C ~~s~~Safety ~~I&C~~ systems should be designed to have deterministic behaviour, ~~i.e.,~~in that any given input sequence that is within the specification of the item's ~~specification~~ will always produce~~s~~ the same outputs, and response times, i.e., the time delay between stimulus and response has a guaranteed maximum and minimum.

7.75. Ensuring deterministic response times might, for example, involve the following:

- ~~Avoiding~~ Avoidance of process-related interrupts, so that no plant condition can directly affect the rate of interrupts that the I&C system ~~needs~~ will have to handle~~.~~;

- ~~Allocating~~ Allocation of resources statically at design time~~;~~, ~~and~~

- Bounding iterations of loops that are~~,~~ set by predefined limits.

7.76. The ~~R~~response time and accuracy of digital systems functionally depend on the sample rate~~,~~ and on the processing cycle time. In systems that have not been correctly designed, these parameters could also depend on the processor speed.

7.77. The design and analysis of digital systems should be such that ~~the effects of~~ failures of individual components (e.g.~~,~~ computer processors) result in a predictable range of accepted system behaviour.

7.78. Loss of power to or restart of a digital system should not result in undesirable modification of configuration data or software.

Digital data communication

7.79. The data communication for safety systems should be designed to have deterministic transmission times.

7.80. A means of ensuring deterministic transmission times might, for example, involve the following:

- Predetermined, time-based behaviour,; i.e., the actions of the data communication system are not determined by its client nodes, but are predetermined by design, based on a time schedule;,

- Predetermined data communication load,; i.e., the size of the message to be transmitted at any given time is predetermined by design, so that the communication load is always consistent with the transmission capacity of the data communication system,; and

- Predetermined data communication pattern,; i.e., the sender and addressees of the message to be transmitted at any given time are predetermined by design.

7.81. Digital data communication should comply with the recommendations of paraparagraphs 6.26 to 6.56.

7.82. Each message sent and received via digital data communication should be automatically checked and flagged if errors are identified.

7.83. Errors might include corrupted data, invalid data (unplanned messages), or inauthentic messages (messages from unexpected sources).

7.84. If communications systems encrypt data or use proprietary protocols, these features should not prevent detection of errors.

7.85. The actions to be taken when errors are detected in data communications should be defined in advance.

7.86. Actions that might be taken when errors are detected include, for example, the automatic rejection of invalid or inauthentic data, the correction of corrupted data where possible, or the rejection of corrupted data.

7.87. The design should ensure that failures of data transmission and of the data communication equipment are detected, that suitable alarms are provided to the operators and that records are made for analysis of performance.

7.88. The existence of certain types of error in digital data communication does not by itself constitute a failure in the system as such errors are expected and communication protocols are designed to deal with certain types of errors and a range of error occurrence rates of errors. Consequently, the implementation application of the guidance in para. paragraph 7.87 will involve defining specification of what constitutes a failure of data transmission. The criteria might, for example, specify a maximum allowable time interval between successful transmissions or a maximum error rate.

7.89. Features for the detection and correction of errors improve the reliability of signal transmission.

7.90. The extent of methods used for dealing with errors and detection of communications failures should be appropriate for the use of the data, appropriate for the frequency of demand for the functions that use the data, and balanced against the complexity that is introduced.

Communications features in safety systems

7.91. If ~~safety data~~ the communication~~s~~ of safety related data malfunctions in any way, the safety system should continue to perform its safety function or go to a safe state.

7.92. Often this recommendation is accomplished by using two processors that share data via carefully controlled access to shared memory. One processor is dedicated to performing the safety function and the other is dedicated to data communications tasks. Separation of calculation and logic functions from communications and interrupt functions prevents errors in these ~~later~~ latter functions from disrupting the deterministic behaviour and timing of safety calculations or logic functions. This separation, sometimes called buffering, seeks to prevent faults and failures of the communication originating outside the ~~safety~~ division from propagation to the processors that implement safety functions.

7.93. Only predefined messages should be processed by a receiving safety system.

7.94. The specific elements of message~~s~~ ~~elements~~ to be predefined include: the message protocol, the message format~~,~~ and the set of valid messages.

Independence of Ddata communications ~~independence~~

7.95. This section supplements the guidance of paras ~~paragraphs~~ 6.26 to 6.56 with guidance that is specific to data communications in digital systems.

Avoidance of common cause failure

7.96. The topology of the data communication network ~~topology~~ and ~~media~~ access control to media should be designed and implemented to avoid common cause failure ~~CCF~~ of safety systems.

Communications between safety divisions

7.97. Communications, including communications errors or failures, in a safety division~~s~~ should not prevent connected safety divisions from performing their safety function.

7.98. The intent of the recommendation in para.~~graph~~ 7.97 is to prevent the propagation of failures between divisions. Typically a combination of data validation (see para~~graph~~s 7.82 to 7.94)~~,~~ and buffering is employed.

7.99. Architectures using a central hub or router ~~where~~ in which communications from multiple safety divisions are transmitted across a single link should not be used.

Communications between systems inof different safety classes

7.100. Data communications between digital systems and devices of different safety classes should conform to the guidance of paras paragraphs 6.25 26 to 6.56. Demand for actuation initiation of a protection system function should have a priority to actuate the device.

Formatted: Highlight

Computer security

7.101. IAEA Nuclear Security Series No. 17, Reference. [328], provides guidance on concerns, requirements, and strategies for implementing computer security programmes at nuclear facilities. This section supplements the guidance of Nuclear Security Series No. 17, Ref. [832].

Interaction between safety and security

7.102. SSR 2/1 Rrequirement 8 [1] states:

> "Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another."

7.103. Neither the operation nor the failure of any computer security feature should adversely affect the ability of a system to perform its safety function.

7.104. The failure modes of computer security features and the effects of these failure modes on I&C functions should be known, documented, and considered in system hazard analyses.

7.105. If computer security features are implemented in the hHuman mMachine Iinterface, they should not adversely affect the operator's ability of operators to maintain the safety of the plant.

7.106. Where practicable, security measures that do not also provide a safety benefit, should be implemented in devices that are separate from I&C systems.

7.107. Adding The addition of security functions to an I&C system increases that system's the complexity of that system and might introduce potential failure modes to the system that would challenge its ability to reliably perform its safety function or increase the potential for spurious operation.

7.108. Computer security features included in I&C systems should be developed according in accordance withto Ssection 2 of this guide Safety Guide and qualified to the same level of qualification as the system in which the features resideare located.

7.109. The development process, operation and maintenance of digital systems or components should be conducted in accordance with a computer security plan that specifies and details the means for achieving computer security.

7.110. The computer security plan should include appropriate physical, logical and administrative controls to be implemented during the development of I&C systems development.

7.111. The development environment for digital systems and the subsequent installation, operation, and maintenance of digital systems should have suitable measures to for preventing the intentional or unintentional intrusion or corruption of the software or data, the introduction of malicious code, incorrect connection to external networks, or and hacking attacks.

Control of access to digital systems important to safety

7.112. All data connections for systems and components should be placed within enclosures for which both access to the enclosure and access to the inside of the enclosure is are controlled in accordance with para. paragraph 6.156.

Formatted: Highlight

7.113. Data connections include network connections, connections for external memory, and access to portable media such as memory sticks, flash cards, and data disks.

7.114. Unused data connections should be disabled.

7.115. Connections needed for temporary use, e.g., for the connection of maintenance computers, should be disabled when not in use.

7.116. Forms of disabling unused connections include removal, physical measures, or logical measures.

7.117. If logical measures are used as a means of disabling data connections, additional measures should be provided to ensure that the connection remains disabled or that any change in connection configuration or status will be detected and evaluated for its impact on system the operability of the system.

7.118. Access to functions that allow changes to software or configuration data and the changes themselves should be monitored and logged.

7.119. Monitoring and logging may be performed automatically or manually by administrative procedure.

7.120. The method used should be justified as providing the needed necessary security without interfering with the performance of safety functions.

7.121. Paragraphs 7.118 to 7.120 do not apply to changes in configuration data that can, by design, be made by control room operators.

Security of communication with emergency facilities

7.122. Data from plant I&C systems in the plant may be transmitted to other locations within on the plant site (e.g., a tTechnical sSupport cCentre) and to locations beyond the plant site (e.g., an Emergency Operations Facilityoperational support centre [?pls check!]emergency response

organization) to in support of emergency response, provided that I&C systems are not adversely affected by these connections.

7.123. Communication links between the plant and the emergency controloperationaltechnical support centre and between the plant and emergency response centresorganization, including those that are used for human communications, should be dedicated to the purpose and protected from tampering.

7.124. Data communication might include information about the status of the fundamental safety functions and other information to support emergency management.

Features for operational security

7.125. The use of Aactive computer security features should be considered for detecting and mitigating computer security threats and mitigating their effects.

7.126. Active computer security features for I&C systems should not adversely affect functions that are important to safety.

7.127. Active computer security features might increase the complexity of a system complexity, compete for use of system resources, increase the potential for spurious operation, or introduce new failure modes. Consideration should be given to the application of Ppassive computer security features could be applied at all times.

7.128. It is desirable to apply active security features only when the system is off line. For I&C systems, it is preferable to perform scanning functions off -line.

7.129. Computer systems should include provisions for periodic verification, and post-maintenance verification that computer security features are properly configured and are properly operating.

7.130. Procedures should be established for reviewing and acting upon the results produced byobtained from computer security monitoring should be established.

Devices configured with hardware description languages (HDL)

7.131. HDL Devices configured devices with hardware description languages are programmable electronic modules providing logic structures (e.g. arrays of gates and switches) which that are customized by the I&C developer to provide specific functions. Field pProgrammable gGate aArrays (FPGA) are a common example of devices in this class.

7.132. This customization involves special software tools to formally describe formally the required functionsspecificationsrequirements to implement these functions.

7.133. The guidance of this subsection relating to devices configured with hardware description languages is to should be applied in conjunction with the life cycle guidance of Ssection 2, the guidance for digital systems given provided above in this section and the guidance for software given provided in Ssection 9. It is applicable to devices that directly implement safety classified functions.

7.134. The Ddevelopment of applications using hardware programmed HDL configured devices should follow a previously defined life cycle that fulfils the recommendations of Ssection 2.

7.135. Development plans should call for the justification of each technical decision in a manner that is understandable by ato third partiesy.

7.136. The Iimplementation plan for hardware HDL programmed devices should define specify the means to ensure that each produced part complies with the design.

7.137. Design requirements for hardware HDL programmed devices _should include timing requirements, such as requirements on gate delays and setup times.

7.138. The selection HDL of hardware programmedable devices and associated items, such as libraries, iIntellectual pProperty (IP) cores to be included in the final product, and hardware definition languages, should follow a defined and documented process to ensure their suitability.

7.139. IP Intellectual property cores should only be used only if the following conditions are satisfied:

a. The IP intellectual property cores used should be obtained from qualified vendors, who followed a high quality IP cores development process for the intellectual property core, including a rigorous engineering process, well-defined and useful documentation, and ease of integration:, and

b. Evaluations should be performed to determine potential ensure there is no introduction of hazards.

7.140. If modifications of the pre-developed item are necessary to achieve acceptance, they should be specified, designed, implemented, and verified before review forthe acceptance review.

7.141. If the selected hardware HDL programmed device includes auxiliary features (e.g., built-in self-test), their the suitability of such devices in contributing to the performance of a safety function should be determined by evaluation of various elements including their development process (including verification process) and of their design.

7.142. Standardized hardware description languages HDLs with qualified and compatible software tools should be selected for programming the hardware HDL programmedable devices.

