Date: 2013 April 25

IAEA SAFETY STANDARDS

for protecting people and the environment

Draft K

Step 7

Submission for NUSSC review with resolution of NUSSC member comments.

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

TABLE OF CONTENTS **3**

1. INTRODUCTION **7**
BACKGROUND 7
OBJECTIVE 8
SCOPE 8
STRUCTURE 10

2. MANAGEMENT SYSTEMS FOR I&C DESIGN **11**
USE OF LIFE CYCLE MODELS 13
Process planning *15*
Coordination with human factors and computer security activities *17*
ACTIVITIES COMMON TO ALL LIFE-CYCLE PHASES 19
Configuration Management *19*
I&C systems hazard analysis *22*
Verification and validation *23*
Use of insights from probabilistic safety analysis *24*
Safety assessment *24*
Documentation *26*
LIFE CYCLE ACTIVITIES 27
Requirement specification *27*
Selection of pre-developed items *29*
I&C system design and implementation *30*
System integration *30*
System validation *31*
Installation, overall I&C integration, and commissioning *32*
Operation and maintenance *33*
Modifications *33*

3. I&C DESIGN BASES **35**
IDENTIFICATION OF I&C FUNCTIONS 35
CONTENT OF I&C DESIGN BASES 36

4. GUIDANCE FOR I&C ARCHITECTURE **39**
ARCHITECTURAL DESIGN 39
CONTENT OF THE OVERALL I&C ARCHITECTURE 40
CONTENT OF INDIVIDUAL I&C SYSTEM ARCHITECTURES 41
INDEPENDENCE 41
CONSIDERATION OF COMMON CAUSE FAILURE 42

5. SAFETY CLASSIFICATION OF I&C FUNCTIONS, SYSTEMS, AND EQUIPMENT **44**

6. GENERAL RECOMMENDATIONS FOR ALL I&C SYSTEMS IMPORTANT TO SAFETY **49**
GENERAL 49
DESIGN FOR RELIABILITY 49
Single failure criterion *50*
Redundancy *51*
Independence *51*
Diversity *56*
Failure modes *57*

EQUIPMENT QUALIFICATON 58
Suitability and correctness *59*
Environmental qualification *60*
Internal and external hazards *61*
DESIGN TO COPE WITH AGEING AND OBSOLESCENCE 64
CONTROL OF ACCESS TO SYSTEMS IMPORTANT TO SAFETY 65
TESTING AND TESTABILITY DURING OPERATION 66
Test provisions *66*
Test program *69*
MAINTAINABILITY 71
PROVISIONS FOR REMOVAL FROM SERVICE FOR TESTING OR MAINTENANCE 72
SETPOINTS 72
MARKING AND IDENTIFICATION OF ITEMS IMPORTANT TO SAFETY 74

7. SYSTEM AND EQUIPMENT SPECIFIC DESIGN GUIDELINES 75
SENSING DEVICES 75
CONTROL SYSTEMS 75
PROTECTION SYSTEM 76
Automatic and manual safety actions *76*
Information display *77*
Protection system sensors and settings *77*
Operational bypasses *78*
Latching of protection system functions *78*
Spurious initiation *79*
Interaction between the protection system and other systems *79*
POWER SUPPLIES 80
DIGITAL SYSTEMS 81
Digital system functions *81*
Digital data communication *82*
Data communications independence *84*
Computer security *85*
Devices configured with hardware description languages (HDL) *87*
SOFTWARE TOOLS 89
QUALIFICATION OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY FOR SAFETY APPLICATIONS 91

8. HUMAN-MACHINE INTERFACE CONSIDERATIONS 93
CONTROL ROOMS 93
Main control room *93*
Supplementary control room *94*
ACCIDENT MONITORING 95
OPERATOR COMMUNICATIONS SYSTEMS 97
GENERAL HFE PRINCIPLES FOR I&C SYSTEMS 98
Considerations for human-automation interaction *100*
Considerations for task design in I & C systems *101*
Considerations for accessibility and work environment *102*
RECORDING OF HISTORICAL DATA 103

9. SOFTWARE 103
GENERAL 103

SOFTWARE REQUIREMENTS 103
SOFTWARE DESIGN 105
SOFTWARE IMPLEMENTATION 107
SOFTWARE VERIFICATION AND ANALYSIS 108
PRE-DEVELOPED SOFTWARE 111
SOFTWARE TOOLS 111
THIRD PARTY ASSESSMENT 111

REFERENCES 114

ANNEX I. BIBLIOGRAPHY OF INTERNATIONAL I&C STANDARDS 118

ANNEX II. CORRELATION BETWEEN THIS GUIDE AND NS-G-1.1 AND NS-G-1.3 124

ANNEX III AREAS WHERE PRACTICES OF MEMBER STATES DIFFER 128
INTRODUCTION 128
RELIABILITY DETERMINIATION FOR DIGITAL SYSTEMS 128
ASSESSMENT OF COMMON CAUSE VULNERABILITIES IN SAFETY SYSTEMS 129
Scope of analysis 129
Accepted consequences 129
Analytical approaches 130
DIVERSE ACTUATION SYSTEMS 130
Safety classification 130
Diverse Actuation System technology 130
Use of manual actions for diverse actuation 130

LIST OF DEFINITIONS 132

1. INTRODUCTION

BACKGROUND

1.1. This guide gives recommendations on the design of Instrumentation and Control (I&C) systems to meet the requirements established in SSR 2/1, Ref. [1].

1.2. This publication is a revision and combination of two previous Safety Guides - Safety Series Nos. NS-G-1.1, Ref. [2], and NS-G-1.3, Ref. [3], which are superseded by this Safety Guide. The revision takes account of developments in I&C systems since the publication of the predecessor guides in 2000 and 2002. The main changes are due to continued development of computer applications and 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 references and takes account other IAEA Safety Standards and Security Series documents that have given guidance that affects I&C design. Most notable among these are the Requirements for Management Systems, GS-R-3, Ref. [4], and its supporting Guides GS-G-3.1, Ref. [5] and GS-G-3.5, Ref. [6], and Safety Assessment for Facilities and Activities GS-R-4, Ref. [7].

1.3. The main topic areas for which this Guide gives new or updated guidance are:

- Considerations specific to I&C for achieving compliance with GS-R-3, Ref. [4],
- Design inputs to be considered when developing I&C system design bases,
- The interdependent set of life cycles needed for the design and implementation of I&C systems, and in particular the life cycle for the overall I&C, individual I&C systems, software, and for the integration of human factors engineering 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 for gaining assurance of their correct performance,
- The overall I&C architecture to support the defence in depth concept applied in the design of the nuclear and mechanical systems and to establish 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 for cases where the system receiving data is of a higher category than the system sending data,
- Provisions for ensuring the security of digital safety systems,
- Computer software development activities including design, verification and validation, from the principles given or implicit in the detail of previous Safety Guide NS-G 1-1, Ref. [2].

1.4. Throughout the document, the term ‘I&C system’ refers to any I&C system important to safety as defined by the IAEA Safety Glossary, Ref. [8]. The term ‘important to safety’ is not repeated again

except for emphasis. Where recommendations are specific to safety systems, this is identified. In a few cases, recommendations or explanations apply to both I&C systems important to safety and I&C systems that are not important to safety; in that case the term ‘All I&C systems’ is used.

1.5. This guide has a particularly strong relationship with DS-430, Ref. [9] (the draft safety guide on Design of Electrical Power Systems for Nuclear Power Plants), which gives recommendations for power supply, cable systems, protection against electromagnetic interference, equipment and signal grounds, and other topics that are necessary for satisfactory operation of I&C systems.

1.6. Additional guidance for the design and development of I&C systems, equipment, and software are available from Member States and Standards Development Organizations. Their documents give much greater detail than is appropriate for IAEA Safety Standards. It is expected that this Safety Guide will be used in conjunction with an appropriate set of more detailed 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 of the safety goals of the plant.

1.8. The 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, plant layout process, and from safety analysis. The I&C design basis will, for example, give the functional requirements to be achieved by the I&C, the extremes of environmental temperature in which equipment is to operate, the external events that I&C equipment is to withstand, and the conditions for which an automatic shutdown is 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 IAEA SSR 2/1, Ref. [1]. This Safety Guide also discusses certain I&C specific issues which are relevant to implementing the recommendations of certain other Safety Guides, such as those which cover management systems, commissioning, installation, operation, and operating limits and conditions.

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

- Sensors,
- Actuator controls,
- Equipment for automatic and manual control of plant equipment,
- Operator interfaces.

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

- Computer systems,
- Software,
- Devices that are programed using Hardware Description Languages (e.g., field programmable gate arrays), and
- Industrial digital devices of limited functionality.

1.12. This safety guide does not give recommendations for support features of I&C systems such as cooling, lubrication, and energy supply. Recommendations for electrical energy supply are given in DS-430, Ref. [9]. Recommendations for other support features are to be given in a new safety guide on the topic of auxiliary systems.

1.13. Although this safety guide covers certain aspects of human factors and computer security as they relate to I&C, it is not a comprehensive guide on these domains. The intent in this guide 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.

1.14. The guidance applies to the design of I&C systems for new plants, modification of existing plants, and to the modernization of the I&C of existing plants. The IAEA safety guide NS-G-2.3, Ref. 10 deals with plant modification. The overlap of this guide with NS-G-2.3 is minimized.

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 further discusses the term ‘important to safety’ and other safety classification terminology. Examples of I&C systems to which this guide may ~~applies~~ apply include:

- Reactor protection systems,
- Reactor control, reactivity control, and their monitoring systems,
- Systems to monitor and control reactor cooling,
- Systems to monitor and control emergency power supplies,
- Systems to monitor and control containment isolation,
- Accident monitoring instrumentation,
- Effluent monitoring systems, and

- I&C for fuel handling.

1.16. This safety guide also provides recommendations for the development of computer software for use in I&C systems important to safety and digital data communication, and the measures needed for I&C functions that are programmed into integrated circuits using HDL descriptions. Field Programmable Gate Arrays (FPGA) are a common example of integrated circuits that are often programmed in this way.

1.17. The IAEA's Technical Reports Series No. 387, Ref. [11], and Nuclear Energy Series NP-T-3.12, Ref. [12], present overviews of concepts that underlie this Safety Guide and give examples of systems discussed in it. These references provide useful background material for some users, although they should not be used directly as guidance.

STRUCTURE

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

1.19. Section 2 gives guidance for the application of the IAEA Management System standards as they relate specifically to the development of I&C systems. It also considers the use of life-cycle models to describe management system processes for the development of I&C, gives guidance on the generic processes for I&C design, and gives guidance on the implementation of specific I&C development activities.

1.20. Section 3 identifies the inputs to the design and the need to provide the design basis of I&C systems.

1.21. Section 4 gives guidance on the architecture of the overall I&C.

1.22. Section 5 describes the safety classification scheme that is used to grade the recommendations of this guide according to the safety significance of items to which they apply.

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

1.24. Section 7 gives 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 HDL. The guidance of Sections 2-7 and Sections 9 and 10 also apply to the specific systems discussed in Section 8.

1.25. Section 8 is concerned with the human-machine interface (HMI). It includes guidance on the application of Human Factors Principles to I&C and the characteristics to be achieved by the HMI.

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

1.27. This guide should be considered as a whole, not as a series of stand-alone sections. For example, the guidance on software given in section 9 is to be applied in conjunction with the management systems and lifecycle guidance given in section 2.

1.28. Informative annexes include references, a listing of internationally used standards that provide more detailed guidance on the topic areas of this guide and relating this guide to the two preceding guides, and a list of definitions.

2. MANAGEMENT SYSTEMS FOR I&C DESIGN

2.1. SSR 2/1 Requirement 6 states:

> 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 states:

> 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, Ref. [4] establishes requirements for management systems of nuclear facilities and activities.

2.4. GS-R-3 Paragraph 2.1 states:

> 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.

2.5. Management systems include the organizational structure, organizational culture, policies, resources (e.g., personnel, equipment, infrastructure, working environment), and processes for developing an I&C system that meets safety requirements.

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

2.7. Safety Guides GS-G-3.1, Ref. [5] and GS-G-3.5, Ref. [6] give guidance on the application of the GS-R-3, Ref. [4] requirements to nuclear power plants and other kinds of installations, facilities, and activities.

2.8. The management systems for development of I&C systems should comply with the requirements of GS-R-3, Ref. [4], the recommendations of Safety Guides GS-G-3.1, Ref. [5] and GS-G-3.5, Ref. [6].

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 particular interest in the development of I&C systems are listed below.

- Management Systems;
- Safety culture;
- Management commitment;
- Statutory and regulatory compliance;
- Organizational policies;
- Planning;
- Responsibilities and authority;
- Provision of resources;
- Human resources;
- Development of management system processes;
- Process Management;
- Control of documents, products (including tools), and records;
- Purchasing;

- Communication;
- Management of organizational change;
- Monitoring and measurement;
- Self-Assessment;
- Independent Assessment;
- Non-conformances and corrective and preventative actions; and
- Improvement.