7.143. The design of hardware HDL programmed devices should:

a. Should Eensure that the behaviour of the hardware HDL programmed devices (HPD) is deterministic. Deterministic design may be achieved, for example, by using internal synchronous design. Synchronous design favours correctness (avoidance of metastability issues) and testability, and allows for the best use of software tools for design and verification tools.

b. Should Uuse only HPD hardware programmed device structures having well-defined implementation and behavioural properties. Methods for achieving well-defined implementation and behaviour include: development of a formalized description of the device

such as a register-transfer level description, (use of strict semantic and syntax rules, use of a '"safety"' subset of the hardware description languageHDL language, and use of pre-defined language and coding rules.

c. Should, tTo the extent feasible, support using the use of verification techniques based on proving of mathematical theorems proving..

d. Should Eexplicitly handle all possible cases of logic and all operating modes of the hardware programmed device, HPD such as reset, power-on and normal operation.

e. Should Bbe correct for all possible timing cases resulting from bounding variations in supply voltages, temperature and microelectronic processes.

f. Should Eensure that each function that is implemented in the hardware HPD programmed device is testable.

7.144. Post-route analysis should be used to demonstrate the compliance of the design and implementation of the device with the technology rules defined by the supplier of the design and with software tools for implementation tools.

7.145. The process of integrating the HPD designing of the hardware programmed device should be part ofintegrated into the overall system development process of the I&C system.

7.146. Verification and validation should:

a. Should be used to cConfirm that no unspecified function has been programmed that will affect the functioning of the hardware programmed device;HPD,

b. Should iInclude testing of all signal paths in the hardware programmed device;HPD,

c. Should aAddress the aspects of the system that are particular to hardware programmed devices;HPD, and

d. Should IInclude timing analysis and simulation of timings..

7.147. Environmental qualifications and analyses should be used to demonstrate that the inclusion of pre-developed items or auxiliary features does not degrade the ability of systems important to safety to perform their safety functions.

SOFTWARE TOOLS

7.148. Software tools should be used to support all aspects of the I&C development life cycle where benefits result through their use and where such software tools are available.

7.149. The use of appropriate software tools can reduce the risk of introducing faults during I&C development and can improve the probability that faults will be found during checking, verification, and validation. Consequently, the use of software tools can increase the integrity of the I&C development process, and hence increase component reliability. The use of software tools can also have economic benefits as they can reduce the time and human effort required to produce systems,

components, and software. Software tTools can be used to automatically check automatically for adherence to rules of construction and standards, to generate proper records and consistent documentation in standard formats, and to support change control. Software tTools can also reduce the effort required for testing and can maintain automated logs. Some specific development methodologies require the use of software tools.

7.150. Software tools used in the development of I&C systems include, for example:

- Software tools providing Infrastructure infrastructure tools and development support systems such as requirements management systems or integrated development environments;

- Automated circuit and raceway scheduling software;

- Transformational software tools, such as code generators, compilers, logic synthesizers, and tools that transform text or diagrams at one level of abstraction into another, usually lower, level of abstraction;

- Software tools automating Electronic electronic design automation software;

- Software tools for Vverification and validation tools, such as static code analysers, automated circuit testers, monitors of test coverage monitors, theorem proving assistants, electronic circuit simulators, and plant system simulators;

- Software Ttools for preparing system configuration data;

- Software tools for Cconfiguration management and control tools; and

- Software tools for Ssecurity testing tools for detecting known and unknown vulnerabilities.

7.151. A key element of integrated project support environments is to ensure proper control and consistency. If software tools are not available, consideration should be given to the development of new software tools might need to be considered.

7.152. The benefits and risks of using a software tool should be balanced against the benefits and risks of not using a software tool.

7.153. The important principle is to select choose Ssoftware tools that limit the opportunity for making errors and introducing faults, but maximize the opportunity for avoiding or detecting faults. System development might be adversely affected by the use of software tools in several ways. For example, software design tools for design might introduce faults by producing corrupted outputs, and or verification tools might fail to reveal certain faults or types of faults.

7.154. Software Ttools should be selected to remain available throughout the system's service life of the system and should be compatible with other software tools used during system development.

7.155. The functionality and limits of applicability of all software tools should be identified and documented.

7.156. ~~The~~ Software tools and their output should not be used outside their declared functionality or limits of application without prior justification.

7.157. For example, software tools cannot replace humans when judgement is ~~involved~~required. In some cases, software tool support is more appropriate than complete automation of a process.

7.158. Software t~~T~~ools should be verified and assessed ~~consistent~~ in accordance with the ~~tool~~ requirements on reliability ~~requirements~~of the software tool, the type of software tool, the potential ~~of~~ for the software tool to introduce faults or fail to make the user aware of existing faults, and the extent to which the software tool may affect redundant elements of a system or diverse systems.

7.159. Examples of situations that can affect the degree of verification and assessment ~~needed~~ necessary include, for example:

- Software T~~t~~ools that have the ability to introduce faults ~~need to~~should be verified to a greater degree than software t~~t~~ools that are demonstrated not to ~~not~~ have that capability;

- Software t~~T~~ools that can fail to make the user aware of existing faults ~~need to~~should be verified to a greater degree than software tools that do not have that capability;

- Verification is not necessary for software tools when the output of the software tool is systematically and independently verified;

- Less rigour in ~~tool~~ the verification of software tools may be ~~accepted~~ acceptable if ~~there is~~provision has been made for mitigation of the consequences of any potential software tool faults (e.g. by process diversity or system design).

7.160. The verification and assessment of software tools should take into account experience from prior use, including experience of the developers and experience gained from the processes in which the software tools are used.

7.161. The choice, verification and assessment of software tools should be justified and documented.

7.162. All software tools should be placed under appropriate configuration management.

7.163. Software t~~T~~ool settings used during the development, verification~~,~~ or validation of baseline equipment, software ~~or~~ and hardware description language ~~HDL~~ configured devices should be ~~recorded~~ documented in the development records.

7.164. ~~This~~ Such documentation is useful not only for ensuring consistency in the final software ~~consistency~~; it also helps in assessing the origin of a fault, which might lie in the source code, in the software tool, or in the software tool settings. Information about the tool settings used may be critical ~~to~~ in assessing the potential for common cause failures due to software tools.

QUALIFICATION OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY FOR SAFETY APPLICATIONS

7.165. This section provides guidance on the qualification of industrial digital devices of limited functionality that are to be used in nuclear power plant safety systems, but that have not been developed specifically for use in such applications. This guidance describes an approach to fulfilling the qualification recommendations of paras paragraphs 6.789 to 6.1345 for devices in this category.

7.166. A device of limited functionality has the following characteristics:

- It Ccontains pre-developed software or programmed logic;

- It is autonomous and performs only one conceptually simple principal function, that which is defined by the manufacturer and that which is not modifiable by the user;

- It iss not designed to be reprogrammable; and

- If it is reconfigurable, the configurability is limited to parameters relatinged to compatibility with the process being monitored or controlled, or interfaces with connected equipment.

7.167. All other devices are not 'industrial digital devices of limited functionality', i.e. those devices that have the following characteristics:

- They Uuse commercial computers (such as PCs, industrial computers or PLCsprogrammable logic controllers),);

- They aAre developed for an I&C platform;, or

- Are They are specifically developed for the nuclear industry.

7.168. Confirmation of the suitability and correctness of industrial digital devices of limited functionality for their intended functions should produce evidence for the following:

a. That Tthe principal functions of the device should meet the functional requirements for the application;

b. That Nneither operation nor failure of functions other than the principle principal function[34] can result in unsafe operation of the principle principal functions;

Functions other than the principle functions include, for example, functions used to maintain or configure the device and functions that are not needed for the intended application.

c. That Tthe device is free from systematic faults that could credibly cause near simultaneous common cause failure where similar devices are installed in elements of I&C systems that are redundant or diverse to each other;

---

[34] Functions other than the principal functions include, for example, functions used to maintain or configure the device and functions that are not needed for the intended application.

    d.   ~~That t~~The development process was systematic and followed the general principles outlined in ~~S~~section 2 of this Safety ~~g~~Guide; ~~and~~

    e.   ~~That q~~Quality assurance for manufacturing is sufficient to provide a basis for accepting the same or similar models of the device ~~which~~ that are manufactured at a later time.

7.169. Information developed during ~~safety~~ certification for safety purposes in other industries may be used as evidence to support device qualification. A certificate alone is not sufficient~~;~~ rather, it is the information developed by the certification process that may provide value.

7.170. If one or more of the recommendations above are not met, compensatory evidence should be provided that directly addresses the weaknesses in the evidence of suitability and correctness.

7.171. Such ~~C~~compensatory evidence ~~should~~:

    a.   Should ~~D~~directly address the requirements that it is intended to substantiate~~;~~ ~~and~~

    b.   Should ~~B~~be shown to be applicable to the device in question.

7.172. Examples of techniques to provide compensatory evidence include the following:

- Complementary tasks specific to the d~~D~~evice ~~specific complementary tests~~that are appropriate to the intended application and other elements of evidence of correctness~~;~~

- Evaluation of applicable and credible operational experience~~;~~

- Verification of design outputs~~;~~ ~~and~~

- Statistical testing.

7.173. Users may configure devices to make them suitable for the intended application. Such modifications should meet the criteria of this Safety ~~g~~Guide for design correctness and documentation, and should not invalidate previous operating experience or testing that is credited in the qualification.

7.174. Restrictions that are to be observed for the safe use of the device in the intended application should be identified.

7.175. Such restrictions include, for example:

- Restrictions on t~~T~~he applications for which the device is qualified;

- Specific options and unused functions that are to be enabled or disabled;

- Limits on operating environments and operating life;

- Measures that are to be observed during operation, testing~~,~~ and maintenance.

8. CONSIDERATIONS RELATING TO THE HUMAN-MACHINE INTERFACE ~~CONSIDERATIONS~~

CONTROL ROOMS

Main control room

8.1. SSR 2/1 Rrequirement 65 [1] states:

"A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions."

8.2. SSR 2/1 Rrequirement 59 [1] states:

"Instrumentation shall be provided for determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant, for obtaining essential information on the plant that is necessary for its safe and reliable operation, for determining the status of the plant in accident conditions and for making decisions for the purposes of accident management."

8.3. SSR 2/1 para. ~~paragraph~~ 5.57 states:

"The operator shall be provided with the necessary information:

(a) To assess the general state of the plant in any condition;

(b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);

(c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended;

(d) To determine both the need for and the time for manual initiation of the specified safety actions."

8.4. The I&C should allow ~~the~~ operators in the control room to initiate or take manual control of each function necessary to control the plant and maintain safety.

8.5. There should be sufficient displays in the control room to monitor all functions important to safety including the status of the plant, its ~~and~~ safety status and trends ~~of~~ in key plant parameters.

8.6. Safety classified indications and controls should be provided to implement emergency operating procedures ~~(EOP)~~ and severe accident management guidelines.

8.7. The guidance of para. ~~paragraph~~ 8.6 is not intended to preclude the option to use other means appropriate to satisfy the goals of the ~~EOP~~emergency operating procedures and severe accident management guidelines.

8.8. If a system or part of a system that is required to control the plant and maintain safety has failed or been intentionally made inoperative, this condition should be displayed in the control room and in locations where this information needs to be communicated to operators.

8.9. Changes in the status of safety systems should be annunciated, and the status should be indicated where this information is needed by operators.

8.10. Change~~s~~ in the status ~~needing~~ that necessitates an alarm might include deviations from normal operational limits, loss of availability of safety systems, or unavailability of standby equipment due to failure, maintenance or testing.

8.11. Advances in the functionality of alarm system~~s functionality~~ have enabled desirable features to be implemented, such as alarm processing, alarm prioritization and alarm control and management, ~~that~~ which help the operator to ~~effectively~~ monitor effectively and to respond to ~~plant~~ events at the plant.

8.12. The design of the main control room and supplementary control room should be such that no fire, internal hazard~~,~~ or postulated initiating event ~~PIE~~ can prevent ~~the~~ operators from ~~preserving~~ fulfilling the fundamental safety functions.

Supplementary control room

8.13. SSR 2/1 R~~r~~equirement 66 [1] states:

> "Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room."

8.14. Some plant designs may have more than one supplementary control room or may have supplementary control points that are not in a supplementary control room.

8.15. The supplementary control room should contain information displays for monitoring plant conditions as ~~needed~~ necessary to support the response to events ~~which~~ that may result from situations that necessitate evacuation of the main control room.

8.16. The supplementary control rooms should contain controls, indications, alarms and displays that are sufficient for the operator to bring the plant to a safe state, confirm that a safe state has been

reached and is maintained, and to monitor the status of the plant and the trends in key plant parameters.

8.17. Where it is impractical to provide in the supplementary control room all controls needed to fulfil the recommendation of para. paragraph 8.16, controls at local control points may be used.

8.18. Suitable provision outside the main control room should be made for transferring priority control to a new location whenever the main control room is abandoned.

ACCIDENT MONITORING

8.19. SSR 2/1 para. Paragraph 6.31 [1] states:

"Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the status of essential equipment and the course of accidents, for predicting the locations of release and the amount of radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis."

8.20. Information displays for monitoring accident conditions in the plant should be provided and displayed where appropriate (i.e., in the main control room and in supplementary control rooms) and in accordance with the roles and responsibilities of operating personnel.

8.21. The set of displays for monitoring accident conditions is usually called an 'aAccident mMonitoring sSystem' or a 'pPost aAccident mMonitoring sSystem. These Such displays may be provided as part of another system or may be a collection of individual instrument channels.

8.22. The accident monitoring system should indicate the values of variables needed by plant operators under in accident conditions by plant operators, to enable them:

a.   To take pre-planned manual actions to bring the plant to a safe state;

b.   To dDetermine if the fundamental safety functions are being achievedfulfilled;

c.   To dDetermine the potential for a breach or the presence of an actual breach of the barriers to preventing release of fission products release (e.g., the fuel cladding, the reactor coolant pressure boundary, and the containment);

d.   To Ddetermine the status and performance of plant systems necessary to mitigate the consequences of a design basis accident and design extension conditions and bring the plant to a safe state;

e.   To Ddetermine the need to initiate action to protect the public from the a release of radioactive material; and

f.   To Iimplement the severe accident management guidelines at the plant.

8.23. Instrumentation performing the indication functions given listed in para. paragraph 8.22 items a, b, c and c d should be classified as important to [?] safety and should be provided by I&C equipment capable of performing under design basis accident conditions and design extension conditions.

8.24. Instrumentation for severe accident monitoring should be designed and qualified for the full range of expected environmental conditions.

8.25. It may not always be feasible to ~~fully~~ type test fully the instrumentation monitoring severe accident monitoring ~~instrumentation~~ for the worst credible conditions that might be experienced. In such cases~~,~~ testing may be supplemented by other methods including, but not limited to, those described in para. ~~paragraph~~ 6.82.

Formatted: Highlight

8.26. Accident monitoring functions that support implementation of the severe accident management guidelines ~~should~~:

   a. Should ~~Nn~~ot be disabled by the operation, failure~~,~~ or mal-operation of I&C equipment that is not part of the severe accident monitoring instrumentation,

   b. Should ~~Ee~~ither not depend upon external power, or should have a designed capability to be powered from sources other than the ~~plant~~ electrical power system of the plant.

8.27. Classification as safety results in the need to fully apply the criteria of ~~Chapter~~ Section 67, including compliance with the single failure criterion for safety groups.

Formatted: Highlight

8.28. Where failure of a single display channel of instrumentation performing the functions ~~given~~ listed in para. ~~paragraph~~ 8.22 items a, b, c, and f could result in ambiguous indication, means should be provided that allows operators to resolve the ambiguity.

8.29. Failure of a display channel might cause a pair of redundant displays to disagree. Means for resolving ambiguity include, for example, provision of an additional channel or procedures for comparing the ambiguous reading to a different variable of known relationship to the reading in question.

8.30. The instrumentation provided for accident monitoring should cover the full range of parameter values that may be reached under accident conditions.

8.31. Displays of accident monitoring variables should be readily recognizable as such.

8.32. Electronic operator aids (e.g. a '~~s~~Safety ~~p~~Parameter ~~d~~Display ~~s~~System') should be provided to assist operators in rapidly determining the status of the plant, in confirm~~ing~~ operation of accident monitoring channels, in validat~~inge~~ their readings, and ~~to~~ in determin~~inge~~ the value of indirectly measured variables from direct measurements.

8.33. Computer guidance may enhance safety and ~~give~~ provide greater certainty that correct actions are taken.

8.34. In the design of modern control room~~s~~, ~~designs~~ the ~~s~~Safety ~~p~~Parameter ~~d~~Display ~~s~~System ~~(SPDS)~~ and functions of the accident monitoring system ~~functions~~ are often integrated into the normal operator human-machine interface~~HMI~~. Advice may be limited to specific operations, or to accident scenarios, or it may cover all operations ~~for~~ including start-up and normal power situations.

8.35. Operator aids that are not dependent upon a power source should also be available for instrumentation performing the indication functions given in para. paragraph 8.22 items a, b, c, and f.

OPERATOR COMMUNICATIONS SYSTEMS

8.36. SSR 2/1 Requirement 37 [1] states:

"Effective means of communication shall be provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and to be available for use following all postulated initiating events and in accident conditions."

8.37. SSR 2/1 para. paragraph 5.66 [1] states:

"Suitable alarm systems and means of communication shall be provided so that all persons present at the nuclear power plant and on the site can be given warnings and instructions, in operational states and in accident conditions."

8.38. SSR 2/1 para. paragraph 5.67 [1] states:

"Suitable and diverse means of communication necessary for safety within the nuclear power plant and in the immediate vicinity, and for communication with relevant off-site agencies shall be provided."

8.39. Communications systems should be provided for operating personnel to securely interface securely with locations internally within the plant and externally without their having to leave the I&C systems that they are expected to monitor and control.

8.40. Systems provided for the operating personnel to communicate with each other and with off-site emergency services should not be made ineffective by any personnel protective equipment, postulated initiating event PIE or single malicious act.

8.41. The characteristics of I&C equipment should not preclude communications among operating personnel.

8.42. For example, if I&C equipment interferes with the communication radios, communication radios interfere with the I&C equipment, or personnel protection equipment precludes the use of telephones, other forms of communications may be needednecessary.

8.43. The main control room, the supplementary control room, and the emergency controltechnical support centre should have at least two diverse methods for communications with the following:

a. Areas where communications are needed during aAnticipated oOperational oOccurrences or aAccident cConditions;

b. Emergency response facilities such as the tTechnical sSupport Centercentre, the oOperational sSupport Center centre [?] and the eEmergency oOperations fFacilityresponse organization; and

    c.   Associated facilities.[35]

    ~~Associated facilities include other facilities that might be affected by operation of the nuclear unit, e.g., other units on the same site.~~

8.44. Examples of diverse communications methods include~~:~~ email, data, fax, video links, landline, satellite and cell telephones~~,~~ and portable radios.

8.45. The diverse communications links identified above ~~should be~~:

    a.   Should be d~~D~~esigned such that they will not both be affected by the same failure, internal hazard~~s~~, external hazard~~s,~~ or postulated initiating event~~PIE~~, and

    b.   Should be C~~c~~apable of operating independently of both the plant power systems and off-site power systems.

8.46. Communications systems should be provided for making announcements that can be heard by all personnel on the site and in the plant.

GENERAL ~~HFE~~ PRINCIPLES RELATING TO HUMAN FACTORS ENGINEERING FOR I&C SYSTEMS

8.47. SSR 2/1 Requirement 32 [1] states:

"Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process."

8.48. SSR 2/1 para. ~~paragraph~~ 5.55 [1] states:

"The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the effects of operating errors on safety. The design process shall pay attention to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant."

8.49. SSR 2/1 para. ~~paragraph~~ 5.56 [1] states:

"The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make a decision to act shall be simply and unambiguously presented."

8.50. The design of the H~~h~~uman m~~M~~achine i~~I~~nterface ~~(HMI) design~~ should retain positive features associated with reference designs and should avoid problems that have resulted in poor operational experience.

---

[35] Associated facilities include other facilities that might be affected by operation of units of the nuclear power plant, e.g., other units on the same site.

8.51. The design of ~~HMI~~ human machine interface required for the supervisory control of safety systems should ~~follow~~ apply the principles of defence -in -depth.

8.52. The I&C system should provide operators with the information necessary to detect changes in system status, to diagnose the situation, to affect the system (when necessary)~~,~~ and to verify manual or automatic actions.

8.53. A satisfactory design will take into account ~~operator~~ the cognitive processing capabilities of operators as well as process-related time constraints.

8.54. The design should ensure that the longest time from operating any control to when the input is acknowledged by the control system is acceptable to the operators.

8.55. The I&C system design should ensure that operator tasks can be performed within the time specified by system requirements.

8.56. Information flow rates and control performance that are too fast or too slow could diminish ~~operator~~ the performance of operators.

8.57. Where possible, the I&C system should be designed to prevent and detect operator errors, where an action might be taken in an incorrect context, or with an inappropriate plant configuration. This includes validation of setpoint changes to control systems, monitoring systems~~,~~ and protection systems.

8.58. The I&C system should provide simple, comprehensible notification of detectable operator errors, and should make available simple, effective methods for recovery.

8.59. No single operator error should result in loss of reactor control.

8.60. The human machine interface~~HMI should~~:

   a.   ~~Should, A~~as far as practica~~ble~~, accommodate the different roles and responsibilities of the many types of operating personnel expected to interact with the systems;

   ~~c.~~b. ~~Should B~~be designed with primary attention given to the role of the operator who is responsible for the safe operation of the equipment;

   ~~d.~~c. ~~Should s~~Support the development of a common situational awareness ~~of~~ on the part of the control room crew, e.g. via large wall--mounted plant status displays.

   ~~e.~~d. ~~Should P~~provide an effective overview of the plant status;

   ~~f.~~e. ~~Should, A~~as far as practica~~ble~~, apply the simplest design consistent with function and task requirements;

   ~~g.~~f. ~~Should B~~be designed to minimize reliance on operator training;

    h.g. Should Ppresent information such that it can be rapidly recognized and understood by operators;[36]

      ~~Display of information in an easily understood form reduces operator cognitive workload. HMI designs that meet this guidance will, for example, minimize the need for operators to make mental calculations, transformations, and the use of recall memory.~~

    i.h. Should Aaccommodate failure of analogue and video displays without significant interruption of control actions; ~~and~~

    j.i. Should Rreflect consideration of human physiological characteristics[37], characteristics of human motor control, and anthropometry.

      ~~Human physiological characteristics include, for example, visual/auditory perception and biomechanics (reach and motion).~~

8.61. The human machine interface~~HMI~~, procedures, training systems, and training should be consistent with each other.

8.62. The presentation of information should be integrated into a harmonized arrangement that optimizes the ~~operators'~~ understanding of operators of the ~~plant's~~ status of the plant and the activities necessary to control the plant.