USE OF LIFE CYCLE MODELS

2.10. GS-R-3 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 I&C systems are complex entities that need design and qualification approaches beyond those that were typically applied to older systems. Often the functional characteristics and performance of previous generations of I&C systems could be well characterized by models based upon physics principles and testing that validates these models.

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

2.13. As a result, 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. In modern I&C systems, verification and validation is necessary to ensuring that the final product is suitable for use. However, correct system performance over the full range of conditions cannot be inferred from the combination of testing and physics models to the same extent that this can be done for 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, the nuclear power community as well as other safety critical domains such as aerospace, have applied development processes 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 related to a given development step are grouped into the same phase.

2.15. A well-documented development process also produces evidence that can allow independent reviewers and regulators to gain confidence in the final product.

2.16. The recommendations for life cycle processes described in this section also apply to life cycle activities described in section 9. The life cycle process guidance in this section supplements the requirements of GS-R-3, Ref. [4] and the recommendations of GS-G-3.1, Ref. [5] and GS-G-3.5, Ref. [6] as they apply to I&C system development.

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

- An overall I&C architecture development life cycle;
- One or more individual I&C system development life cycles; and
- One or more individual component development life cycles. Component life cycles are typically managed in the framework of a platform development and 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 outside of the I&C development will have an important influence on the I&C system requirements and design. Human factors engineering and computer security are examples of such activities. These have a broader purpose than support of I&C design, but they will have a strong influence on I&C development. Furthermore, security features are easier and more cost-efficient to implement in the design phase. Afterwards 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 Human Factors Engineering (HFE) and computer security programs.

2.20. The V-model shown in Figure 2 is a useful alternative view of an example development lifecycle. This model illustrates the relationship between requirement specification, design, integration, and system validation activities and how V&V 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 lessons learned 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 1 and 2 do not show the iteration paths.

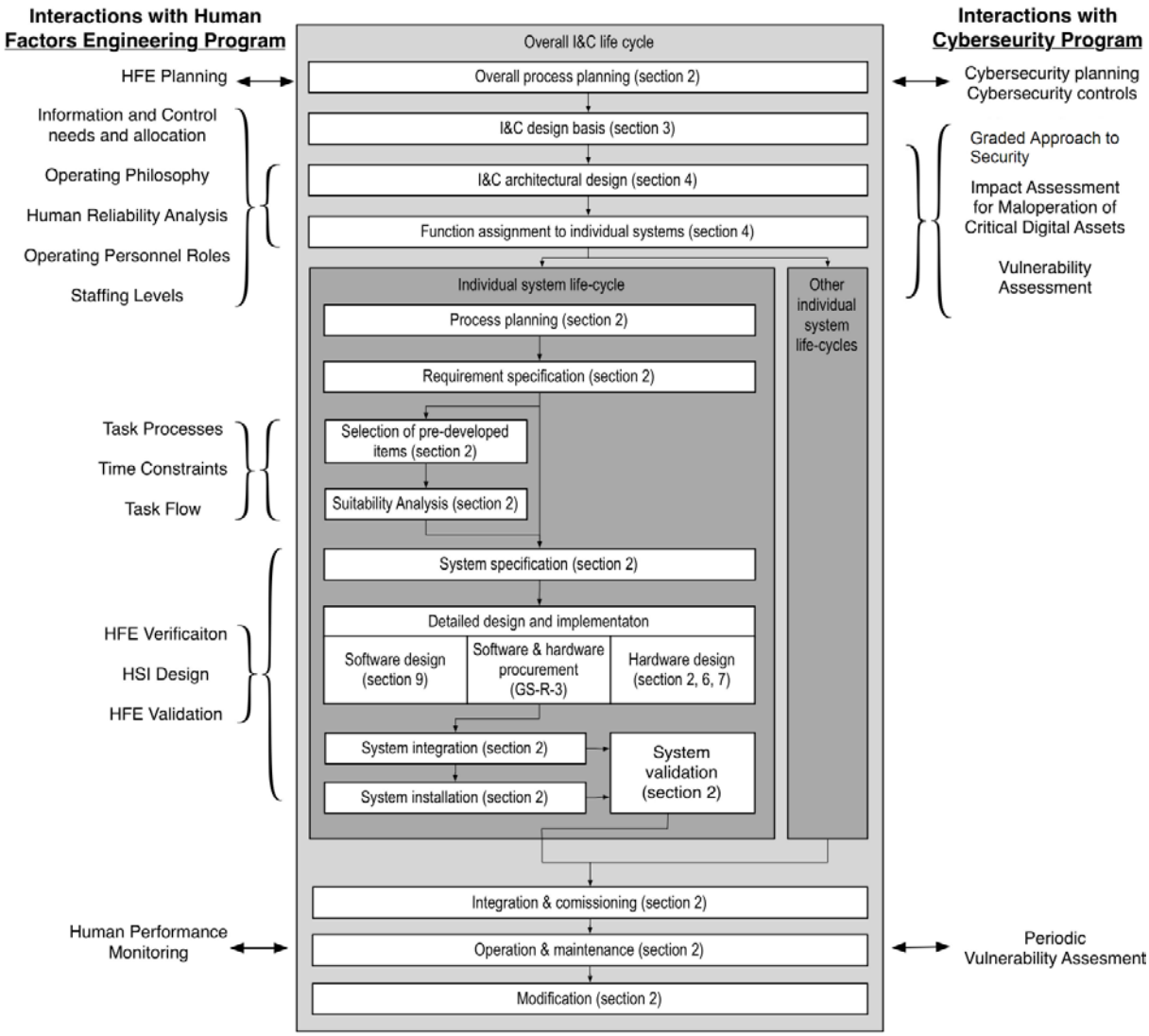


FIG. 1. Typical I&C life cycle activities and interfaces with HFE and Computer Security programs

2.22. All activities associated with development, implementation, and operation of the overall I&C architecture, individual I&C systems, and I&C components (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 period that starts with deriving their requirements and finishes when they are no longer required for the safety of the plant.

Process planning

2.24. Before initiation of any technical activity, a plan identifying the inputs, products, and processes, of that activity and the relationship of the activity with other activities should be prepared and approved in accordance with the management system.

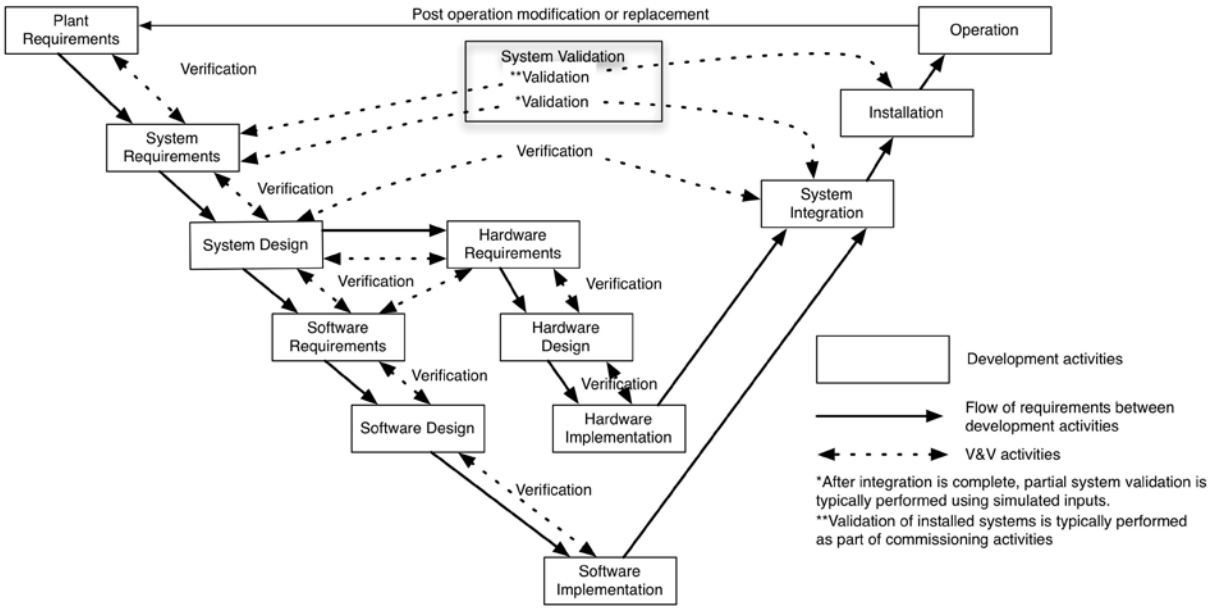


FIG. 2 Typical relationship Between I&C life cycle processes and V&V activities

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 below.

- Life cycle models;
- Configuration management;
- Identification, control, and resolution of non conformances;
- I&C system hazard analysis;
- Verification and validation;
- Use of insights from probabilistic safety assessment;
- I&C safety analysis;
- 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 descriptions;
- Integration;
- System validation;

- Installation;
- Commissioning;
- Equipment qualification;
- Qualification and use of tools;
- Maintainability;
- Obsolescence mitigation;
- Software maintenance/recovery.

2.26. Several topics may be combined into a single plan.

2.27. The development of I&C 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 and computer security activities

2.29. Though HFE and Computer Security life cycle processes are not covered by this guide, these 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, outputs of the HFE V&V activities, technical security measures and computer security requirements.

2.30. I&C development should be coordinated with HFE and computer security activities.

2.31. I&C development should implement requirements developed by the Human Factors Engineering program, including:

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

b. Safety classification of the elements of the Human Machine Interface;

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

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

e. Task process, time constraints, flow of operating personnel and information identified by analyses (i.e. task analysis, see paragraph 8.78);

f. Context based annunciation strategies;

g. Context based annunciation avoids flooding of messages which might occur, for example, during start-ups and transients;

h. I&C system fault reporting;

i. Provisions to support I&C maintainability, and

j. Insights resulting from consideration of human error in safety analysis (i.e. Human Reliability Analysis).

2.32. Human Factors Engineering Verification and validation activities should:

a. Verify the resolution to HFE recommendations and deficiencies identified during analyses of the HMI design;

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

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

d. Verify that the HFE design elicits proper operator response to annunciation messages, including time adequacy 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 which the system is expected to function.

2.33. The development of HFE requirements and V&V of HFE activities are normally performed within the Human Factors Engineering program. The HFE program is not described in any further detail within this guide with the exception of the interfaces to the I&C life cycle process.

2.34. The overall I&C 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. 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 implementation of computer security at nuclear facilities is given in IAEA Nuclear Security Series No. 17, Ref. [13].

Configuration Management

2.38. GS-R-3 paragraphs 5.12 through 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. [4] these topics are discussed under the heading of control of documents, control of products, and control of records. For engineering activities the control of documents and products is more commonly grouped under the heading of configuration management. The GS-R-3 requirements 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, Ref. [5] and GS-G-3.5, Ref. [6] provide additional recommendations on the four topics identified in paragraph 2.38.

2.40. Objectives of configuration management during the life cycle of I&C systems include:

- To identify all items under configuration management, i.e. documents, I&C products and associated records,
- To provide for secure storage and retrieval of configuration items,
- To identify dependencies and relationships between items under configuration management,
- To identify all changes of items under configuration management,
- To prevent the inadvertent and unauthorized modifications of items under configuration management,
- To ensure continued conformance with the design bases,
- To define configuration baselines, i.e. configuration of mutually compatible and consistent components of an item in every hierarchical level of configuration under configuration management.

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 consistency between the physical plant and the technical documentation, and
- To specify 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 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 the deliverable and separately installed items of a system, the documents and files that define these items, and the tools that might affect the quality of the installed items. I&C products may be developed items, reused items, or procured items.

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

- Procured items, reused items, and newly developed items;
- Software components such as source and executable code, HDL descriptions, 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 descriptions;
- 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 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 paragraph 5.21 requires:

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

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

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

2.49. Life cycle records to be 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 that document the system safety demonstration and its supporting evidence, e.g. artefacts or records of: Assurance; Verification (including analysis and testing), Validation (including validation of requirements); Process assessment and audit; Authenticity; Integrity, Traceability;
- Records of verification and validation activities;
- Test specifications, procedures, plans, and results;
- Limiting safety system settings and the methodology for establishing limiting safety system settings;
- System integration procedures, plans and results;
- Process review and audit documents;
- Requirements traceability matrices;
- Maintenance and operating procedures;
- Technical aspects of purchasing specifications for equipment and spares;
- Qualification records; and
- I&C system and component documentation, see paragraph 2.91.

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

2.51. Configuration control applies to the original development of I&C, changes made during development and the modification after it has been placed in service.

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

2.53. Information to be recorded might include, for example, when the item was 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.

2.55. The ability to retrieve the identity of installed items and the values of configuration data support verification that the devices are properly configured. Automatic checking features or tools may assist this verification.

I&C systems hazard analysis

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

2.57. For safety systems, hazards analyses should be performed to identify conditions that might defeat their safety function.

2.58. Hazards to be considered include internal hazards and external hazards, failures of plant equipment, and I&C failures or spurious operation due to hardware failure or to software errors.

2.59. I&C system hazard analysis should consider all plant states and operating modes, including transitions between operating modes.

2.60. The initial results of the I&C system hazard analysis should be available before the design basis for the overall I&C is completed.

2.61. The hazard analysis should be updated during the design of the overall I&C architecture, and during the specification of requirements, design, implementation, installation and modification of safety systems.

2.62. The 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 of their safety classification.

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

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

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

Verification and validation

2.66. Each phase of an I&C development process 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 should be verified against the requirements set by the previous phases.

2.68. A Requirements Traceability Matrix can be used to document confirmation that requirements are satisfactorily met in each life cycle phase and 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 validated to confirm it implements all of their requirements (both functional and non-functional), and to investigate for the existence of behaviour that is not required (see paragraphs 2.129 to 2.143).

2.70. Note that the term component includes hardware, software such as application software and firmware, and HDL descriptions.

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

2.72. Establishing independence of verification and validation normally involves ensuring that the V&V teams, individuals, or groups:

- Have adequate technical competence and knowledge,
- Can set their own scope,
- Are not subject to pressure from the developers,
- Are not subject to reduction in budget or schedule constraints that would prevent them from completing their scope, and
- Are allowed to submit their findings to programme management without adverse pressure from the development group.

2.73. The amount and type of independence of the V&V should be suitable for the safety class of the system or component involved.

2.74. Verification and validation activities, including records of detected anomalies and their disposition, should be documented and recorded.

2.75. Technical communications between the V&V teams, system integration teams, commissioning teams and the system designers and developers should be recorded.

Use of insights from probabilistic safety analysis

2.76. SSR 2/1 paragraph 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.

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

2.78. Detailed information on PSAs and the use of PSA results during design can be found in SSG-3, Ref. [14] and SSG-4, Ref. [15].

Safety assessment

2.79. Safety assessment of I&C should be conducted according to the requirements of GS-R-4, Ref. [7] and the recommendations of SSG-2, Ref. [16].

2.80. 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.

2.81. Paragraph 3.14 recommends topics to be considered in 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.

2.82. Typical design analysis, verification and validation techniques include, for example:

- Traceability analysis. Traceability analysis is typically used to confirm implementation and validation of requirements.
- Failure Mode and Effects Analysis (FMEA). 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.

- Defence-in-Depth and Diversity Analysis. Defence-in-Depth and Diversity Analysis is one of the means of investigating vulnerability of safety systems to common cause failure. See NP-T-3.12, Ref. [12].
- 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, reliability block diagrams, and fault tree analysis.
- Validation. Validation testing involves deterministic techniques and may include statistical techniques.
- Security testing. Security testing usually involves vulnerability assessment and respect of security good practice~~known vulnerabilities/unknown vulnerability testing and penetration testing~~.
- Analysis to confirm that items have been designed for reliability. Such analysis confirms 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 rigours qualification.

  For I&C systems a combination of qualitative analysis, quantitative analysis, and testing is usually needed to verify compliance with reliability requirements.
- Confirmation of functional requirements for various 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 (daylight saving time, leap years, etc.) are examples of other transition points.

2.83. Each assumption of an analysis should be stated, and justified in that analysis.

2.84. The methodology for any analysis conducted should be thoroughly defined and documented together with analysis inputs, results, and the analysis itself.

2.85. Given current state of the art, for an individual system which 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) due to 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, taking into account all of the factors mentioned.

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

2.87. 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].

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

Documentation

2.89. I&C documentation should:

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

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

c. Communicate operationally essential and safety design related information to the plant operating personnel;

d. Provide a foundation for plant maintenance and for potential future revisions to the design;

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

f. Be controlled under a configuration management system, and;

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

2.90. 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.

2.91. 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 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;

h. Interfaces with and dependencies on other plant systems;

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

j. Documentation of test 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 instructions;

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

q. Security design features and their application.

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.

2.92. Documentation of acquisition and supply processes and requirements, design, fabrication activities, software code, and verification and validation should be available for assessment by the operating organization, regulatory authorities, or independent third parties acting for these organizations (see paragraphs 9.95 to 9.98).

LIFE CYCLE ACTIVITIES

Requirement specification

2.93. The overall I&C, each individual I&C system, and I&C components should have documented requirements in appropriate form.

2.94. 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.

2.95. Requirements specifications for the overall I&C and each individual I&C system should be derived from the I&C design basis.

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

2.97. The system and component requirements should specify as applicable:

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, accuracy, and 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 and recovery times);

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

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 access privileges);

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

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. Design constraints.

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

j. Safe response to particular failure modes.

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

2.99. 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.

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

2.101. Requirements engineering is a specific process for assuring the safety goals of I&C systems are included in the design.

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

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

2.104. The origin of and rationale for every requirement should be defined, to facilitate verification, traceability to higher level documents and demonstration that all relevant design basis requirements have been accounted for.

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

2.107. Requirements documentation should refer to, include, or be complemented by additional information, e.g., background 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 target audience.

2.108. Requirements that have a potential impact on safety should be identified as such.

Selection of pre-developed items

2.109. Pre-developed items should be appropriately qualified in accordance with the guidance given in paragraphs 6.79 through 6.135.

2.110. Pre-developed items might be 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 description.

2.111. NP-T-3.12, Ref. [12], gives more detail about the use of COTS devices.

2.112. 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.

2.113. Where feasible, pre-developed items should be configured such that unused functions are disabled.

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

2.115. 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 COTS device could be more difficult because commercial development processes may be less transparent and controlled than those described in this guide. Often qualification is impossible without cooperation from the vendor. The difficulty with accepting a COTS device may often be with the unavailability of the information to demonstrate quality and reliability.

2.116. In the process of deciding whether to use COTS devices or not, the licensee should pay attention to the maintenance of their qualification during the plant lifetime.

2.117. There might, for example, 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 identify such modifications especially with regard to I&C maintenance and 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 become unavailable for purchase.

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

I&C system design and implementation

2.119. 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.

2.120. 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 HDL, and software (if present).

2.121. Hardware might include application specific integrated circuits. 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 account for lower level design decisions made for parts outside the I&C system, e.g. the type and performance of actuated devices.

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

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

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

System integration

2.125. System integration should:

a. Challenge all integration interfaces such as hardware–software or software module to module;

b. Confirm that the interface requirements between the various components of the system are satisfied; 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 out-of-range values, exception handling, and timing related requirements.

2.126. A consistent configuration of verified modules (hardware and software) should be submitted to system integration.

2.127. Software tools are typically used to control the issue of modules for assembly into system components and to control the build used for system validation and for on-site use in operation to

facilitate configuration control and traceability between installed components and validated components.

2.128. A documented traceability analysis should demonstrate that the system integration is complete with respect to the system design specification and that the objectives of paragraph 2.125 have been met.

System validation

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

2.130. For the purpose of this guide, system validation ends when installation into the plant is complete. Some additional elements of system validation may be performed after the system is installed in the plant. These may be included in commissioning tests provided that the results are included into validation test records and appropriate independence is maintained between the design team and the validation team.

2.131. The system subjected to validation testing should be representative of the final configuration of the I&C system at the site.

2.132. The software subject to system validation should be identical to the software that will be used in operation.

2.133. System validation should demonstrate that the system meets all requirements under all possible interface and load conditions.

2.134. 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 validated through supplementary analysis.

2.135. System validation should cover:

a. All parts of the system,
b. The full ranges of interface signals 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.

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

2.137. 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.

~~2.138. The number and scope of tests executed should be documented and justified as sufficient to provide confidence that the system is adequate to perform its functions important to safety.~~

2.138 The functional tests should be designed to cover all behaviours allowed by the functional requirements. The functional tests structural coverage, resulting from these functional requirements, should be justified.

2.139. Validation testing using statistical techniques should be considered.

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

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

2.142. A documented traceability analysis should demonstrate that the system validation is complete with respect to the system requirements specification and that the objectives of paragraphs 2.133 and 2.135 have been met.

2.143. 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.

Installation, overall I&C integration, and commissioning

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

2.145. Equipment receipt inspection, or commissioning tests should verify that the systems and components have not suffered damage during transportation.

2.146. The following paragraphs discuss considerations in implementing the guidance of IAEA NS-G-2.9, Ref. [17] for I&C systems.

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

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

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

2.150. During 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.

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

2.152. 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

2.153. Maintenance and surveillance of I&C systems should be performed in accordance with the guidance of IAEA NS-G-2.6, Ref. [18].

2.154. NS-G-2.6, Ref. [18] provides guidance on planning, organisational aspects, and implementation of maintenance and surveillance, including calibration, of I&C systems.

2.155. The following paragraphs discuss considerations in implementing the guidance of NS-G-2.6, Ref. [18] for I&C systems.

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

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

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

Modifications

2.159. The following paragraphs discuss considerations in implementing the guidance of NS-G-2.3, Ref. [10] for I&C systems.

2.160. The design of I&C upgrades and modification should consider:

a. The limitations due to the physical characteristics of the installed plant, which 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 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 commercially available and the prospects for securing support of such equipment and technology by manufactures or third parties for the installed life of the equipment, and

d. The possible need to update existing design documentation.

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.

2.161. 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.

2.162. The level of rigour should be based upon 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.

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

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

2.165. The life cycle for even the simplest changes should include at least the phases of the individual system life cycle shown in Figure 2.

2.166. Interim Human-Machine Interface configurations that represent a transition between new and existing I&C might need further HFE analysis to accommodate the use of temporary equipment or procedures. Enhancements to the operator interface might increase errors by operations and maintenance personnel for some time after the change. In some cases incremental training might be necessary.

2.167. When an I&C system is replaced, 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.

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

2.169. The consequences of a tool update or change between the time of initial development and modification may be significant and should be subject to impact assessment (for example a compiler upgrade could invalidate previous analysis or verification results concerning the adequacy of the compiler).

3. I&C DESIGN BASES

IDENTIFICATION OF I&C FUNCTIONS

3.1. SSR 2/1 requirement 4 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 paragraph 4.1 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 paragraph 4.2 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 2/1) and a systematic approach is followed to allocate these functions to plant structures, systems and components.

3.5. The required functions of the I&C systems should be determined as part of 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 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 radiation.

CONTENT OF I&C DESIGN BASES

3.7. SSR 2/1 Requirement 14 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 paragraph 5.3 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 then be used to allocate functions to each I&C system and to identify the safety classification of I&C systems. Also, the design basis will be used to establish design, implementation, construction, testing, and performance requirements.

3.12. Note that in some instances, I&C system requirements will be identified as the nuclear power plant design and design basis are developed. Thus, the complete content of the I&C design bases 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 should provide the following information:

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

b. The safety functions to be provided (see paragraph 3.11),

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

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

e. Member State requirements for I&C licensing,

f. Member state requirements for I&C safety classification,

g. Member State requirements with respect to operational requirements,

h. Identification of critical digital assets for computer security,

i. Computer security vulnerability assessments and impact analyses,

j. Information and control needs and allocation,

k. Operating philosophy,

l. Human reliability analysis,

m. Operating personnel roles, and

n. Staffing levels.

3.14. The design bases should specify the necessary capability, reliability and functionality for the overall I&C and each individual I&C system, including:

a. All functional requirements, for example:

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

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

3. The functional requirements for each plant state, each plant operational mode and during extended shutdown;

Note: Functional requirements define, for example, the transformations of inputs to outputs and the actions taken.

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

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

6. The I&C system role in the defence-in-depth concept of the overall I&C architecture;

7. The variables, or combination of variables, to be monitored;

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

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

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

1. The requirements for independence of safety functions;

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

3. The qualitative or quantitative reliability and availability goals;

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.

4. The failure behaviour requirements from the process and plant safety analysis;

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

1. The security and operational constraints that are to be observed in the design; and
2. The security measures to be implemented.

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

1. The design criteria including identification of standards with which the I&C systems should comply;
2. The plant conditions with the potential to functionally degrade the performance of systems and the provisions to be made to retain the necessary capability;
3. The range of internal and external hazards (including natural phenomena) under which the system is required to perform functions important to safety;
4. The range of plant environmental conditions 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.
5. The limitations on materials to be used;
6. The constraints imposed by the physical plant design and layout, with those on equipment location, cable access and power sources; and
7. The physical location of and interfaces between equipment.