8.63. The operation and appearance of the human machine interface ~~HMI~~ should be consistent across information and control locations and platforms and should reflect a high degree of standardization.

8.64. The use of a single language and compatible script for all descriptive identification and labels ~~is desirable~~should be considered.

8.65. All aspects of the I&C system (including controls and display arrangements ~~and displays~~) should be consistent with the ~~operators'~~ mental models used by operators and with established conventions.

8.66. Mental models incorporate the ~~operator's~~ understanding of operators and expectations about how the system behaves. ~~These~~ Such models are developed through training, use of procedures, and experience.

8.67. The conventions for each type of control and display are determined in design and are then followed fully in the identification, layout and arrangement of the controls, and of the displays of plant conditions.

---

[36] Display of information in an easily understood form reduces operator cognitive workload. Designs of the human machine interface that meet this guidance will, for example, minimize the need for operators to make mental calculations abd transformations and use recall memory.

[37] Human physiological characteristics include, for example, visual/auditory perception and biomechanics (reach and motion).

Considerations for human-automation interaction

8.68. The methodology for determining the appropriate allocation of I&C functions to humans and I&C systems should be systematic and consistently applied.

8.69. Factors that might affect the allocation of functions to humans versus machines include:

- Potential human work-load under all operating modes;

- Requirements for Aaccuracy and repeatability requirements;

- Time factors;

- Types and complexities of decision-making and action logic needed;

- Environmental factors; and

- Human physiology and anthropometry.

8.70. SSR 2/1 para. paragraph 5.59 [1] states:

> "The need for intervention by the operator on a short time scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act."

8.71. The I&C should provide automatic actions when operators are not capable of reliable and timely manual action, or when reliance on manual control would place an unreasonable burden on the operator.

8.72. The I&C should provide operators with the information necessary to monitor each automatic function.

8.73. The I&C should give the operators multiple means to verify automatic actions.

8.74. The information provided to monitor automatic functions should be displayed at a rate and level of detail (e.g., identification of targets or goals, opportunities for verification) that the operator can monitor effectively.

8.75. The I&C should allow the operators to manually initiate or control each function necessary to control the plant and maintain safety.

Considerations for task design in I-&-C systems

8.76. The operator's role of the operator should consist of purposeful and meaningful tasks that enable personnel to maintain familiarity with the plant and maintain a level of workload that is not so high as to negatively affect performance negatively, but sufficient to maintain vigilance.

8.77. The I&C should have all characteristics that have been identified as necessary by the a tTask aAnalysis.

8.78. TheA task analysis will should consider all plant states, all plant operating modes and all groups of operating personnel, e.g., reactor operator, turbine operator, shift supervisor, field operator, safety engineer, operation and maintenance staff. Task analysis will should provide design input for the characteristics of I&C such as the accuracy, and precision of display information, system response time, physical layout, type of controls, displays, and alarms. and the integration of soft controls within information displays.

8.79. The human machine interface HMI should permit displays and controls on video display units to be formatted in a configuration that is most convenient for the task where this offers advantages in the performance of tasks performance.

8.80. Examples of where such configurability is advantageous include where different configurations might better accommodate different levels of operator experience, or where different configurations might be more effective during in different operating modes.

8.81. All aspects of the human machine interface HMI (formats, terminology, sequencing, grouping, and operator's decision-support aids for the operator) should reflect an obvious logic based on task requirements or some other non-arbitrary rationale.

8.82. The relationship of each display, control, and data-processing aid to the associated tasks and functions should be clear.

8.83. The HMhuman machine interfaceI should present information to operators in forms and formats that are consistent with the results of the tTask aAnalysis.

8.84. The I&C should provide control options that cover the range of potential operator actions identified by the tTask aAnalysis.

8.85. The I&C should give the operators multiple means to carry out actions.

8.86. The I&C should permit operators to complete tasks with a minimum number of actions.

Considerations for accessibility and the working environment

8.87. SSR 2/1 para. paragraph 5.61 [1] states:

"The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts."

8.88. In areas where operating personnel are expected to monitor and control plant systems, the necessary provisions should be made to ensure suitable conditions in the working environment, and to protect against hazardous conditions.

8.89. Normal aspects of the working environments to be considered include lighting, temperature, humidity, noise, vibration, and in cases where continuous monitoring is required, facilities such as rest areas and washrooms.

8.90. Hazards to be considered include, for example, include radiation, smoke and toxic substances in the atmosphere.

8.91. SSR 2/1 para. paragraph 5.60 [1] states:

"The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel."

8.92. When human machine interface HMI stations are distributed[38], operating personnel should have means to access these different locations in a safe and timely manner.

8.93. Examples of distributed human machine interface HMI stations include the supplementary control room and other field locations where operator actions are expected to occur.

8.943. One way of establishing suitable means of access is to provide a qualified route, with provisions to protect against potential internal hazards or external hazards, to supplementary control points and other field locations where operator actions are expected to occur.

RECORDING OF HISTORICAL DATA

8.945. The human machine interface HMI should provide the capability to record, store, and display historical information where such displays will help operating personnel identify patterns and trends, understand the past or current state of the system, perform post incident analysis, or predict future progressions.

9. SOFTWARE

GENERAL

9.1. The guidance recommendations inof this section applies to all types of software for application in or to I&C equipment important to safety, e.g., operating systems, pre-developed software or firmware, software to be specifically developed for the project, or software to be developed from an existing pre-developed equipment family of hardware or software modules.

9.2. Digital systems require different approaches to the assessment of reliability than analogue systems. Reliability is inferred from the assessment of the quality of production activities, and the results of verification and validation. Software by its nature and intent tends to allows for a much larger design space than (electrical or mechanical) hardware. If not systematically constrained, it can become defect-prone and unverifiable.be complex and prone to design errors which may be more difficult to detect than in an analogue or mechanical system. Complexity in software implementation

---

[38] Examples of distributed human machine interface stations include the supplementary control room and other field locations where operator actions are expected to occur

Formatted: Font: 10 pt

can generate additional faults in design, increase the difficulty in detecting and correcting faults, introduce failure modes and effects that are not present in simpler designs, and reduce the confidence in any demonstration of conformance to safety system design criteria. such as independence, testability and reliability.

9.3. The guidance on management systems and lifecycle processes given provided in Ssection 2 is particularly relevant to software since the activities covered are integral to effective software development.

9.4. SSR-2/1 Rrequirement 63 [1] states:

"If a system important to safety at the nuclear power plant is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the lifetime service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system."

9.5. Development of software for systems should follow a previously predefined life cycledevelopment process, be duly planned and documented and include thorough verification and validation. (See Ssection 2.)

SOFTWARE REQUIREMENTS

9.6. All software necessary to satisfy the I&C system requirements, including reused or automatically generated code, should have documented requirements in appropriate form complying with the recommendations of in this section.

9.7. Software requirements should be established using a predetermined combination of techniques commensurate with the system's importance to safety of the system.

9.8. Techniques for establishing requirements might include, for example, include the use of specification languages with well-defined syntax and semantics, models, analysis, and review.

9.9. The developers of software requirements should have an appropriate understanding of the underlying system design basis for the system as described in Ssection 3.

9.10. Understanding of the system design basis is needed necessary to ensure that software requirements properly implement satisfy essential properties of the system properties. Relevant issues include the following:

- Potential failure conditions;.

- Operation Operating modes;.

- Safety Mmonitoring for safety purposes;.

- Self-supervision;.

- Failure detection.;

- Safe conditions to be attained in the event of a detected but unrecoverable failure;.

- Other fail--safe behaviour;, and

- Input and output relationships relevant to safety.

9.11. The specification of Ssoftware rRequirements Specifications should:

a. Should Ddefine what each individual software item is required to do and how it will interact with other components items of the system.

b. Should Ooriginate from the relevant processes of the I&C life cycledevelopment process (including consideration of system hazards identified in previous analyses) and from processes that interface with the I&C life cycledevelopment process, e.g., human factors engineering and computer security activities. See Fig. 2.

c. Should Bbe written as far as possible in terms of what needs to be achieved rather than how they are to be designed for and implemented.

d. Should Bbe complete, unambiguous, consistent, readable, understandable to their target audience (e.g., domain experts, safety engineers, software designers), verifiable and traceable.

e. Should satisfy the system requirements allocated to the software items, including the quality requirementsAaddress, as appropriate, the sSystem rRequirements allocated to software.

f. Should sSpecify as necessary the required minimum precision, numerical accuracy, a description of the interfaces[39], independence of execution threads, self-supervision, timing performance[40] and security[41].

   Interfaces examples include those between the software and the operator, sensors and actuators, computer hardware and other software, and between systems. Timing performance includes failure detection and recovery times. Security examples are validity checks and access privileges.

g. Should Iinclude the necessary level of reliability and availability to be achieved.[42]

   The level of reliability and availability might be defined quantitatively, or qualitatively, for example in terms of the supporting software requirements referred to above and the development processes (e.g., standards compliance).

---

[39] Interfaces examples include those between the software and the operator, between sensors and actuators, between computer hardware and other software, and between systems.

[40] Timing performance includes failure detection and recovery times.

[41] Examples of security are validity checks and access privileges.

[42] The necessary levels of reliability and availability might be defined quantitatively, or qualitatively, for example in terms of the supporting software requirements referred to in a to f, and the development processes (e.g. compliance with standards).

h.   Should Aallow for the capabilities of the computers, software tools and similar existing systems to ensure that the software requirements are feasible.

i.   Should Rrefer to, include, or be complemented by additional information applicable to its the target audience, e.g., background information for specific requirements, risk considerations, recommendations for the design of functions or safety features, to the extent necessary to ensure it is understandable by its the target audience.

j.   Should Ddefine any functions, behaviour or interactions that it is particularly important the software does not do.

9.12. Where design constraints are necessary, these should be specified, justified and traceable.

9.13. The origin of every software requirement should be documented sufficiently to facilitate verification, validation, traceability to higher-level documents and a demonstration that all relevant requirements have been addressed.

9.14. A requirements tracking system should be used so that the software requirements can be traced through the design, implementation, integration, and validation stages of the development project.

9.15. Software requirements important to safety should be identified as such.

SOFTWARE DESIGN

9.16. The completed software design should be unambiguous, correct and demonstrably complete with respect to the software requirements, consistent, well-structured, readable, understandable to their target audience (e.g., domain experts, safety engineers, software designers), verifiable, able to be validated, traceable, maintainable and documented.

9.17. The software design should be established and kept current using a predetermined combination of techniques commensurate with the system's importance to safety of the system.

9.18. Such Ttechniques might include descriptions, logic diagrams and graphical representations with well-defined syntax and semantics, models, analysis and review.

9.19. The software design should be developed with an understanding of the origin of the safety requirements.

9.20. Parts of the software design should be distinguished sufficiently to enable useful traceability of requirements through the design.

9.21. The design of safety system software for safety systems should maximize simplicity at all levels, including overall architecture, external interfaces, internal interfaces between modules, and detailed design.

9.22. Simplicity in design is a key means for achieving and demonstrating safety, but will always involve trade-offs, for example with functionality, flexibility and cost. Whereas the recommendation of para. paragraph 9.21 applies only to safety systems, simplicity is a worthwhile goal for software in

a system of a lower safety class~~ification~~. For systems of a lower safety class~~ification,~~ the balance between safety and complexity is different and higher levels of complexity may be accepted.

9.23. The software design architecture should be structured to allow for future modification, maintenance and upgrades.

9.24. The software architecture should be hierarchical to provide graded levels of abstraction.

9.25. Use of information hiding, where possible, is encouraged to enable piecewise review and verification and to aid modification.