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

3.16. In addition to the recommendations given in paragraph 3.14 the design basis for the safety systems should specify:

a. The limiting values of parameters required to actuate safety systems (analytical limits, see paragraph 6.209 and figure 4);

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

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

1. The occasions, incidents, time durations and plant conditions for which manual control is allowed;
2. The justification for permitting initiation or control after initiation, solely by manual means;

3. The range of environmental conditions of the operators' environment when they are expected to take manual action during plant operational states and accident conditions;
4. 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;

d. The conditions under which bypass of I&C safety functions are to be permitted;
e. The conditions which must be satisfied before an actuated protective system can be reset; and
f. The requirements for diverse functions to mitigate the consequences of common cause failure.

4. GUIDANCE FOR I&C ARCHITECTURE

ARCHITECTURAL DESIGN

4.1. The overall I&C architectural design establishes:

- The high level definition of the I&C systems;
- The tiered structure of these systems;
- The assignment of I&C functions to these systems, and
- The communications between I&C systems and the topology of communication links.

4.2. 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 defence in depth concept.

4.3. Individual I&C system architectural design establishes:

- The subsystems that will compose the I&C system;
- The individual I&C items that will compose these subsystems;
- The hierarchical structure of subsystems and the hierarchical structure of individual I&C items within subsystems;
- The assignment of I&C functions to individual I&C items;
- The layout of communications between items and subsystems within the individual I&C system; and
- The partitioning to avoid unnecessary system complexity and unnecessary interactions between individual I&C system elements.

4.4. Modern I&C systems are more integrated and more complex than were the earlier generations of I&C systems. A well designed I&C system architecture will ensure proper implementation of a defence-in-depth concept and locate essential complexity in systems where it can be better managed or where it will pose less risk to plant safety.

4.5. The overall I&C architecture and the individual system architectures should satisfy the plant requirements, including system interfaces, performance requirements (e.g., timing and reliability), and facilitate achievement of computer security goals.

4.6. SSR 2/1 Requirement 7 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.

4.7. INSAG-10, Ref. [19] and INSAG-12, Ref. [20] explain the concept of defence-in-depth and the levels of defence-in-depth.

4.8. The overall I&C architecture should not compromise the defence-in-depth strategy of the plant design.

4.9. The overall I&C architecture should define the defence-in-depth and diversity strategy to be implemented within the overall I&C.

4.10. Defence-in-depth within the overall I&C architecture is achieved by independent lines of defense so that the failure of one line of defence is mastered by the following one.

CONTENT OF THE OVERALL I&C ARCHITECTURE

4.11. The overall I&C architecture should:

a. Include all I&C functions needed to fulfil the plant design basis;

b. Identify topics that are to be dealt with consistently across all I&C systems;

   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.

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

   1. Support the plant defence-in-depth concept;
   2. Support overall I&C design basis requirements for independence; and
   3. Adequately separate systems and functions of different safety classes;

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

e. Establish the design strategies to be applied to fulfil the reliability requirements of each safety function allocated to the overall I&C architecture;

   Strategies for achieving reliability requirements might include, for example, compliance with the single failure criterion, redundancy, independence between redundant functions, fail-safe

design, diversity, and testability. Section 7 discusses considerations in implementing strategies to achieve reliability.

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

g. Provide necessary information in the main control room, the supplementary control room, and other areas where information is needed for operation or accident management;

h. Provide necessary operator controls in the main control room, the supplementary control room, and other areas where controls are needed for operation or accident management; and

i. Provide 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 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. Provide all I&C functions needed to fulfil the role assigned to it in the overall I&C architectural design;

b. Where appropriate, partition the system into redundant divisions and specify the required degree of independence between divisions;

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 the I&C items to be included in each division;

d. Describe the allocation of I&C functions and other system requirements to each I&C item;

e. Define the interfaces and means of communications between the I&C items within the system; and

f. 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. Examples of such CCF sources 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 the different levels of the plant defence-in-depth concept.

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

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

4.18. Redundant divisions within safety systems should be independent of each other.

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

4.20. Safety 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 6.56.

4.21. Safety systems or components may also be operated from operator controls of 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 lower safety classification if the recommendations of paragraphs 6.26 to 6.57 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, internal hazards or external hazards in which their response is necessary.

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

CONSIDERATION OF COMMON CAUSE FAILURE

4.25. SSR 2/1 Requirement 24 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. [8], defines a common cause failure as failure 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 development tools, failure propagation between systems or components, or inadequate specification, 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 as independent as is practical.

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

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

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

4.32. An analysis should be done of the consequences of each PIE within the scope of safety analysis in combination with CCF that will prevent a protection system from performing the needed safety functions.

4.33. A defence-in-depth and diversity analysis is one method of performing the analysis described in paragraph 4.32. See paragraph 2.82.

4.34. If the analysis described in paragraph 4.32 determines that a PIE in combination with a 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 CCF is not achievable, but justification should be provided for accepting identified vulnerabilities.

Diversity

4.36. The IAEA Safety Glossary, Ref. [8], 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 reduce CCF vulnerability resulting from requirements, design, manufacture or maintenance error, and to include 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 common cause mitigation that is claimed.

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

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

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 states:

> The engineering design rules for items important to safety at a nuclear facility 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.~~1~~2. SSR 2/1 Requirement 22 states:

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

5.~~2~~3. SSR 2/1 paragraph 5.34 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;
>
> (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.~~3~~4. SSR 2/1 paragraph 5.36 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.

~~5.4. The possibility that the failure or spurious operation of an item important to safety may directly cause a PIE or make the consequences of a PIE worse should be considered when determining safety classification.~~

~~5.5. 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.~~5.5. The draft Safety Guide DS 367 Safety Classification of Structures, Systems and components in Nuclear Power Plants, Ref. [21] provides recommendations and guidance on how to meet the requirements established in Refs [1] and [7] 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. [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, the classification process should primarily consider:

- The design basis of 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 the facility, 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 or make the consequences of a PIE worse should be considered when the list of 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. The I&C system functions should then be categorized on the basis of their safety significance, using a constant risk approach, 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 367, 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 if desired.

~~5.6. The various Member States use many different classification schemes. This guide does not recommend any specific scheme. The classification scheme that is defined for plant equipment in the IAEA safety glossary is used to grade the recommendations of this guide according to safety significance.~~

~~5.7. The classification terminology given in the IAEA safety glossary applies to items important to safety. Items are systems, structures, or components. In this guide the same classification terms are also applied to specific functions performed by an item.~~

~~5.8. All I&C functions, systems, and components fit into one of two safety categories defined in the IAEA safety glossary: important to safety or not important to safety.~~

~~5.9. An item important to safety is an item that is part of a safety group or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public. Items important to safety include:~~

~~Those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public;~~

~~Those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions;~~

~~Those features that are provided to mitigate the consequences of malfunction or failure of structures, systems and components.~~

~~5.10. Functions, structures, systems, and components important to safety are further categorized as either safety or safety related.~~

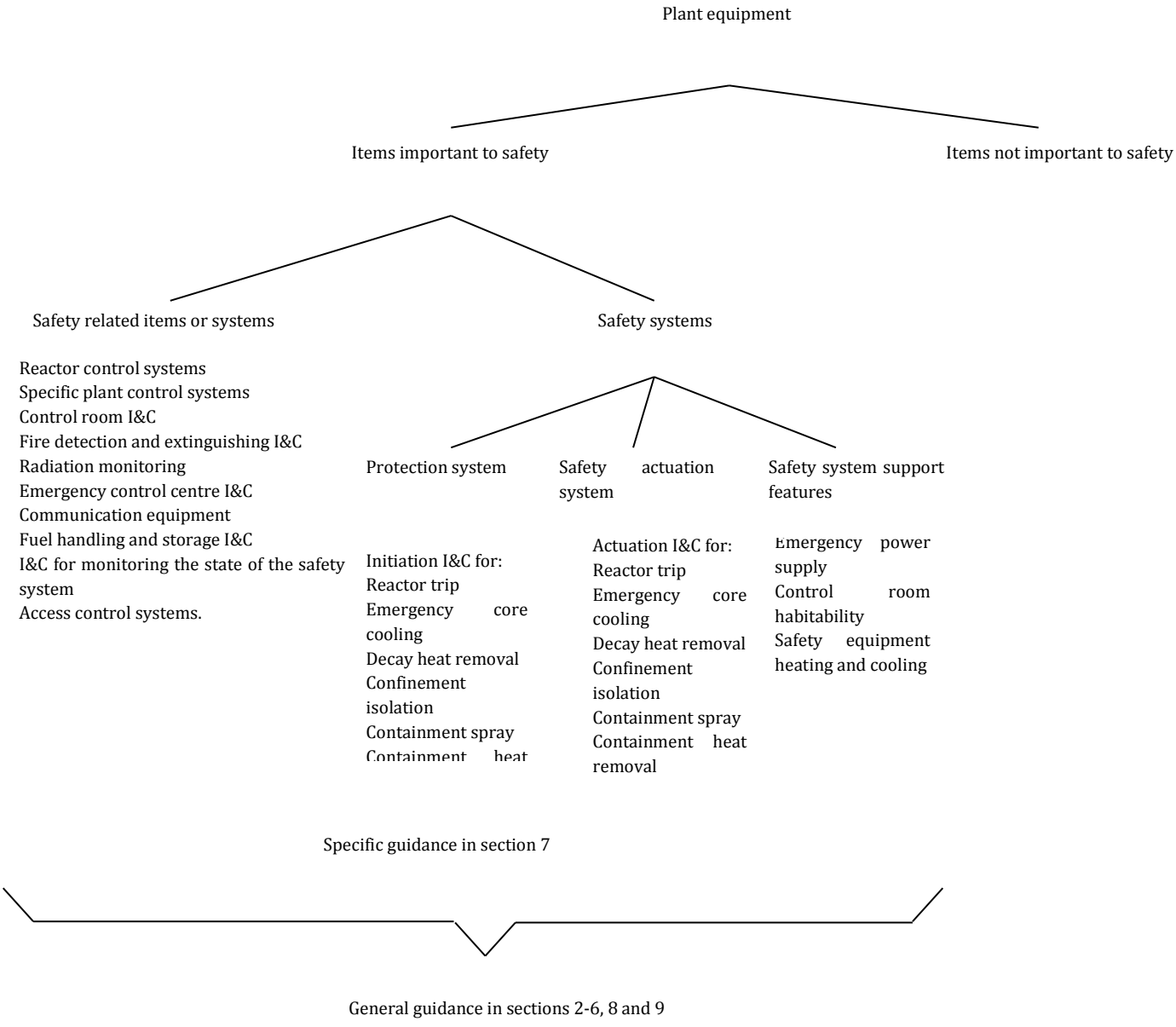
~~5.11. Safety classified functions, structures, systems, and components are those provided to ensure control of reactivity, removal of heat from the core and confinement of radioactive material, shielding against radiation, and control of planned radioactive releases, limitation of accidental radioactive releases, or to limit the consequences of anticipated operational occurrences (AOO) or design basis accidents (DBA). (Note: safe shutdown is the same as achieving a controlled state, which is defined in SSR 2/1.) The term "safety component" is used in this guide to mean a component of a safety system.~~

~~5.12. Safety related items are items important to safety that are not part of a safety system. This guide avoids using the term 'safety related' because it is used with a very different meaning in some Member States.~~

~~5.13. The classification scheme described in paragraphs 5.8 to 5.12 can be mapped to most of the Member State classification schemes currently in use. The classification schemes of some Member States have more than two categories of items important to safety.~~

~~5.14. Figure 3 illustrates the relationship between the safety categories used in this guide, and indicates the safety classifications that are typically assigned to I&C functions that are commonly provided.~~

~~5.15. Some member states apply a two step process to classify items important to safety. In these states the safety significance of the function to be performed is categorized using a scheme that follows the philosophy of this Safety Guide. Once the function is categorized, the systems or components that implement the function are then placed into safety classes. This approach is particularly useful when more than one system has responsibility for fulfilling a function. In this case the different systems might be placed in different safety classes.~~



~~FIG. 3. Examples of I&C systems important to safety. (Examples are given for illustration. Some systems are listed in one column although they might also belong in multiple columns, e.g. control room I&C.)~~

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

GENERAL

6.1. I&C systems should fully implement 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 its safety requirements. Examples of complexity to be avoided are the inclusion of functions that do not contribute to the safety functionality or its reliability, use of design and implementation features not amenable to sufficient analysis or verification, and use of implementation platforms that are too complex to facilitate an adequate safety demonstration. Architecture 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 complexity.

DESIGN FOR RELIABILITY

6.6. SSR 2/1 Requirement 23 states:

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

6.7. SSR 2/1 Requirement 62 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 paragraph 6.34 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.

~~6.5. The intent of avoiding complexity is to keep the I&C system as simple as possible but still fully implement its safety requirements. Examples of complexity to be avoided are the inclusion of functions that do not contribute to the safety functionality or its reliability, use of design and implementation features not amenable to sufficient analysis or verification, and use of implementation platforms that are too complex to facilitate an adequate safety demonstration. An architecture with simple interactions and simple communication links is needed therefore. Careful documentation and~~

~~review of the rationale for each requirement is one effective means for avoiding inessential complexity.~~

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 states:

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

6.11. SSR 2/1 paragraph 6.39 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 PIE in the presence of the following:

a. Any single detectable failure within the safety system in combination with:

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

c. All failures caused by the single failure,

d. All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety group, and

e. The removal from service or 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. Management systems are expected to result in properly addressing known errors. The effects of unknown errors cannot be predicted, 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 CCF due to such errors is discussed in section 4.

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

6.16. Non-compliance with the single failure criterion may be justified for:

- Very rare PIEs;
- Very improbable consequences of PIEs;
- Withdrawal from service of certain components for purposes of maintenance, repair or periodic testing, for limited periods of time;
- Features that are provided only for response to design extension conditions; or
- Postulated failures whose likelihood can be shown to be sufficiently remote as to be discounted.

6.17. Great care is needed when analysing low frequency events, such as external hazards, to justify non-compliance with the single failure criterion. It is advisable to pay particular attention to ensuring the long-term availability of the electrical and other support systems that that are necessary for operation and monitoring of safety systems.

6.18. 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.

6.19. The situations in which the single failure criterion is not met, the maintenance, repair or testing, should be consistent with plant operating limits and conditions.

6.20. 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

6.21. I&C systems should be redundant to the degree needed to meet the I&C reliability requirements.

6.22. Redundancy is commonly used in I&C systems to achieve system reliability goals including conformity with the single failure criterion. Redundancy is not fully effective unless the redundant elements are also independent. Taken alone, 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

6.23. SSR 2/1 Requirement 21 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.

6.24. SSR 2/1 Paragraph 5.35 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.

6.25. The IAEA Safety Glossary, Ref. [8], defines independent equipment as equipment that possesses both of the following characteristics: (a) The ability to perform its required function is unaffected by the operation or failure of other equipment; (b) the ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function.

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

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

6.28. When isolation devices are used between systems of different safety importance, they should be a part of the system of higher importance.

6.29. Measures provided for isolation from various physical effects, electrical faults, and communications errors do not necessarily need to be in the devices being protected. Features for isolating systems from the various different kinds of threats do not need to be in the same physical device or 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 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 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.

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

Physical separation

6.31. Physical separation:

- Protects 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;
- May be used to protect against common cause failure due to normal, abnormal, or accident environments, the effects of design basis accidents, or the effects of internal and external hazards.

  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;
- May reduce the likelihood of CCF as a result of external events that have localized effects (e.g., aircraft crash, tornado, or tsunami); and
- Reduces the likelihood of inadvertent errors during operation or maintenance on redundant equipment.

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

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

6.34. 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.

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

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

6.37. NS-G-1.7, Ref. [22] and NS-G-1.11, Ref. [23] give additional guidance on protection against fires and other internal hazards.

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

- Containment penetrations,
- Motor control centres,
- Switchgear areas,
- Cable spreading rooms,
- Equipment rooms,
- The main and other control rooms, and
- The plant process computer.

Electrical isolation

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

6.40. Safety systems and components should be electrically isolated from systems and components of lower safety classification.

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

6.42. Electrical 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.

6.43. Examples of provisions for electrical isolation include: the absence of electronic connections, electronic isolating devices, optical isolating devices (including optical fibre), relays, separation distance, internal mechanical structures, or combinations of these features.

Associated circuits

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

a. Analysed or tested to demonstrate that the association does not unacceptably degrade the safety class circuits with which it is associated;

   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 as part of the safety division with which it is associated; and

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

Functional Independence

6.45. 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 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 redundancies.

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

6.47. Inputs from I&C systems of lower safety classification should not adversely affect the ability of safety systems to perform their safety functions.

6.48. Safety systems may, however, depend upon inputs from non-safety maintenance systems, for example, to perform maintenance, software updates, testing, or to set configuration data. Such inputs are typically made with the affected division off line and are verified after data are entered.

6.49. Monitoring systems of lower safety classification may be connected to safety systems provided that it is demonstrated that they cannot disturb them. When safety systems may be connected to maintenance systems of lower safety classification, the connection should be made only: when the affected division or channel is offline, use of data from the maintenance system is restricted to a specific purpose, and connection of the maintenance system complies with computer security programs.

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

6.51. The plant operational modes in which the maintenance system may be connected should be defined.

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

6.53. 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.

6.54. In computer systems, one-directional, broadcast data communication is often used where computer based systems of a higher classification provide data to systems of lower safety classification. Hardware characteristics that enforce the one-directional feature, e.g., the use of a link that is connected only to a transmitter in the higher classified system and only to a receiver in the lower classified system, are a favoured means of ensuring one-directional communication.

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

- Completion of safety actions cannot be interrupted by commands from the system of lower safety classification, and
- The potential for failures in the system of lower safety classification that cause spurious actuation is assessed and shown to be acceptable.

6.56. When safety systems actuators act on information from other systems, including those of lower safety classification, provisions 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.

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

Diversity

6.58. 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 the adequate reliability of 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 the different Member States.

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

6.60. Where diversity is provided to cope with the potential for CCF, the use of more than one type of diversity should be considered.

6.61. Examples of different types of diversity include:

- Design diversity: achieved by using different design approaches to solve the same 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 vs. digital, solid-state vs. electromagnetic, computer-based vs. FPGA-based);
- Functional diversity: achieved by systems that take different actions to achieve the same safety intent;
- Life cycle diversity: achieved by using different design organizations, different management teams, different design and development teams, and different implementation and testing teams.

6.62. Where diversity is provided the choice of the types of diversity used should be justified as achieving the common cause mitigation that is claimed.

6.63. Diversity need not always be implemented in separate systems. For example, functional diversity and signal diversity might be implemented within a single system.

6.64. The provision of diversity also involves avoiding areas of potential commonality in the application of diversity, such as materials, 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. Claims for diversity based only on a difference in manufacturers' names or model numbers are insufficient without consideration of this possibility.

Failure modes

6.65. SSR 2/1 Requirement 26 states:

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

6.66. Loss of power to any I&C component or 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.

6.67. 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 place the system in a safe condition.

6.68. Where such practices are applied, failures of the fail-safe design features themselves should be considered when applying the guidance of paragraph 6.66.

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

6.70. Knowing the failure modes of components is important in applying 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 analyses.

6.71. The failures that might result from software errors are difficult to predict. Nevertheless, it is not necessary to know how the software fails to determine the possible failure states as seen at device terminals. The most likely possible failure modes could be identified and classified into a manageable set of possibilities, e.g. wrong output, delayed output, frozen output.~~The failure modes can be classified into a manageable set of possibilities, e.g., output fails high, output fails low, output fails in place, produces incorrect message, produces incorrect checksum, produces incorrect data, produces incorrect address.~~

6.72. The failure modes that are most likely to result from systematic errors 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 errors. Disciplined development processes (see section 2), Hazard analysis (paragraphs 2.56 to 2.65), the concept of defence in depth (see section 4), and the application of diversity (see paragraphs 6.58 to 6.64) are more effective tools for reducing the number of such errors, and coping with the effects of such errors that remain.

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

6.74. It is preferred that failures be self-revealing except where this would put the system in an unsafe condition or result in spurious actuation of safety systems.

6.75. 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.

6.76. As far as practicable, the failure of a component should not cause spurious actuation of safety systems.

6.77. On restart or restoration of power 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

6.78. SSR 2/1 Requirement 30 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.

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

6.80. The qualification of I&C components should include their software, HDL descriptions, and process interfaces, if any.

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

6.82. The qualification programs 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.

6.83. 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 extrapolate test results or operating experience under relevant conditions;

g. Evaluation of manufacturer production processes;

h. Inspection of components during manufacture.

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

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

6.86. 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.

6.87. For safety systems, qualification evidence based upon operating experience is normally combined with type testing, and testing of supplied equipment, as well as evaluation of manufacturers' production processes, or inspection of components during manufacture.

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

6.89. 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.

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

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

Suitability and correctness

6.92. The equipment qualification program should demonstrate that the design of I&C systems, and components meet all functional, performance, and reliability requirements contained in the I&C design bases and equipment specifications.

6.93. Examples of functional requirements include, functionality required by the application, functionality required to support system or equipment operability, operator interface requirements, and input /output range requirements.

6.94. Examples of performance requirements include accuracy, resolution, range, sample rate, and response time requirements.

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

6.96. The equipment qualification program should demonstrate that the design and the as-built I&C systems and installed components correctly implement the qualified design.

Environmental qualification

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

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

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

6.100. Details of equipment qualification requirements, processes and methods are given in IAEA Safety Report Series No. 3 – Equipment Qualification, Ref. [24].

Components exposed only to mild environments

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

Components exposed to harsh environments

6.102. 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 (harsh environments) should show 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.

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

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

6.105. If it is necessary to separately test for different environmental conditions (e.g., separate tests for radiation 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.

6.106. The most rigorous environmental qualification methods may need to be applied only to safety components.

6.107. Environmental qualification of safety components that are required to operate in harsh environments should include type tests.

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

Internal and external hazards

6.109. 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.

6.110. 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. [22].

6.111. 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 [23].

6.112. 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. [25].

6.113. 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. [26].

Electromagnetic qualification

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

6.115. EMI includes Radio Frequency Interference (RFI) and as used in this Safety Guide includes electrical surges, for example, voltage spikes resulting from switching transients.

6.116. 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's capability to withstand the disturbances caused by the components around it or connected to it.

6.117. Significant sources of electromagnetic interference include fault current clearance by switchgear, circuit breaker or fuse 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.

6.118. 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, and testing to demonstrate that electromagnetic emissions are within tolerable levels.

6.119. Techniques for minimizing the production and coupling of electromagnetic noise include:

- Suppression of electromagnetic noise at the source;
- Separation and isolation of instrument and control signal cables from power cables;
- Shielding of equipment and cables from external magnetic and electromagnetic sources;
- Filtering 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, raceway, cabinets, components, and cable shields.

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

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

6.122. International EMC standards for industrial environments may serve as the basis for the requirements provided that they are supplemented, where necessary, to cover the plant-specific EMC that might be more demanding. Determination of EMC requirements 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).

6.123. Establishing the EMC environment of I&C components at each nuclear power plant unit generally involves unit-specific analyses. These analyses are used to judge adequacy of each I&C component's EMC characteristics.

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

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

- 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 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.

6.126. In the vicinity of certain sensitive equipment it may be appropriate to establish exclusions zones where operation of wireless devices and other portable EMI sources (e.g., welders) is restricted.

6.127. The equipment qualification program should show 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.

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

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

6.130. Emission limits placed on individual components should be below the EMI operating envelope by an amount that is sufficient to ensure that no single item makes a significant contribution to the EMI hazard.

6.131. The equipment qualification program should show that electromagnetic emissions of all plant equipment are within the defined limits.

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

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

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

6.135. DS-430, Ref. [9] gives recommendations for grounding, cable selection, and cable routing to reduce production and propagation of electromagnetic interference.

DESIGN TO COPE WITH AGEING AND OBSOLESCENCE

6.136. SSR 2/1 Requirement 31 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.

6.137. SSR 2/1 Paragraph 5.51 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.

6.138. SSR 2/1 Paragraph 5.52 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.

6.139. The qualified life of electrical and electronics systems and components might be considerably less than plant life.

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

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

6.142. Identification of potential ageing impacts involves first understanding of the relevant ageing phenomena for the various I&C components.

6.143. 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 6.142.

6.144. Maintenance programs should include activities to identify any trend towards degradation (ageing) that could cause the equipment to become incapable of performing its safety function.

6.145. Examples of monitoring techniques include:

- 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.

6.146. Examples of means to address ageing impacts include:

- Component replacement before the end of its 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.

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

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

6.149. On-going qualification might show that the qualified life of a component is validated or is indicated to be different than 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.

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

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

6.152. At the present time it is expected that ageing or obsolesce may cause the service life of some I&C systems to be significantly shorter that that plant life. 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 installation of new equipment and associated cable.

6.153. NS-G-2.12, Ref. [27] gives additional guidance on ageing and obsolescence management. It includes a discussion of the interface between equipment qualification and the ageing management program.

CONTROL OF ACCESS TO SYSTEMS IMPORTANT TO SAFETY

6.154. SSR 2/1 Requirement 39 states:

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

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

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

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

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

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

TESTING AND TESTABILITY DURING OPERATION

6.160. SSR 2/1 Requirement 29 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.

6.161. SSR 2/1 Paragraph 6.35 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

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

6.163. Test provisions that are permanently connected to safety systems are themselves safety systems unless they meet the independence guidance of paragraphs 6.26 to 6.57.

6.164. 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.

6.165. Periodic tests during plant operation will normally be needed to achieve the reliability required of safety systems; however it is sometimes desirable to avoid testing during operation if it puts at risk

normal or safe plant operation. The capability for testing and calibration during power operation is not necessary if doing so would adversely affect the safety or operability of the plant.