9.26. The software design should include the interfaces between the software and its external environment.

9.27. The software design should include the detailed design of all software modules.

9.28. The description of a software module should completely define its function, its interface with other modules and the context of its function in the overall software.

9.29. Software modules performing similar functions should have a consistent structure.

9.30. Module interfaces should be consistent.

9.31. Both sides of each interface between modules should match, there should be a consistent use of variable names between module input and output interfaces, and, as far as possible, recursive calls should be avoided.

9.32. If the system includes multiple processors and the software is distributed among them, the software design should define which software process runs on which processor and where data and displays are located.

9.33. The software design should support deterministic behaviour and timing of safety systems.

9.34. Communication protocols should comply with the recommendations of para~~paragraph~~s 7.79 to 7.94.

9.35. As the design is refined~~,~~ the need for additional features for fault detection and self-supervision ~~features~~ should be considered and included in the software design. See paras ~~paragraphs~~ 6.166 to 6.172.

9.36. On detection of a failure ~~detection~~, appropriate action should be taken to meet the software requirements in terms of recovery, halting procedures, and error messages and logs, to ensure that the system is maintained in a safe condition.

9.37. The software design documentation should include those constraints on implementation ~~constraints~~ that need to be observed during the design phase.

9.38. Such constraints on implementation ~~constraints~~ may include any need to ensure diversity, and

particular attributes of the programming languages, compilers, subroutine libraries and other supporting software tools.

9.39. ~~These~~ Such constraints should be justified or be traceable to higher-level requirements or constraints.

9.40. For systems other than safety systems, it may be sufficient for constraints on implementation ~~constraints on~~ for a proprietary system to be traceable to the ~~supplier's~~ standard documentation provided by the supplier.

9.41. The software design architecture should account for constraints on modules and interfaces that might result from the decision to ~~use~~ apply diversity.

9.42 The software design should take into account ~~the~~ best practices in terms of information security, in order to avoid the creation of vulnerabilities by design, that are easy to exploit by malware or hackers, and difficult to fix.

9.43 Where appropriate, software design should be peer reviewed.

SOFTWARE IMPLEMENTATION

9.43. The software implementation should:

   a.   Should ~~Bb~~e correct and complete with respect to the software requirements and complete with respect to design, well structured, readable, verifiable, traceable, maintainable and documented appropriately.

   b.   Should ~~Bb~~e established using a predetermined combination of techniques commensurate with the ~~system's~~ importance to safety of the system, covering languages, software tools, coding practices, analysis, review and testing.

   c.   Should ~~Dd~~emonstrably address all software requirements and the software design.

   d.   Should ~~Bb~~e simple and readily understandable, with readability and maintainability taking precedence over ease of programming.

   e.   Should ~~Ii~~nclude readable forms of the source code and executable code, the results of unit interface tests and module interface tests, and sufficient contextual information to verify the ~~code's~~ correctness of the code with respect to its specification.

9.44. All code should be adequately documented.

9.45. For safety systems, the availability of documentation for all parts of the code (including run-time support code and fault supervision functions) ~~enables~~ will enable the testing guidance of this Safety Guide to be met.

9.46. Coding rules should be prescribed before coding commences and ~~their~~ adherence to the rules should be verified.

9.47. Data structures and naming conventions should be consistently applied.

9.48. The software implementation should be subject to:

    a.   Defined procedures for change control (including impact analysis),;

    b.   Configuration management;, and

    c.   Ensuring appropriate test coverage for the results of all changes.

9.49. The programming language (or language subset) used should be adequate in terms of expressive power, avoidance of insecurities, level of abstraction, support for modularization and information hiding, compilation and run time checking, and error handling.

9.50. The programming language used for safety systems should support simple implementation.

9.51. The choice of programming languages and functional definition methods (such as logic diagrams or graphical representations) used should be based on a systematic assessment of the requirements on functionality and integrity requirements of for the processes involved.

9.52. For safety systems, the choice of programming language should be justified and documented.

9.53. For safety systems, the language syntax and semantics should be complete, available, and rigorously defined.

9.545. Software functions are programming elements that perform a specific task. They might be intrinsic to the programming language, contained in libraries or otherwise pre-developed.

9.554. Software functions should be used with the aim of maximizing simplicity and should be identified, have well defined interfaces and always be called in accordance with the relevant restrictions in on their use.9.55. Software functions are programming elements that perform a specific task. They might be intrinsic to the programming language, contained in libraries or otherwise pre-developed.

9.56. If an operating system is used, it should be or have been thoroughly and satisfactorily tested and its suitability for the target application should be justified.

9.57. For safety systems, any operating system software should comply with the full recommendations of this Safety Guide.

9.58. A suitable set of software tools for implementation tools should be selected with the aim of minimizing error. See paras paragraphs 7.148 to 7.164 for relevant recommendations.

9.59. The recommendations in this section apply to all possible combinations of the use of code generation and classical software development.

9.60. Software diversity (i.e., the use of independent development teams, and/or different methods, languages, timing, order of functions or, algorithms) may be considered as a means of reducing the likelihood and effect of software common cause failures in software. However, this such software diversity can introduce design constraints that could themselves lead to new failures.

9.61. Precautions should be taken to ensure that the independence between systems supporting different levels of defence in depth is not jeopardized by the use of identical software, such as the operating system, network communication, or other running support software.

9.62. ~~Implementation T~~teams implementing software should be trained on secure development techniques.

SOFTWARE VERIFICATION AND ANALYSIS

9.63. Software requirements, design and implementation should be verified against the specification of the I&C system requirements ~~specification~~.

9.64. Verification of traceability should be an on-going activity to ensure that shortfalls are addressed as early as possible and hence necessary changes remain practicable.

9.65. The results of each phase in the software life cycle ~~phase~~ should be verified against the requirements set by the previous phases.

9.66. A software verification plan should be produced that documents the following:

   a.   The verification techniques to be used;

   b.   Details of or references to the procedures to be used in applying each technique, including its scope and depth;

   c.   How non-functional requirements and constraints will be demonstrated to be met;

   d.   Criteria for determining when sufficient verification has taken place, including targets for completeness with respect to the outputs of the previous phase and for structural coverage of the functional tests, and how these will be demonstrated;

   e.   The means by which results will be recorded;

   f.   The means by which non-compliances and faults will be recorded and resolved;

   g.   The team or teams performing the verification and their independence from the designers of the software;

   h.   The functionality of any software tool for verification ~~tool~~, including expectations and limitations on how it is to be used (e.g., domain, language, process); ~~and~~

   i.   The rationale for each of the elements listed in items a to h, ~~above~~ and justification that the verification will be ~~this isthese elements are~~ sufficient for software ~~of~~ in the system of the safety class~~ification~~ to which it is applied.

9.67. Verification should include the following techniques:

   a.   Manual examinations such as reviews, walk-throughs, inspections, and audits;

   b.   Static analysis of the source code; ~~and~~

   c.   Dynamic analysis.

9.68. Static analysis should be performed on the final version of the software.

9.69. Static analysis techniques used will differ according to the ~~system's~~ importance to safety of the system. Static analysis includes techniques such as verification of compliance with design and~~,~~ coding~~,~~ ~~and~~ standards ~~constraints~~, analysis of control, data and information flow ~~analysis~~, symbolic execution, and formal code verification.

9.70. All non-functional requirements implemented in software should be verified.

9.71. Relevant operating experience should be used to identify anomalies for correction~~,~~ and to provide further confidence in ~~its~~ the dependability of the software.

9.72. Relevant operating experience can supplement, but cannot replace~~,~~ other verification techniques.

9.73. ~~See~~ Pparagraphs 7.148 to 7.164 ~~for~~ provide guidance relevant to the use of tools for software verification and analysis.

9.74. A test strategy (e.g.~~,~~ a bottom-up strategy or a top-down strategy) should be determined for verification and validation of the software implementation.

9.75. The ~~test case~~ specifications ~~for~~of the test cases ~~used~~ should ensure adequate testing of the following:

a. Interfaces (such as module-module interfaces, software-hardware interfaces, system boundary interfaces)~~;~~.

b. Data passing mechanisms and interface protocols~~;~~.

c. Exception conditions~~;~~.

d. The full range of each input variable (using techniques such as equivalence class partitioning and boundary value analysis)~~;, and~~.

e. All modes of system operation.

9.76. To facilitate regression testing, test plans should ensure that tests are repeatable and the test results are recorded.

9.77. It is also desirable to minimize the human intervention required for repeated tests.

9.78. ~~GS-G-3.1,~~ Ref~~erence~~ [35] provides guidance for ensuring suitability of measuring and test equipment used for testing.

9.79. The ~~test case~~ specifications of the test cases and their effectiveness ~~of the test case used~~ should be reviewed and any shortfalls against the targets in the verification plan should be resolved or justified.

9.80. Verification should be carried out by teams, individuals~~,~~ or organizational groups that are independent of the designers and developers.

9.81. The code should be reviewed to check for software security vulnerabilities, using automated software tools and complemented by manual review of the critical sections of the code (e.g. ~~I/O~~input/output handling, exception handling)

9.82 All Ooutputs from Aallof the I&C system outputs should be monitored during the verification and any deviation from the expected results should be investigated and documented.

9.83. Any shortfall in the verification results against the verification plan (e.g., in terms of the test coverage achieved) should be resolved or justified.

9.84. Detected Any errors detected should be analysed for cause and should be corrected under the controlby means of agreed modification procedures and regression tested as appropriate.

9.85. The error analysis should include an evaluation of applicability to other parts of the I&C systemss.

9.86. Records of the numbers and types of anomalies discovered should be maintained, reviewed for their insight into the development process, and used to implement appropriate process improvements for the benefit of the current and future projects. (See GS-G-3.1, Ref. [35] paras paragraphs 6.50 to 6.77 and GS-G-3.5, Ref. [46] paras paragraphs 6.42 to 6.69.)

9.87. Verification and analysis documentation should provide a coherent set of evidence that the products of the development process are complete, correct, and consistent.

9.88. The verification results, including test records, should be documented, maintained and be kept available for quality assurance audits and third party assessments.

9.89. Traceability of design documents should include the sequential links between the documentation of each lifecycle phase and the functional requirements.

9.90. The documentation of the test results should be traceable to and from the test case specifications forof the test cases used and should indicate which results failed to meet expectations and how these were resolved.

9.91. The tTest coverage should be clearly documented.

9.92. For safety systems, it should be possible to trace each of the test cases using a traceability matrix showing the linkage between software requirements, design, implementation and testing.

9.93. For safety systems, the resulting application should be submitted to security specific testing to ensure that is specifically for computer security purposes (such as penetration testing), to make sure that common security vulnerabilities are not easy to detect, and to allow for continuous improvement of the software design and implementation of the software.

9.94. Test documentation should be sufficient to enable the testing process to be repeated with confidence of achieving the same results.

PRE-DEVELOPED SOFTWARE

9.95. For safety systems, pPre-developed Software used in I&C safety systems should have the same level of qualification as for software that is written specifically for the application.

9.96. Pre-developed software functions should comply with the recommendations of paras ~~paragraphs~~ 2.1~~100908~~ to 2.11~~97~~8.

9.97. For systems important to safety that are not safety systems, the pre-developed software should have user documentation that describes the following:

a. The functions provided;~~,~~

b. The interfaces, including the roles, types, formats, ranges and imposed constraints ~~of posed by~~ of inputs, outputs, exception signals, parameters and configuration data;~~,~~

c. The different modes of behaviour and the corresponding conditions of transition, if applicable;~~,~~

d. Any constraint to be satisfied when using the pre-developed software;~~,~~

e. A justification that the pre-developed software is correct with respect to the ~~above~~ user documentation's description of aspects a to d;~~, and~~

f. A justification that the functions are suitable for the I&C system.