6.166. Where the ability to test a safety system or component during power operation is not provided:

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 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

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

6.168. These features should include input rationality checking.

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

6.170. Designing systems or components so that their failure would be self-revealing is one means of accomplishing the recommendation of paragraph 6.167.

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

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

6.173. 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

6.174. SSR 2/1 paragraph 5.46 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.

6.175. The test provisions for I&C systems (both manual 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.

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

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

Test interfaces

6.178. SSR 2/1 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.

6.179. Provisions for testing I&C systems and components should:

a. Have appropriate test interfaces and status indication,

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

b. Operate such that faults in the equipment are readily detectable,

c. Have features to prevent unauthorized access,

d. Be readily accessible to testing staff and test equipment,

e. Have the communications facilities needed to support the tests.

f. Be located such that neither testing nor access to the testing location expose operating personnel to hazardous environments,

   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.

6.180. Where equipment to be tested is located in hazardous areas, facilities should be provided to allow testing from outside the hazardous area.

Test program

6.181. The design of I&C systems should include identification of a testing and calibration programme that supports implementation of the guidance given in NS-G-2.2, Ref. [31]; NS-G-2.4, Ref. [32], NS-G-2.6, Ref. [18]; and NS-G-2.14, Ref. [33].

6.182. An I&C test program will normally include:

- A description of program objectives;
- Identification 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 test intervals;
- A description of required documentation and reports;
- A requirement for periodic review of program effectiveness; and
- Specification of the individual test procedures that will be used to control the conduct of tests.

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

6.184. The tests defined in the test programme should ensure that, 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 and performance requirements.

6.185. The test program should arrange tests into a sequence such that the overall condition of the system or component under test can be immediately assessed without further testing of other components or systems.

6.186. Conduct of the test programme should not cause deterioration of any plant component beyond that provided for in the design.

6.187. Conduct of the test program and the decision about when the end of qualified life for a component has been reached may, for example, need to consider wear and aging due to the testing.

6.188. Implementation of the test program should provide for:

a. Objective information on 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 repetition of the failed test can be credited as establishing operability.

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.

6.189. The test program 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 and performance requirements of safety functions 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 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;

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 plant component configuration parameters unless previously identified as service parameters;

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

k. Individually test each sensor, to the extent practicable.

6.190. In addition to the recommendations of paragraph 6.190, the processes defined for periodic tests and calibration of safety systems should:

a. Be a single on-line test;

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. Independently confirm the functional and performance requirements of each channel of sense, command, execute, and support functions;

c. Include as much of the function under test as practical (including sensors and actuators) without jeopardizing continued normal plant operation;

d. Wherever possible, be accomplished under actual or simulated operating conditions, including sequence of operations;

e. Test and calibrate all variables used, where combinations of variables are used to generate a particular signal for a safety system; and

f. Be capable of detecting faults in redundant equipment.

Redundant equipment might be equipment in redundant divisions or redundant equipment within a division.

6.191. 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.

6.192. 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

6.193. The design of I&C systems should include maintenance plans for all systems and components.

6.194. 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.

6.195. Design to facilitate maintenance, troubleshooting and repair includes:

- Avoiding locating equipment in areas where conditions of extreme temperature, or humidity are expected during plant normal operation;
- Avoiding locating equipment in areas where there is a risk of high radiation levels. (See NS-G-1.13, Ref. [34]);
- Taking 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.

6.196. If components are located in inaccessible areas examples of other strategies for coping with failure include:

- 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.

6.197. Means provided for the maintenance of I&C systems should be designed such that any effects on the safety of the plant are acceptable.

6.198. Typical examples for such means are the disconnection of one division in a system with redundant divisions, or provisions for alternative manual actions.

PROVISIONS FOR REMOVAL FROM SERVICE FOR TESTING OR MAINTENANCE

6.199. 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.

6.200. The design should ensure that systems cannot unknowingly be left in a test or maintenance configuration.

6.201. Removal from service of any single safety system component or division should not result in loss of the required minimum redundancy unless system operation with acceptable reliability can be adequately demonstrated.

6.202. SSR 2/1 Paragraph 6.36 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.

6.203. Inoperability or bypass of safety system components or divisions should be indicated in the control room.

6.204. For items that are frequently bypassed or frequently rendered inoperable, these indications should be automatic.

6.205. NS-G-2.6, Ref. [18] provides guidance for returning systems and equipment to service after testing and maintenance.

SETPOINTS

6.206. SSR 2/1 Paragraph 5.44(2) states:

> The requirements and operational limits and conditions established in the design for the nuclear power plant shall include…limiting settings for safety systems….

6.207. The operational limits and conditions for safe operation include I&C setpoints for safety systems.

6.208. Determination of I&C safety system setpoints usually considers the following values:

- Safety limits – limits on certain operational parameters within which the operation of the reactor has been shown to be safe.

  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.

  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 Trip setpoint – a predetermined value for actuation of the final setpoint device to initiate a protective action.

- Allowable value - The 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 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 – The 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.

  Limiting settings for safety systems, also called safety system settings or limiting safety system settings, is a legal term in some Member States. These might be expressed as trip setpoints, allowable values, or both. NS-G-2.2, Ref. [31] provides additional guidance on establishing and implementing safety system settings.

6.209. Figure 4 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.

6.210. Setpoints may be either 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 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 account for measurement and channel biases, uncertainties and any changes to these values which 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 HMI should be determined and followed throughout the design, installation and operation phases of the plant.

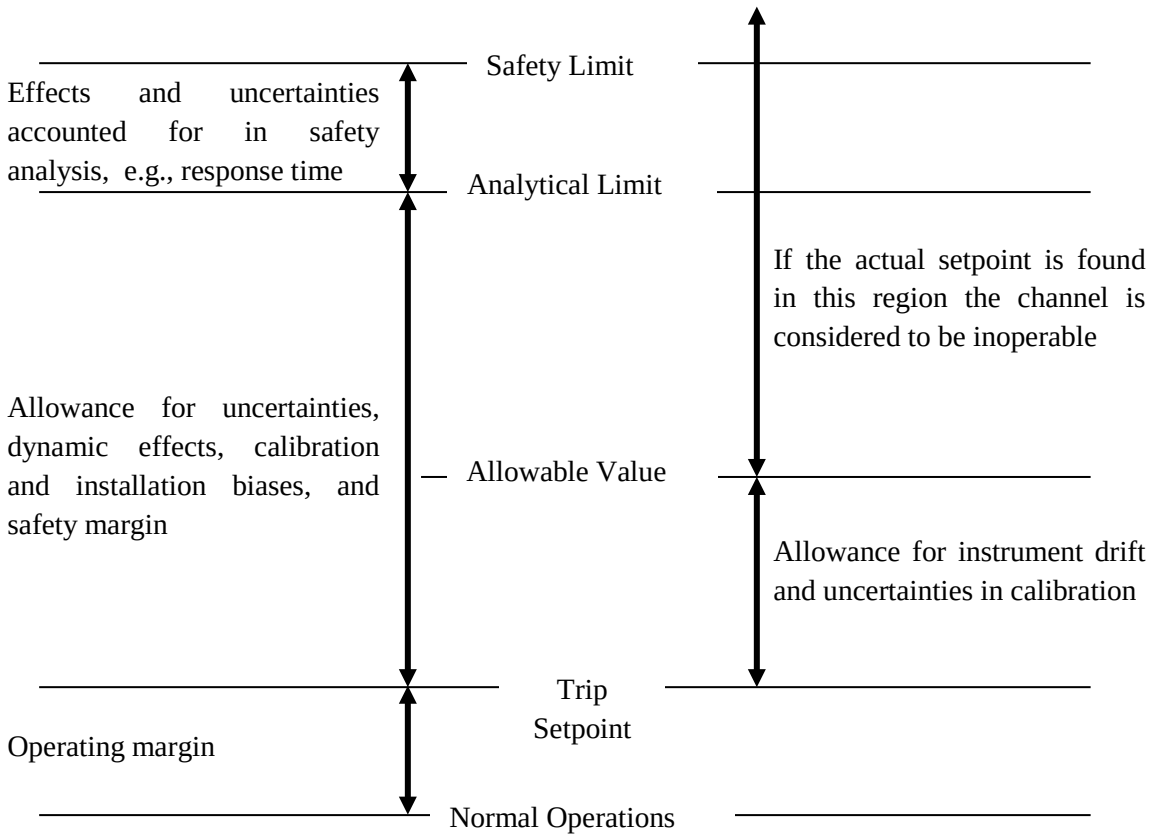


FIG. 4. Setpoint terminology and errors to be considered in setpoint determination

6.214. A suitable identification scheme would 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, maintenance, and construction staff as well as for use to label the controls, displays and indications.

6.216. I&C components in the plant should 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.

6.218. The components of different safety divisions should be easily distinguishable from each other and from components of lower safety classification.

6.219. Clear identification of components reduces the likelihood of inadvertently performing maintenance, tests, repair or calibration on an incorrect channel.

6.220. Identification may, for example, take the form of tagging or colour coding.

7. SYSTEM AND EQUIPMENT SPECIFIC DESIGN GUIDELINES

SENSING DEVICES

7.1. Measurements of plant variables should be consistent with the requirements of the I&C and 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, and range needed to monitor the variable in all plant states during which the information from the sensor is needed.

7.6. The consequences of sensor CCF combined with a PIE should be no greater than those considered to be acceptable for the analysis described in paragraphs 4.30 to 4.34.

7.7. No identified CCF vulnerability of sensing devices should have the potential of denying operators the information and parameters that they need to control and mitigate 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 over effects do not prevent the required function from being performed.

7.9. If the spatial dependence of the measurement of a variable (i.e., the measured value of variable depends upon 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 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 defense 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 and manual control modes, and where switchover occurs between an online 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 automatic control system failures, including multiple spurious control system actions, should not exceed the acceptance criteria established for anticipated operational occurrences.

PROTECTION SYSTEM

7.15. SSR 2/1 Requirement 61 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 and manual safety actions

7.18. SSR 2/1 Paragraph 6.33(b) states:

> The design (of the protection system) shall … 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 protection system safety actions except those for which manual action alone has been justified.

7.20. Typically automatic initiation will be provided for most protection system functions.

7.21. Examples of situations in which manual action alone might be justified include:

- 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 PIE.

7.22. In order to justify that manual action alone is acceptable it should be shown that:

a. Safety systems provide the operators with information that is clearly presented and sufficient to make reasoned judgments on the need to initiate the required safety actions;

b. The operator is provided with written procedures and training for the safety tasks;

c. The operator is provided with sufficient means of plant control to perform the required actions;

d. The communication links between operators carrying out the actions are adequate to ensure the correct accomplishment of these actions; and

e. The operator is allowed sufficient time to evaluate the status of the plant and to complete the required actions.

For new designs it 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 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 action provides a form of defence in depth for abnormal conditions and supports long-term post accident operation.

7.26. Mechanical safety systems are, for example, the individual divisions of control rods, emergency feed water, emergency core cooling, or containment isolation.

Information display

7.27. SSR 2/1 paragraph 6.33(c) states:

> The design (of the protection system) shall … 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 protection system functions, the state of each trip and actuation function in each division, and the state of each system initiation.

Protection system sensors and settings

7.29. The sensors that provide signals to the protection system should only feed other systems through appropriate buffering and isolation devices.

7.30. Design techniques, such as functional diversity, redundancy and signal diversity, should be used to the extent practical 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 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 means for determining the setpoint values for each 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 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 needs to be operated.

7.37. Indication of the operational bypass 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 bypass are not met:

a. Remove the activated operational bypass,
b. Put the plant in a condition where the operational bypass is permissible, or
c. Initiate appropriate protective actions.

Latching of protection system functions

7.39. SSR 2/1 paragraph 6.35(a) states:

> The design (of the protection system) shall 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 protection system actions is normally implemented at the level of actuation signals to plant equipment. Seal-in of individual measurement channels is not required.

7.42. Once a protection system function is initiated all actions performed by that function should be completed.

7.43. The guidance of 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. [9], gives guidance on electrical protection of items important to safety.

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 safety systems 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 actions of the protection system.

7.47. Spurious initiation of protection system functions could lead to:

- Unnecessary stress on equipment and reduction of plant life,
- The need for other safety actions,
- Erosion of the operators' confidence in equipment, potentially leading to subsequent disregard 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 the plant requires protection, then safe conditions should be maintained through actions that are initiated and carried out by parts of the protection system or 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 requirement 64 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 paragraph 6.38 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 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 paragraph 6.32(a) states:

> The protection system shall be designed to be capable of overriding unsafe actions of the control system.

7.54. If a PIE can cause a control system action that results in a plant condition requiring initiation of a protection system function, then the same PIE should not prevent proper action of the safety systems providing that action.

7.55. The possibility that a failure in the protection system may be itself a PIE that triggers a control system action for which the protection system is necessary cannot be disregarded.

7.56. Examples of measures that have been used to prevent interference between control and protection systems causing incorrect operation include:

- Provision of separate instrument channels for protection and for control;
- Additional equipment in the safety group to deal with the potential interference;
- Provision of barriers or alternative plant arrangements to limit the damage resulting from the PIE; or
- Combinations of these items such that the safety group and plant design are sufficient to maintain the plant conditions within acceptable limits.

7.57. Paragraphs 7.52, 7.54 and 7.55 are meant 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 lower safety classification, any protection system demand for actuation of a 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 protection system demand overrides control system commands.

POWER SUPPLIES

7.60. Power supplies for I&C systems, regardless of type (e.g., electrical, pneumatic, hydraulic), should have classification, reliability provisions, qualification, isolation, testability, maintainability, and indication of removal from service, 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 I&C design bases.

7.62. I&C systems may be transferred by operators or by automatic switching action to a stand-by power supply instead of the normal supply when operating circumstances need it, provided that the functions of the I&C systems can tolerate the associated interruption in supply. Normally the transfer system will be treated as part of the power supply system and will be of the same safety category 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 which 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 paragraph 6.133).

7.65. DS-430, Ref. [9] provides recommendations for electrical power supplies and associated distribution systems. Recommendations for other forms of power supply (e.g., pneumatic, hydraulic, mechanical) are currently contained in the historical document NS-G-1.8, Ref. [34], 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 Hardware Description Languages.

7.67. SSR 2/1 requirement 63 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 operator interfaces, capability for self test and self diagnostics, 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 they are in analogue systems. In digital technology functions are combined in one or more processing units. Combining functions in a processing unit could lead to a high degree of complexity and the failure of a processing unit will result in simultaneous failure of several functions.

7.70. Full verification and validation of such complex components could be very difficult or even practically impossible if they were not correctly designed. Unidentified errors ~~are likely to~~might exist and they might exist in all redundant component uses or to spread to other systems based on the same platform, because software modules, programmed devices, or libraries could be common to all.

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 processing or communication load of a digital system could affect transmissions speed and response time, if they were not correctly designed. Changes to processing or communications load might result from changes in plant parameters, operation in different system or plant states, or equipment failures.

7.72. Section 3 of Ref. [12], NP-T-3.12: Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants discusses 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 the response time and accuracy requirements in all specified operating conditions and all possible conditions of data loading.

7.74. Safety I&C systems should be designed to have deterministic behaviour, i.e., any given input sequence that is within the item's specification always produces 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 process-related interrupts, so that no plant condition can directly affect the rate of interrupts the I&C system needs to handle,
- Allocating resources statically at design time, and
- Bounding iterations of loops, set by predefined limits.

7.76. Response time and accuracy of digital systems ~~are heavily influenced by~~functionally depend ~~-~~on the sample rate, and on the processing ~~processor~~ cycle time ~~and processor speed~~. In systems not 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:

- 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 paragraphs 6.27 to 6.57.

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 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. Consequently, the implementation of paragraph 7.87 will involve defining what constitutes 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 communications 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 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 message elements to be predefined include: message protocol, message format, and the set of valid messages.

Data communications independence

7.95. This section supplements the guidance of paragraphs 6.27 to 6.57 with guidance that is specific to data communications in digital systems.

Avoidance of common cause failure

7.96. The data communication network topology and media access control should be designed and implemented to avoid CCF of safety systems.

Communications between safety divisions

7.97. Communications, including communications errors or failures, in a safety divisions should not prevent connected safety divisions from performing their safety function.

7.98. The intent of the recommendation in paragraph 7.97 is to prevent the propagation of failures between divisions. Typically a combination of data validation (see paragraphs 7.82 to 7.94), and buffering is employed.

~~7.99. One-directional communication without handshaking is an acceptable and commonly used means of complying with the recommendation of paragraph 7.97.~~

7.99. Architectures using a central hub or router where communications from multiple safety divisions are transmitted across a single link should not be used.

Communications between different safety classes

7.100. Data communications between digital systems and devices of different safety classes should conform with the guidance of paragraphs 6.26 to 6.57. demand for actuation of a protection system function should have priority to actuate the device.

Computer security

7.101. IAEA Nuclear Security Series No. 17, Ref. [32], provides guidance on concerns, requirements, and strategies for implementing computer security programs at nuclear facilities. This section supplements the guidance of Nuclear Security Series No. 17, Ref. [32].

Interaction between safety and security

7.102. SSR 2/1 requirement 8 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 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 Human Machine Interface, they should not adversely affect the operator's ability to maintain the safety of the plant.

7.106. Where practical, 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 security functions to an I&C system increases that system's complexity 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 to section 2 of this guide and qualified to the same level of qualification as the system in which the features reside.

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 I&C system development.

7.111. The development environment for digital systems and the subsequent installation, operation, and maintenance of digital systems should have suitable measures to prevent intentional or unintentional intrusion or corruption of the software or data, the introduction of malicious code, incorrect connection to external networks, or 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 controlled in accordance with paragraph 6.156.

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., 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 impact on system operability.

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 security without interfering with 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 may be transmitted to locations within the plant site (e.g., Technical Support Centre) and to locations beyond the plant site (e.g, Emergency Operations Facility) to support emergency response provided that I&C systems are not adversely affected by these connections.

7.123. Communication links between the plant and the emergency control centre and between the plant and emergency response centres, 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 fundamental safety functions and other information to support emergency management.

Features for operational security

7.125. Active computer security features~~, such as scanning for security vulnerabilities,~~ should be considered for detecting and mitigating computer security threats.

7.126. Active security features for I&C systems should not adversely affect functions that are important to safety.

7.127. Active computer security features might increase system complexity, compete for use of system resources, increase the potential for spurious operation, or introduce new failure modes. Passive 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 ~~safety~~ I&C systems, it is preferable to perform scanning functions off-line.

7.129. Computer systems should include provisions for periodic, and post-maintenance verification that security features are properly configured and are properly operating.

7.130. Procedures for reviewing and acting upon the results produced by computer security monitoring should be established.

Devices configured with hardware description languages (HDL)

7.131. HDL configured devices are programmable electronic modules providing logic structures (e.g. arrays of gates and switches) which are customized by the I&C developer to provide specific functions. Field Programmable Gate Arrays (FPGA) are a common example of devices in this class.

7.132. This customization involves special tools to formally describe the required functions to implement these functions.

7.133. The guidance of this subsection is to be applied in conjunction with the life cycle guidance of section 2, the guidance for digital systems given above and the guidance for software given in section 9. It is applicable to devices that directly implement safety classified functions.

7.134. Development of applications using HDL configured devices should follow a previously defined life cycle that fulfils the recommendations of section 2.

7.135. Development plans should call for the justification of each technical decision in a manner that is understandable by a third party.

7.136. Implementation plan for HDL programmed devices should define the means to ensure that each produced part complies with the design.

7.137. Design requirements for HDL programmed devices should include timing requirements, such as gate delays and setup times.

7.138. The selection HDL of programmable devices and associated items such as libraries, Intellectual Property (IP) cores to be included in the final product, and hardware definition languages, should follow a defined and documented process to ensure their suitability

~~7.140. The use of IP cores in HDL programmed devices should be avoided.~~

7.139. If use of IP cores cannot be avoided:

a. The IP cores used should be obtained from qualified vendors, who followed high quality IP-cores development process, including a rigorous engineering process, well-defined and useful documentation, and ease of integration, and

b. Evaluations should be performed to determine potential 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 the acceptance review.

7.141. If the selected HDL programmed device includes auxiliary features (e.g., built-in self-test), their suitability 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 HDLs with qualified and compatible tools should be selected for programming the HDL programmable devices.

7.143. The design of HDL programed devices should:

a. Ensure that the behaviour of the 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 testabity, and allows for the best use of design and verification tools.

b. Use only ~~HDL~~ HPD 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 HDL language, and use of pre-defined language and coding rules.

c. To the extent feasible, support using verification techniques based on mathematical theorem proving,

d. Explicitly handle all possible cases of logic and all operating modes of the HPD such as reset, power-on and normal operation.

e. Be correct for all possible timing cases resulting from bounding variations in supply voltages, temperature and microelectronic process.

f. Ensure that each function that is implemented in the ~~HDL~~ HPD programmed device is testable.

7.144. Post-route analysis should demonstrate the compliance of the design and implementation with the technology rules defined by the supplier of the design and implementation tools

7.145. The process of integrating the HPD design should be part of the overall system development process.

7.146. Verification should:

a. Confirm that no unspecified function has been programmed ~~Confirm that no hidden circuits exist~~ that will affect the function of the ~~HDL programmed devices~~HPD,

b. Include testing of all signal paths in the ~~HDL programmed device~~HPD,

c. Address the aspects of the system that are particular to ~~HDL programmed devices~~HPD, and

d. Include timing analysis and simulation,

7.147. Environmental qualifications and analyses should demonstrate that the inclusion of pre-developed items or auxiliary features does not degrade the ability of safety systems to perform their safety functions.

SOFTWARE TOOLS

7.148. Tools should be used to support all aspects of the I&C development life cycle where benefits result through their use and where 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 tools can increase the integrity of the I&C development process, and hence component reliability. The use of tools can also have economic benefits as they can reduce the time and human effort required to produce systems, components, and software. Tools can be used to automatically check for adherence to rules of construction and standards, to generate proper records and consistent documentation in standard formats, and to support change control. Tools can also reduce the effort required for testing and can maintain automated logs. Some specific development methodologies require the use of tools.

7.150. Software tools used in the development of I&C systems include, for example:

- Infrastructure tools and development support systems such as requirements management systems or integrated development environments;
- Automated circuit and raceway scheduling software;

- Transformational 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;
- Electronic design automation software;
- Verification and validation tools such as static code analysers, automated circuit testers, test coverage monitors, theorem proving assistants, electronic circuit simulators, and plant system simulators;
- Tools for preparing system configuration data;
- Configuration management and control tools; and
- Security 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 tools are not available, the development of new tools might need to be considered.

7.152. The benefits and risk of using a tool should be balanced against the benefits and risk of not using a tool.

7.153. The important principle is to choose 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 tools in several ways. For example, design tools might introduce faults by producing corrupted outputs, and verification tools might fail to reveal certain faults or types of faults.

7.154. Tools should be selected to remain available throughout the system’s service life and be compatible with other tools used during system development.

7.155. The functionality and limits of applicability of all tools should be identified and documented.

7.156. The tools and their output should not be used outside their declared functionality or limits of application without prior justification.

7.157. For example, tools cannot replace humans when judgment is involved. In some cases, tool support is more appropriate than complete automation of a process.

7.158. Tools should be verified and assessed consistent with the tool reliability requirements, the type of tool, the potential of the tool to introduce fault or fail to make the user aware of existing faults, and the extent to which the 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 include, for example:

- Tools that have the ability to introduce faults need to be verified to a greater degree than tools that are demonstrated to not have that capability;

- Tools that can fail to make the user aware of existing faults need to be verified to a greater degree than tools that do not have that capability;
- Verification is not necessary for tools when the output of the tool is systematically and independently verified;
- Less rigour in tool verification may be accepted if there is mitigation of any potential 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 tools are used.

7.161. The choice, verification and assessment of tools should be justified and documented.

7.162. All tools should be under appropriate configuration management.

7.163. Tool settings used during the development, verification, or validation of baseline equipment, software or HDL configured devices should be recorded in the development records.

7.164. This is useful not only for the final software consistency; it also helps in assessing the origin of a fault, which might lie in the source code, in the tool, or in the tool settings. Information about the tool settings used may be critical to 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 paragraphs 6.79 to 6.135 for devices in this category.

7.166. A device of limited functionality :

- Contains pre-developed software or programmed logic;
- Is autonomous and performs only one conceptually simple principal function, that is defined by the manufacturer and that is not modifiable by the user;
- Is not designed to be reprogrammable; and
- If it is reconfigurable, the configurability is limited to parameters related 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 that:

- Use commercial computers (such as PCs, industrial computers or PLCs),

- Are developed for an I&C platform, or
- Are specifically developed for the nuclear industry.

7.168. Confirmation of the suitability and correctness of industrial digital devices for their intended functions should produce evidence:

a. That the principal functions of the device meet the functional requirements for the application;

b. That neither operation nor failure of functions other than the principle function can result in unsafe operation of the principle 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 the 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;

d. That the development process was systematic and followed the general principles outlined in section 2 of this guide; and

e. That quality assurance for manufacturing is sufficient to provide a basis for accepting the same or similar models of the device which are manufactured at a later time.

7.169. Information developed during safety certification for other industries may be used as evidence to support device qualification. A certificate alone is not sufficient, 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. Compensatory evidence should:

a. Directly address the requirements that it is intended to substantiate, and

b. Be shown to be applicable to the device in question.