SOFTWARE TOOLS

9.98. Recommendations for software tools are ~~given~~ provided in paras ~~paragraphs~~ 7.148 to 7.164.

THIRD PARTY ASSESSMENT

9.99. A third party assessment of safety system software should be conducted concurrently with the software development process.

9.100. The objective of ~~the~~ such a third party assessment is to provide a view on the adequacy of the system and its software that is independent of both the supplier of the system and/or software and the operating organization. Such an assessment may be undertaken by the regulatory body or by a body acceptable to the regulatory body.

9.101. ~~It is important that~~ It is important that ~~pP~~proper arrangements ~~are should be~~are made with the software originator to permit third party assessment.

9.102. The assessment should involve an examination of the following:

a. The development process (e.g.~~,~~ through quality assurance audits and technical inspections, including examination of lifecycle documents, such as~~,~~ plans, software specifications~~,~~ and the full scope of test activities); ~~and~~

b. The final software (e.g.~~,~~ through static analysis, inspection, audit and testing), including any subsequent modifications.

REFERENCES

[1]   INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR 2/1, IAEA, Vienna (2012).

[2]   International Atomic Energy Agency, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standard Series No. NS-G-1.1, IAEA, Vienna (2000).

[3]   International Atomic Energy Agency, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Guide Series No. NS-G-1.3, IAEA, Vienna (2002).

[24]   INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, Safety Requirements No. GS-R-3, IAEA, Vienna (2006).

[35]   INTERNATIONAL ATOMIC ENERGY AGENCY Safety Guide, Application for of the Management System for Facilities and Activities, IAEA Safety Standards Series No. Safety Guides Series No. GS-G-3.1, IAEA, Vienna (2006).

[46]   INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. Safety Guide Safety Guide GS-G-3.5, IAEA, Vienna (2009).

[57]   INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, General IAEA Safety Standards Series Safety Requirements No. GS-R Part 4, IAEA, Vienna (2009).

[68]   INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, IAEA, Vienna (2007).

[79]   INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems of for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-34 Safety Guide Series DS-430, IAEA, Vienna (Draft August 2011 in preparation).[[DS430]]

[8]   INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[910] INTERNATIONAL ATOMIC ENERGY AGENCY, Modifications to Nuclear Power Plants, IAEA Safety Standards Safety Guide Series No. NS-G-2.3, IAEA, Vienna (20010).

[1011] INTERNATIONAL ATOMIC ENERGY AGENCY, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (1999).

[112] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge ofn Instrumentation and Control Systems in Nuclear Power Plants: A Reference Book, NP-T-3.12, IAEA, Vienna, (20112).

[13]   INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, Nuclear Security Series No. 17, IAEA, Vienna (2011).

[124]   INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. SSG-3, IAEA, Vienna (2010).

[135]   INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. SSG-4, IAEA, Vienna (2010).

[146]   INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. SSG-2, IAEA, Vienna (2009).

[157]   INTERNATIONAL ATOMIC ENERGY AGENCY, Commissioning for Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-2.9SSG-28, IAEA, Vienna (201403).

[168]   INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-Sservice Inspection in Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-2.6, IAEA, Vienna (2001).

[17]   INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

[189]   INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG- Report 10, IAEA, Vienna (1996).

[1920]   INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1, INSAG- Report 12, IAEA, Vienna (1999).

[21]   INTERNATIONAL ATOMIC ENERGY AGENCY, Classification of Structures, Systems and Components in Nuclear Power Plants, Safety Guide DS 367, IAEA, Vienna (2013).

[2022]   INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-1.7, IAEA, Vienna (2004).

[213]   INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-1.11, IAEA, Vienna (2004).

[224] INTERNATIONAL ATOMIC ENERGY AGENCY, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Reports Series No. 3, IAEA, Vienna (1998).

[235] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-1.6, IAEA, Vienna (2003).

[246] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-1.5, IAEA, Vienna (2003).

[257] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management for Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-2.12, IAEA, Vienna (2009).

[268] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[279] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[2830] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (201107).

[2931] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-2.2, IAEA, Vienna (2000).

[3032] INTERNATIONAL ATOMIC ENERGY AGENCY, The Operating Organization for Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-2.4, IAEA, Vienna (2002).

[313] INTERNATIONAL ATOMIC ENERGY AGENCY, Conduct of Operations at Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-2.14, IAEA, Vienna (2008).

[324] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, IAEA Safety Standards Series Safety Guide Series No. NS-G-1.13, IAEA, Vienna (2005).

[33]   INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Emergency Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.8, IAEA, Vienna (2004).

ANNEX I. BIBLIOGRAPHY OF INTERNATIONAL I&C STANDARDS

I-1. SSR 2/1 rRequirement 9 [I-1] states:

"Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national codes and standards".

I-2. This Ssafety Gguide gives provides high-level recommendations that are widely accepted among the IAEA Mmember Sstates. Beyond the guidance provided by the IAEA guidance, there exists a large body of national and international standards that give more detailed recommendations about design methodologies and system characteristics that support compliance with IAEA SSR 2/1Ref. [I-1]. It is expected that designers, users, and regulator bodies will take advantage of the information in these standards.

I-3. Two standards development organizations are responsible for most of the internationally used standards for I&C in nuclear power plants I&C: the International Electrotechnical Commission's (IEC) Subcommittee 45 (SC45A), and the Institute for Electrical and Electronic Engineers' (IEEE) Nuclear Power Engineering Committee (NPEC). Each organization has developed a large number of standards. Both organizations produce standards that respond to the common principles underlying the requirements of SSR 2/1Ref. [I-1] and the recommendations of this guide. Consequently, either set of standards can be used to further interpret the recommendations of this Safety gGuide.

I-4. This annex is intended to help readers understand the relationship between this guide Safety Guide and the IEEE and IEC standards. Table I-1 lists the IEC and IEEE standards that have a strong relationship with the recommendations of this guideSafety Guide. Table I-1 is not a complete list of either set of standards, but it identifies the entry points into the sets of IEC and IEEE standards sets.

I-5. Table I-2 shows how these entry standards relate to the major topic areas of this guideSafety Guide.

I-4. A concerted effort was made to avoid conflicts between the recommendations of this guide Safety Guide and the standards of IEEE and IEC. Members of both the IEC and the IEEE standards committees participated in the development of this guide Safety Guide and both standards organizations reviewed drafts to help identify and eliminate conflicts.

I-5. Users should nNevertheless, users need to recognize and take account for of the fact that there are important differences between the IEC and the IEEE standards.

I-6. IEC standards take the IAEA Safetyr Requirements and Ssafety Gguides as fundamental inputs for the development of their standards. As a result, the IEC standards deal with items important to safety and take the guidance on I&C systems provided by the IAEA I&C safety guide as the source of general recommendations.

I-7. IEEE standards focus largely on safety items and, therefore, their guidance directly applies to a smaller set of functions, systems and equipment than this ~~guide~~Safety Guide does. Nevertheless, the guidance of IEEE can be applied to safety related items (items important to safety ~~but~~ that are not safety system~~s items~~) using a graded approach.

I-8. IEEE standards do not take this ~~guide~~ Safety Guide as a reference. IEEE 603 is the equivalent of this Safety Guide ~~guide~~ in the IEEE framework of standards. Nevertheless, this ~~guide~~ Safety Guide and the IEEE standards respond to the same set of principles for the design of I&C systems. Note that IEEE standards often use the terms 'safety', 'safety related' and '1E' as equivalent to the IAEA term 'safety'. IEEE does not have a term that is equivalent to 'safety related' as it is used by IAEA.

I-9. ~~IAEA report NP-T-3.12,~~ Ref~~erence~~. [I-29], contains a more extensive bibliography of standards for the design of I&C systems.

Table I-1 International standards having a strong relationship to this Safety ~~g~~Guide

IEC 60515	Nuclear power plants - Instrumentation important to safety - Radiation detectors - Characteristics and test methods
IEC 60568	Nuclear power plants - Instrumentation important to safety - In-core instrumentation for neutron fluence rate (flux) measurements in power reactors
IEC 60671	Nuclear power plants - Instrumentation and control systems important to safety - Surveillance testing
IEC 60709	Nuclear power plants - Instrumentation and control systems important to safety – Separation
IEC 60737	Nuclear power plants – Instrumentation important to safety – Temperature sensors (in-core and primary coolant circuit) - Characteristics and test methods
IEC 60780	Nuclear power plants - Electrical equipment of the safety system - Qualification
IEC 60880	Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions
IEC 60964	Nuclear power plants – Control rooms - Design
IEC 60980	Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations
IEC 61226	Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions
IEC 61468	Nuclear power plants - In-core instrumentation - Characteristics and test methods of self-powered neutron detectors

IEC 61500	Nuclear power plants - Instrumentation and control systems important to safety - Functional requirements for multiplexed data transmission
IEC 61501	Nuclear reactor instrumentation - Wide range neutron fluence rate meter - Mean square voltage method
IEC 61513	Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems
IEC 61772	Nuclear power plants - Control rooms - Application of visual display units (VDU)
IEC 61839	Nuclear power plants. Design of control rooms. Functional analysis and assignment
IEC 61888	Nuclear power plants – Instrumentation important to safety – Determination and maintenance of trip setpoints
IEC 62003	Nuclear power plants - Instrumentation and control important to safety - Requirements for electromagnetic compatibility testing
IEC 62138	Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing categories B and C functions
IEC 62241	Nuclear power plants. Main control room. Alarm functions and presentation
IEC 62340	Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)
IEC 62397	Nuclear power plants - Instrumentation and control important to safety - Resistance temperature detectors
IEC 62566	Nuclear power plants - Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions.
IEC 62671	Nuclear power plants - Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality.
IEEE Std. 1023	IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities
IEEE Std. 308	IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
IEEE Std. 323	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

IEEE Std. 338	IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
IEEE Std. 344	IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
IEEE Std. 379	IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems
IEEE Std. 384	IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits
IEEE Std. 497	IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations
IEEE Std. 603	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
IEEE Std. 7-4.3.2	IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
IEEE Std. 1012	IEEE Standard for Software Verification and Validation
IEEE Std. 1074	IEEE Standard for Developing Software Life Cycle Processes
ISO/IEC 15288	Systems and software engineering -- System life cycle processes
ISO/IEC 12207	Systems and software engineering -- Software life cycle processes

Table I-2 Relationship between international standards and the topic areas of this guide

DS-431This Safety Guide	Internationally Used I&C Standards
1. Introduction	
2. Management systems for I&C design	IEC 61513, IEEE 7-4.3.2
- Use of life cycle models	IEC 61513, IEEE 7-4.3.2, ISO/IEC 15288
3. I&C design bases	IEC 61513, IEEE 603
- Identification of I&C functions	IEC 61226
- Contents of I&C design bases	IEC 61513
4. Guidance for I&C architecture	IEC 61513, IEC 62340
5. Safety classification of I&C functions, systems	IEC 61226

DS-431This Safety Guide	Internationally Used I&C Standards
and equipment	
6. General recommendations for all I&C systems important to safety	
- General	IEC 61513, IEC 60709, IEEE 379, IEEE 384
- Design for reliability	
- Equipment qualification	IEC 60780,IEC 980, IEC 62342, IEEE 344, IEEE 323, IEC 2003
- Design to cope with ageing	
- Control of access to systems important to safety	IEC 61513
- Testing and testability during operation	IEC 60671, IEEE 338
- Maintainability	IEC 61513
- Provisions for removal from service for testing or maintenance	IEC 61513
- Set points	IEC 61888
- Marking and identification of items important to safety	
7. System and equipment specific guidelines	
- Sensing devices	IEC 60515, IEC 61501, IEC 60568, IEC 61468, IEC 60737
- Control systems	
- Protection system	IEEE 603
- Power supplies	IEC 61225, IEEE 308
- Digital systems	IEC 61513, IEEE 7-4.3.2, IEC 61500, IEC 62671
- Devices configured with hardware description languages	IEC 62566

DS-431This Safety Guide	Internationally Used I&C Standards
- Software tools	IEC 60880, IEC 62138
8. Human-machine interface considerations	
- Control rooms	IEC 60964, IEC 61772, IEC 62241, IEEE 576
- Supplementary control rooms	IEC 60965
- Accident monitoring	IEEE 497
- Operator communications systems	
- General HFE principles relating to human factors engineering for I&C systems	IEC 61839, IEC 61772, IEEE 1023, IEEE 1082
- Recording of historical data	
9. Software	IEC 60880, IEC 62138, IEEE 7-4.3.2, IEEE 1012, IEEE Std. 1074, ISO/IEC 12207

REFERENCES TO ANNEX I

[I-1]   INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR 2/1, IAEA, Vienna (2012).

[I-2]   INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge of Instrumentation and Control Systems in Nuclear Power Plants, NP-T-3.12, IAEA, Vienna, (2011).

ANNEX II. CORRELATION BETWEEN THIS SAFETY GUIDE

AND NS-G-1.1 AND NS-G-1.3

II-1. This annex presents tables that show where the topics covered in the two predecessor Ssafety gGuides, NS-G-1.1[43] and NS-G-1.3[44], are located in this guideSafety Guide.

Table II.1 Correspondence bBetween NS-G-1.1 and D-431this Safety Guide

NS-G-1.1	DS-431This Safety Guide
1 Introduction	1 Introduction
2 Technical considerations for computer based systems	2 Management systems for I&C design
	10 Software: General
3 Application of requirements for management of safety to computer based systems	2 Management systems for I&C design
	10 Software: Third party assessment
4 Project planning	2 Management systems for I&C design
5 Computer system requirements	2 Management systems for I&C design
6 Computer system design	2 Management systems for I&C design
	6 General recommendations for all I&C systems important to safety
	7 System and equipment specific design guidelines
	8 Human-machine interface considerations
7 Software requirements	9 Software: Software requirements
8 Software design	9 Software: Software design

---

[43] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standard Series No. NS-G-1.1, IAEA, Vienna (2000).

[44] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Guide Series No. NS-G-1.3, IAEA, Vienna (2002).

Formatted: Font: 10 pt

NS-G-1.1	~~DS-431~~This Safety Guide
9 Software implementation	9 Software: Software implementation
10 Verification and analysis	9 Software: Software verification and analysis
11 Computer system integration	2 Management systems for I&C design
12 Validation of computer systems	2 Management systems for I&C design
13 Installation and commissioning	2 Management systems for I&C design
14 Operation	2 Management systems for I&C design
15 Post-delivery modifications	2 Management systems for I&C design
Annex: Use and validation of pre-existing software	2 Management systems for I&C design 9 Software: Pre-developed software

Table II.2 Correspondence Between NS-G-1.3 and ~~DS-431~~this Safety Guide

NS-G-1.3	~~DS-431~~This Safety Guide
1. Introduction	1. Introduction
2. Instrumentation and control systems important to safety	See ~~NS-T-3.12,~~Ref. [II-19]
- Identification of I&C systems	3. I&C design bases
- Classification of I&C systems	5. Safety classification of I&C functions, systems, and equipment
3. The design basis	3. I&C design bases
4. General design guidelines	

NS-G –1.3	DS-431This Safety Guide
- Performance requirements	2. Management systems for I&C design (Requirement specification)
- Design for reliability	6. General recommendations for all I&C systems important to safety (Design for reliability)
- Independence	4. Guidance for I&C architecture (Independence) 6. General recommendations for all I&C systems important to safety (Independence)
- Failure modes	6. General recommendations for all I&C systems important to safety (Design for reliability - Failure modes)
- Control of access to equipment	6. General recommendations for all I&C systems important to safety (Control of access to systems important to safety) 8. System and equipment specific guidelines (Digital systems - Computer security)
- Set points	6. General recommendations for all I&C systems important to safety (Set points)
- Human-machine interface	8. Human-machine interface considerations
- Equipment qualification	6. General recommendations for all I&C systems important to safety (Equipment qualification)
- Quality	2. Management systems for I&C design
- Design for electromagnetic compatibility	6. General recommendations for all I&C systems important to safety (Equipment qualification - Internal and external hazards - Electromagnetic qualification)

NS-G –1.3	DS-431This Safety Guide
- Testing and testability	6. General recommendations for all I&C systems important to safety (Testing and testability during operation)
- Maintainability	6. General recommendations for all I&C systems important to safety (Maintainability)
- Documentation	2. Management systems for I&C design (Activities common to all life cycle phases of the development process - Documentation)
- Identification of items important to safety	6. General recommendations for all I&C systems important to safety (Marking and identification of items important to safety)
5. System specific guidelines	
- Safety systems - Protection systems	7. System and equipment specific guidelines (Protection systems)
- Power supplies	7. System and equipment specific guidelines (Power supplies)
- Digital computer systems	7. System and equipment specific guidelines (Digital systems)
6. Human-machine interface	8.Human-machine interface considerations
7. Design process for I&C systems important to safety	2. Management systems for I&C design 2. Life cycle activities (Modifications)

REFERENCE TO ANNEX II

[II-1]   INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge of Instrumentation and Control Systems in Nuclear Power Plants, NP-T-3.12, IAEA, Vienna, (2011).

Formatted: Normal

ANNEX III AREAS WHERE PRACTICES OF MEMBER STATES DIFFER

INTRODUCTION

III-1. There are a number of areas where the academic bases or engineering practice supporting the design criteria for I&C safety design criteria are not widely accepted by all Mmember Sstates. This annex discusses areas where such differences were identified during the development of this Safety Guide. It may be expected that the practices of Mmember Sstates will evolve over time.

RELIABILITY DETERMINATION FOR DIGITAL SYSTEMS

III-2. Software errors may lead to common cause failure in redundant digital systems if the same software is used in multiple redundancies. Thus, to estimate digital system reliability it is necessary to estimate the probability of system failure due to hardware failure and, for some Member States, software error. For other Member States, design errors (including software errors) and their consequences are adequately treated only by qualitative analyses of the architecture and of the design.

III-3. Some Mmember Sstates, when developing the I&C design basis, ensure consistency between the reliability requirements of the I&C systems and the probabilistic safety analysis by maintaining an explicit numerical reliability target for each I&C system important to safety. Consequently, these Mmembers sStates consider numerical estimates of digital system reliability to be a necessary element for demonstration of reliability demonstration.

III-4. For the Member States who that apply numerical reliability to software, claims of high software reliability are not demonstrable at the present time. Hence, designs requiring a single computer based system to achieve probabilities failure on demand lower than 10^{-4} for software need to be treated with caution.

III-5. Some regulatory authorities bodies that make use of numerical reliability estimates for digital systems have established limits on the reliability levels that they consider to be justifiable for I&C systems. For example, reliability claims for any I&C system that is based upon a common platform, regardless irrespective of the technology used, are limited to 10^{-5} pfd (probability of failure on demand), and reliability claims for any individual I&C system that is based upon a common computer based platform, are limited to 10^{-4} pfd, regardless irrespective of the extent to which the strategies described in Ssection 7 of this Safety Guide (e.g., redundancy) are employed.

III-6. Some mMember Sstates use a qualitative approach for determining SW software reliability. Such a qualitative approach is typically based on strong requirements on the deterministic behaviour of the software to allow a full verification and validation. Such a combination of strong design requirements that allow full verification and validation V&V gives a high confidence in the reliability of the software.

ASSESSMENT OF COMMON CAUSE VULNERABILITIES IN SAFETY SYSTEMS

III-7. Paragraph 4.32 of this Safety Guide recommends that an analysis should be done of the consequences of each postulated initiating event PIE in combination with common cause failure CCF that will prevent the I&C safety systems from performing the needed safety functions. On this point there is general agreement, but there is not general agreement on the scope of the analysis, the radiological consequences that are accepted in the event of a postulated initiating event PIE together with a common cause failure CCF within a safety system, or the type of analytical methods to be used when establishing the radiological consequences.

Scope of analysis

III-8. The scope that regulatory authorities bodies expect for the analysis described in para. paragraph 4.32 of this Safety Guide includes the following examples:.

- Analysis of a common cause failure in a safety system CCF in conjunction with a postulated initiating event PIE that are considered to be aAnticipated oOperational oOccurrences and dDesign bBasis Accident accident conditions.

- Analysis of a common cause failure in a safety system CCF in conjunction with a postulated initiating event PIE with an occurrence frequency greater than 10-3 per year.

Accepted consequences

III-9. Examples of the consequences that regulatory authorities bodies may accept in the event that a postulated initiating event PIE occurs in conjunction with a common cause failure of in a safety systems include the following:

- The consequences of an anticipated operational occurrence occurring in conjunction with a common cause failure in the reactor protection system do not result in:

    - Any individual located at any point on the exclusion area boundary for two hours following the beginning of fission product release, or at the low population zone boundary for the full duration of fission product release, receiving a whole body dose exceeding 25 mSv or a dose exceeding 300 mSv to the thyroid from iodine,; or

    - Exceeding of the design limits of the primary coolant system design limits.

- The consequences of a design basis accident occurring in conjunction with a common cause failure in the reactor protection system do not result in:

    - An individual located at any point on the exclusion area boundary for two hours following the beginning of fission product release, or at the low population zone boundary for the full duration of fission product release, receiving a whole body dose exceeding 0.25 Sv or a dose exceeding 3 Sv to the thyroid from iodine,. or

- Exceeding of the design limits of the primary coolant system or the containment design limits.

- Following a design basis accident occurring in conjunction with a common cause failure in thea reactor protection system, the remaining safety systems are to be capable of:

  - Ensuring dDose limits agreed between the regulatory body and the licensee are met;,

  - Preventing failure of the primary heat transport system due to over pressure;,

  - Preventing excessive fuel temperatures;,

  - Preventing fuel breakup;

  - Limiting the rate of energy production and the total energy production to the extent that containment integrity is not jeopardized;,

  - Maintaining the reactor subcritical for a period long enough to provide alternative means to ensure subcriticality.

- The diversity and other means provided to prevent or mitigate the consequences of a common cause failure ensure a sufficiently high reliability of system function.

- The consequences of a DBA design basis accident do not exceed acceptable dose limits if a safety system fails.

Analytical approaches

III-10. In making consequence determinations on consequences as part of the analysis described in para. paragraph 4.32, some regulatory authorities bodies expect the use of conservative methods; others allow the use of best estimate methods. NS-G-1.2, Ref-erence [III-110] discusses conservative methods, and best estimate analysis methods.

DIVERSE ACTUATION SYSTEMS

III-11. When digital systems are used to implement pProtection sSystem functions it is not uncommon for the analysis described in para. paragraph 4.32 of this Safety Guide to find that common cause failures within the digital protection system might result in unacceptable consequences for certain combinations of common cause failures CCF and postulated initiating eventsPIEs. When this situation is encountered, a Ddiverse aActuation sSystem is often provided to backup the pProtection sSystem.

III-12. There is general agreement that diverse actuation system Diverse Actuation Systems may effectively mitigate the consequences of specific postulated initiating events PIEs in conjunction with a postulated common cause failure CCF of a Protection Systemprotection system. There are, however, different approaches to the safety classification, the use of digital diverse actuation systems Diverse Actuation Systems to back up a digital protection systemProtection System, and the use of manual actuation to mitigate the consequences of Protection System common cause failureCCF of the protection system.

Safety classification

III-13. Some regulatory ~~authorities~~ bodies expect that diverse actuation systems ~~Diverse Actuation Systems~~ will be classified as safety systems. Some regulatory ~~authorities~~ bodies allow them to be systems ~~of~~ in a lower safety class~~ification~~. Some regulatory ~~authorities~~ bodies base the expected ~~level of~~ safety class~~ification~~ upon the reliability claims made for the diverse actuation system~~Diverse Actuation System~~.

Technology of the ~~D~~diverse ~~A~~actuation ~~s~~System ~~technology~~

III-14. Some regulatory ~~authorities~~ bodies expect that diverse actuation systems ~~Diverse Actuation Systems~~ will be hardwired systems. Some regulatory ~~authorities~~ bodies discourage, but do not prohibit, the use of digital systems. Some regulatory ~~authorities~~ bodies allow the use of digital systems if adequate diversity is demonstrated.

Use of manual actions for diverse actuation

III-15. Generally~~,~~. manual actuation may be accepted as a diverse backup for the ~~Protection System~~protection system but the conditions under which manual actuation may be credited vary. The range of accepted practices include the following:

- Manual action may be credited if the action is not needed in less than 30 minutes and human factors analysis has confirmed that a proper decision can be taken and implemented within that time;

- Manual action may be credited if the action is not needed in less than 20 minutes;

- Manual action may be credited for actuation of engineered safety features ~~actuation~~, but not for reactor trip;

- Manual action may be credited without restriction.

It is worth noting that disallowing credit for manual action in the first 20 or 30 minutes effectively disallows it use as a backup for reactor trip.

III-16. While the above illustrates the range of practices among regulatory ~~authorities~~bodies, a regulatory bodies may take a different approach based upon the specific situation proposed.

REFERENCE TO ANNEX III

[III-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2009).

LIST OF DEFINITIONS

(The following definitions are specific to this publication and are either not given provided in or are different* from those given provided in the IAEA Safety Glossary [7]).

architecture: Organisational structure of the I&C systems of the plant which are important to safety.

> [Formatted: Font: Not Bold]

availability.* 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, assuming with the assumption that the required necessary external resources are provided.

calibration.* Set of operations that establish, under specified conditions, the relationship between values of quantities indicated by a measuring instrument or measuring system, or values represented by a material measure or a reference material, and the corresponding values realized by standards.

common cause failure (CCF).* Failure of two or more structures, systems or components due to a single [specific?] event or cause.[do you really need this one to be different from the Glossary def? pls consider leaving it out]

component. One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components.

> NOTE - The terms "equipment", "component", and "module" are often used interchangeably. The relationship of these terms is not yet standardized.

configuration baseline. A set of configuration items formally designated and fixed at a specific time during an item's lifecycle.

design extension condition. Accident conditions that are not considered to be design basis accidents, but that are considered in the design process of the plant in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.

deterministic behaviour. Characteristic of a system or component such that any given input sequence that is within the item's specifications of the item always produces the same outputs.

deterministic timing. Characteristic of a system or component such that the time delay between stimulus and response has a guaranteed maximum and minimum value.

diversity.* 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.

division. The collection of items, including their interconnections, that form one redundancy of a redundant system or safety group. Divisions may include multiple channels.

firmware. Software which is closely coupled to the hardware characteristics on which it is installed.

failure.* ~~Loss of the ability~~ Inability ~~[?]~~ of a structure, system or component to function within ~~acceptance criteria. [do you need really this one to be different from the Glossary def? pls consider leaving it out]~~

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

~~NOTE 2 — A failure is the result of a hardware fault, software fault, system fault, or operator or maintenance error, and the associated signal trajectory, which results in the failure.~~

field programmable gate array ~~(FPGA)~~**.** An i~~I~~ntegrated circuit that can be programmed in the field by the I&C manufacturer. It includes programmable logic blocks (combinatorial and sequential), programmable interconnections between them and programmable blocks for input and/or outputs. The function is then defined by the I&C designer, not by the circuit manufacturer.

functional requirements. Requirements that specify the required functions or behaviours of an item.

hardware description language ~~(HDL)~~**.** Language that allows one to formally describe the functions and/or the structure of an electronic component, for documentation, simulation~~,~~ or synthesis.

hardware programmed device ~~(HPD)~~**.** A hardware ~~HDL~~ ~~p~~ Programmed d~~D~~evice can be an integrated circuit configured (for ~~NPP~~ I&C systems in nuclear power plants), with h~~H~~ardware d~~D~~escription L~~l~~anguages and related software tools.

hazard. A potential for harm.

   contributory hazard. Factor contributing to potential for harm.

hazard analysis. A process of examining a system throughout its lifecycle to identify inherent hazards and contributory hazards, and requirements and constraints to eliminate, prevent, or control them~~that explores and identifies conditions that are not identified by the normal design review and testing process in the design~~.

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

human-machine interface ~~(HMI)~~. The interface between operating staff and I ~~&~~ C system~~s~~ and computer systems linked with the plant. The interface includes displays, controls~~,~~ and the interface with the o~~O~~perator s~~S~~upport s~~S~~ystem ~~interface~~.

non-functional requirements. (also known as quality requirements)~~:~~ Requirements that specify inherent properties or characteristics of an item, other than the required functions and behaviours. Example characteristics include analys~~z~~ability, assurability, auditability, availability, compatibility, documentation, integrity, maintainability, reliability, safety, security, usability and verifiability.

pre-developed block. P~~p~~re-developed functional block usable in a hardware description language ~~HDL description~~. Pre-developed blocks ~~might be~~include, for example, libraries, macros~~,~~ or i~~I~~ntellectual p~~P~~roperty cores. A pre-developed block may need significant work before incorporation in a hardware ~~HDL~~ programmed device.

pre-developed item. Item ~~which~~ that already exists, is available as a commercial or proprietary product, and is being considered for use in an I&C system. Pre-developed items ~~might be~~include hardware devices, pre-developed software ~~(PDS)~~, commercial off the shelf ~~(COTS)~~ devices, digital devices composed of both hardware and software, or hardware devices configured with hardware definition language or pre-developed blocks.

requirements engineering. A~~a~~n engineering process~~,~~ ~~which~~ that includes the activities involved in ~~discovering~~developing, documenting and maintaining a set of requirements.

~~**safe state.** Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and stably maintained for long time.~~

static analysis.~~:~~ A~~a~~nalysis of a system or component based upon its form, structure, content or documentation.

system validation. Confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification~~s~~ as intended (functionality, response time, fault tolerance, robustness).

type test. Conformity test made on one or more items representative of the production.

validation.* Confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended.

verification.* Confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity.

Formatted: Centered

CONTRIBUTORS TO DRAFTING AND REVIEW

Alpeev, A	Scientific-Technical Center on Nuclear and Radiation Safety, —Russian Federation	
Alvarado, R.	US Nuclear Regulatory Commission, United States of America USA	
Asikainen, S.	Teollisuuden Voima Oyj, Finland	Finland
Babcock, B.	Ontario Power Generation, Canada	Canada
Benitez-Read, J.	National Nuclear Research Institute of Mexico, Mexico	Mexico
Bicer, C.	Turkish Atomic Energy Authority, Turkey	Turkey
Boeva, T.	Kozloduy NPPNuclear Power Plant,	Bulgaria
Bouard, J-P,	EDFElectricite de France, France	France
Bowell, M.	Office for Nuclear Regulation, United Kingdom	United Kingdom
Curtis, D.	Private Consultant, United Kingdom	United Kingdom
Debor, J.	Private Consultant, United States of America	USA
Duchac. A	IAEAInternational Atomic Energy Agency	
Edvinsson, H.	Vattenfall, Sweden	Sweden
Eriksson, K-E.	Oskarshamn NPPNuclear Power Plant, Sweden	Sweden
Faya, A.	FANRFederal Authority for Nuclear Regulation, United Arab Emirates UAE	
Fichman, R.	Ontario Power Generation, Canada	Canada
Furieri, E-B.	Comissao Nacional de Energia Nuclear, Brazil	Brazil
Gassino, J.	Institut de radioprotection et de sûreté nucléaire, France IRSN	France
Gonchukov, V.	Rostechnadzor, Russian Federation	Russia
Göring, M.	Vattenfall, Germany	Germany
Harber, J.	AECLAtomic Energy of Canada Limited, Canada	Canada
Hohendorf, R.	Ontario Power Generation, Canada	Canada
Johnson, G.	International Atomic Energy AgencyIAEA	
Karasek, A.	CEZ, Czech Republic	Czech Republic
Kawaguchi, K.	Japan Nuclear Energy Safety Organization, Japan	Japan

Kim, B-Y.	Korea Institute of Nuclear Safety, Republic of Korea	~~ROK~~
Klopkov V.	Rostechnadzor, Russian Federation	~~Russia~~
Lee, J-S.	Korea Atomic Energy Research Institute, Republic of Korea	~~ROK~~
Li, H.	~~US~~ Nuclear Regulatory Commission, United States of America	~~USA~~
Lindskog, U.	Oskarshamn ~~NPP~~Nuclear Power Plant, Sweden	~~Sweden~~
Mangi, A.	Pakistan Nuclear Regulatory Authrority, Pakistan	~~Pakistan~~
Ngo, C.	Candesco, Canada	~~Canada~~
Odess-Gillett, W.	Westinghouse, United States of America	~~USA~~
Park, H-S.	Korea Institute of Nuclear Safety, Republic of Korea	~~ROK~~
Parsons, A.	AMEC, United Kingdom	~~United Kingdom~~
Poulat, B.	International Atomic Energy Agency~~IAEA~~	
Piljugin, E.	~~GRS~~Gesellschaft für Anlagen- und Reaktorsicherheit, Germany ~~Germany~~	
Régnier, P.	Institut de radioprotection et de sûreté nucléaire, France~~IRSN~~	~~France~~
Santos, D.	~~US~~ Nuclear Regulatory Commission, United States of America	~~USA~~
Seidel, F.	Federal Office for Radiation Protection, Germany	~~Germany~~
Shumov, S.	SNIIP, Russian Federation	~~Russia~~
Sjövall, H.	Teollisuuden Voima Oyj, Finland	~~Finland~~
Stattel, R.	US Nuclear Regulatory Commission, United States of America~~USASjövall, H.~~ ~~Teollisuuden Voima Oyj~~	~~USA~~ ~~Finland~~
Svensson, C.	Oskarshamn ~~NPP~~Nuclear Power Plant, Sweden	~~Sweden~~
Takala, H.	~~STUK~~Radiation and Nuclear Safety Authority, Finland	~~Finland~~
Takita, M.	Japan Nuclear Energy Safety Organization, Japan	~~Japan~~
Tate, R.	Office for Nuclear Regulation, United Kingdom	~~United Kingdom~~
Thuy, N.	~~EDF~~Electricite de France, France	~~France~~
Welbourne, D.	Private Consultant, United Kingdom	~~United Kingdom~~
Yastrebenetsky, M.	~~SSTC~~State Scientific and Technical Center for Nuclear and Radiation Safety, Ukraine ~~Ukraine~~	
Yates, R.	Office for Nuclear Regulation, United Kingdom	~~United Kingdom~~
Zeng, Z-C.	Canadian Nuclear Safety Commission, Canada	~~Canada~~