7.172. Examples of techniques to provide compensatory evidence include:

- Device specific complementary tests 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 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:

- The 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. HUMAN-MACHINE INTERFACE CONSIDERATIONS

CONTROL ROOMS

Main control room

8.1. SSR 2/1 requirement 65 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 requirement 59 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 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 operator 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 plant and safety status and trends of key plant parameters.

8.6. Safety classified indications and controls should be provided to implement emergency operating procedures (EOP).

8.7. The guidance of paragraph 8.6 is not intended to preclude the option to use other means appropriate to satisfy the goals of the EOP.

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 in status needing 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 alarm system functionality have enabled desirable features to be implemented, such as alarm processing, alarm prioritization and alarm control and management, that help the operator to effectively monitor and respond to plant events.

8.12. The design of the main control room and supplementary control room should be such that no fire, internal hazard, or PIE can prevent the operators from preserving the fundamental safety functions.

Supplementary control room

8.13. SSR 2/1 requirement 66 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 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 to support the response to events which 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 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 Paragraph 6.31 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., main control room and supplementary control room) 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 ‘Accident Monitoring System’ or a ‘Post Accident Monitoring System. These 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 under accident conditions by plant operators, to:

a. Take pre-planned manual actions to bring the plant to a safe state;

b. Determine if the fundamental safety functions are being achieved;

c. Determine the potential for or presence of an actual breach of the barriers to fission product release (e.g., fuel clad, reactor coolant pressure boundary, and containment);

d. Determine the status and performance of plant systems necessary to mitigate a design basis accident and bring the plant to a safe state;

e. Determine the need to initiate action to protect the public from the release of radioactive material; and

f. Implement severe accident management guidelines.

8.23. Instrumentation performing the indication functions given in paragraph 8.22 items a, b, and c should be classified as 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 severe accident monitoring instrumentation for 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 paragraph 6.83.

8.26. Accident monitoring functions that support implementation of severe accident management guidelines should:

a. Not be disabled by the operation, failure, or mal-operation of I&C equipment that is not part of the severe accident instrumentation,

b. Either not depend upon external power, or have a designed capability to be powered from sources other than the plant electrical power system.

8.27. Classification as safety results in the need to fully apply the criteria of Chapter 7, including compliance with the single failure criterion for safety groups.

8.28. Where failure of a single display channel of instrumentation performing the functions given in 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 Safety Parameter Display System) should be provided to assist operators in rapidly determining the status of the plant, confirm operation of accident monitoring channels, validate their readings, and to determine the value of indirectly measured variables from direct measurements.

8.33. Computer guidance may enhance safety and give greater certainty that correct actions are taken.

8.34. In modern control room designs the Safety Parameter Display System (SPDS) and accident monitoring system functions are often integrated into the normal operator HMI. Advice may be

limited to specific operations, or to accident scenarios, or it may cover all operations for 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 paragraph 8.22 items a, b, c, and f.

OPERATOR COMMUNICATIONS SYSTEMS

8.36. SSR 2/1 Requirement 37 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 paragraph 5.66 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 paragraph 5.67 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 with locations internally within the plant and externally without 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 offsite emergency services should not be made ineffective by any personnel protective equipment, 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 needed.

8.43. The main control room, the supplementary control room, and the emergency control centre should have at least two diverse methods for communications with:

a. Areas where communications are needed during AOO or Accident Conditions;

b. Emergency response facilities such as the Technical Support Center, the Operational Support Center and the Emergency Operations Facility. and

c. Associated facilities.

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, standard telephones, battery operated telephones, self-powered telephones, portable radios.

8.45. The diverse communications links identified above should be:

a. Designed such that they will not both be affected by the same failure, internal hazards, external hazards, or PIE, and

b. Capable of operating independently of both the plant power systems and offsite power systems.

8.46. Communications systems should be provided for making announcements that can be heard by all personnel on site and in the plant.

GENERAL HFE PRINCIPLES FOR I&C SYSTEMS

8.47. SSR 2/1 Requirement 32 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 paragraph 5.55 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 paragraph 5.56 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 Human Machine Interface (HMI) design should retain positive features associated with reference designs and avoid problems that have resulted in poor operational experience.

8.51. The design of HMI required for the supervisory control of safety systems should follow 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, diagnose the situation, affect the system (when necessary), and verify manual or automatic actions.

8.53. 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.

8.54. The I&C system design. should ensure that operator tasks can be performed within the time specified by system requirements.

8.55. A satisfactory design will take into account operator cognitive processing capabilities as well as process-related time constraints.

8.56. Information flow rates and control performance that are too fast or too slow could diminish operator performance.

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, monitoring, and protection systems.

8.58. The I&C system should provide simple, comprehensible notification of detectable operator errors, and make available simple, effective methods for recovery.

8.59. No single operator error should result in loss of reactor control, equipment damage, injury, or inadvertent operation of a safety system.

8.60. The HMI should:

a. As far as practical, accommodate the different roles and responsibilities of the many types of operating personnel expected to interact with the systems;

b. Support the development of a common situational awareness of the control room crew, e.g. via large wall mounted plant status displays.

c. Be designed with primary attention given to the role of the operator who is responsible for the safe operation of the equipment;

d. Provide an effective overview of the plant status;

e. As far as practical, ~~Be~~ apply the simplest design consistent with function and task requirements;

f. Be designed to minimize reliance on operator training;

g. Present information such that it can be rapidly recognized and understood by operators;

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.

h. Accommodate failure of video displays without significant interruption of control actions; and

i. Reflect consideration of human physiological characteristics, characteristics of human motor control, and anthropometry.

Human physiological characteristics include, for example, visual/auditory perception and biomechanics (reach and motion).

8.61. The 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 the plant's status and the activities necessary to control the plant.

8.63. The operation and appearance of the HMI should be consistent across information and control locations and platforms and 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.

8.65. All aspects of the I&C system (including control arrangements and displays) should be consistent with the operators' mental models and established conventions.

8.66. Mental models incorporate the operator's understanding and expectations about how the system behaves. These 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.

Considerations for human-automation interaction

8.68. The methodology for determining 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;
- Accuracy 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 paragraph 5.59 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 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, but sufficient to maintain vigilance.

8.77. The I&C should have all characteristics that have been identified as necessary by the Task Analysis.

8.78. A complete task analysis will consider all plant states, all plant operating modes and all operating personnel, e.g., licensed operators, unlicensed operators, maintainers. Task analysis will provide design input into characteristics of I&C such as accuracy, precision, time response, physical layout, type of controls and displays and control association with information displays.

8.79. The HMI should permit displays and controls on video display units to be formatted in a configuration most convenient for the task where this offers advantages in task 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 different operating modes.

8.81. All aspects of the HMI (formats, terminology, sequencing, grouping, and operator's decision-support aids) 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 HMI should present information to operators in forms and formats that are consistent with the results of the Task Analysis.

8.84. The I&C should provide control options that cover the range of potential operator actions identified by the Task Analysis.

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 work environment

8.87. SSR 2/1 paragraph 5.61 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 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, for example, include radiation, smoke and toxic substances in the atmosphere.

8.91. SSR 2/1 paragraph 5.60 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 HMI stations are distributed, operating personnel should have means to access these different locations in a safe and timely manner.

8.93. Examples of distributed HMI stations include the supplementary control room and other field locations where actions are expected to occur.

8.94. One way of establishing suitable means of access is to provide a qualified route with provisions to protect against potential internal or external hazards to supplementary control points and other field locations where operator actions are expected to occur.

RECORDING OF HISTORICAL DATA

8.95. The 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 of 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 implementation tends to be complex and prone to design errors. Complexity in software implementation 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 design, 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 in section 2 is particularly relevant to software since the activities covered are integral to effective software development.

9.4. SSR-2/1 requirement 63 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 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 defined life cycle, be duly planned and documented and include thorough verification and validation. (See section 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 this section.

9.7. Software requirements should be established using a predetermined combination of techniques commensurate with the system’s importance to safety.

9.8. Techniques for establishing requirements might, 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 as described in section 3.

9.10. Understanding of the system design basis is needed to ensure that software requirements properly implement essential system properties. Relevant issues include:

- Potential failure conditions,
- Operation modes,
- Safety monitoring,
- 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. Software Requirements Specifications should:

a. Define what each individual software item is required to do and how it will interact with other components of the system.

b. Originate from the relevant processes of the I&C life cycle (including consideration of system hazards identified in previous analyses) and from processes that interface with the I&C life cycle, e.g., human factors engineering and computer security activities. See Fig. 2.

c. Be written as far as possible in terms of what needs to be achieved rather than how they are to be designed and implemented.

d. Be complete, unambiguous, consistent, readable, understandable to their target audience (e.g., domain experts, safety engineers, software designers), verifiable and traceable.

e. Address as appropriate the System Requirements allocated to software.

f. Specify as necessary minimum precision, numerical accuracy, a description of the interfaces, independence of execution threads, self-supervision, timing performance and security.

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. Include the necessary level of reliability and availability to be achieved.

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).

h. Allow for the capabilities of the computers, tools and similar existing systems to ensure that the software requirements are feasible.

i. Refer to, include, or be complemented by additional information applicable to its target audience, e.g., background 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 target audience.

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, 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, 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.

9.18. Techniques 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. Design elements should be identified to a level sufficient to facilitate traceability.

9.21. The design of safety system software 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 paragraph 9.21 applies only to safety system simplicity is a worthwhile goal for software of lower safety classification. For systems of lower safety classification 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 paragraphs 7.79 to 7.94.

9.35. As the design is refined; the need for additional fault detection and self-supervision features should be considered and included in the software design. See paragraphs 6.167 to 6.173.

9.36. On 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 implementation constraints that need to be observed during the design phase.

9.38. Such implementation constraints may include any need to ensure diversity, and particular attributes of the programming languages, compilers, subroutine libraries and other supporting tools.

9.39. These 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 implementation constraints on a proprietary system to be traceable to the supplier's standard documentation.

9.41. The software design architecture should account for constraints on modules and interfaces that might result from the decision to use 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.

SOFTWARE IMPLEMENTATION

9.43. The software implementation should:

a. Be 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. Be established using a predetermined combination of techniques commensurate with the system's importance to safety, covering languages, tools, coding practices, analysis, review and testing.

c. Demonstrably address all software requirements and the software design.

d. Be simple and readily understandable, with readability and maintainability taking precedence over ease of programming.

e. Include readable forms of the source and executable code, the results of unit and module interface tests, and sufficient contextual information to verify the code's correctness 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 the testing guidance of this Safety Guide to be met.

9.46. Coding rules should be prescribed before coding commences and their adherence 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 functionality and integrity requirements of 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.

9.54. 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 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 implementation tools should be selected with the aim of minimizing error. See 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 or methods, may be considered as a means of reducing the likelihood and effect of software common cause failures. However, this can introduce design constraints that could themselves lead to new failures. ~~There are many different sources of potential coincident software failures and statistical independence cannot always be assumed; this would need to be accounted for in any claim for the reliability achieved~~.

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 teams should be trained on secure development techniques.

SOFTWARE VERIFICATION AND ANALYSIS

9.63. Software requirements, design and implementation should be verified against the I&C system requirements specification.

9.64. Verification of traceability should be an on-going activity to ensure shortfalls are addressed as early as possible and hence necessary changes remain practicable.

9.65. The results of each 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 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;

h. The functionality of any verification tool, including expectations and limitations on how it is to be used (e.g., domain, language, process); and

i. The rationale for the above and justification that this is sufficient for software of the safety classification 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. Static analysis includes techniques such as verification of compliance with design, coding, and standards constraints, 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 dependability.

9.72. Relevant operating experience can supplement, but cannot replace other verification techniques.

9.73. See paragraphs 7.148 to 7.164 for guidance relevant to the use of tools for software verification and analysis.

9.74. A test strategy (e.g., bottom-up or top-down) should be determined for verification of the software implementation.

9.75. The test case specifications should ensure adequate testing of:

a. Interfaces (such as module-module, software-hardware, system boundary),

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. [5] provides guidance for ensuring suitability of measuring and test equipment used for testing.

9.79. The test case specifications and effectiveness 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 groups that are independent of the designers and developers.

9.81.The code should be reviewed to check for software security vulnerabilities, using automated tools and complemented by manual review of the critical sections of the code (I/O handling, exception handling)

9.82 All 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 coverage achieved) should be resolved or justified.

9.84. Detected errors should be analysed for cause and corrected under the control 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 systems.

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. [5] paragraphs 6.50 to 6.77 and GS-G-3.5, Ref. [6] 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 are complete, correct, and consistent.

9.88. The verification results, including test records, should be documented, maintained and be 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 and indicate which results failed to meet expectations and how these were resolved.

9.91. Test 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 (such as pen 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.

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, Pre-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 paragraphs 2.109 to 2.118.

9.97. For systems important to safety that are not safety systems, the pre-developed software should have user documentation that describes:

a. The functions provided,

b. The interfaces, including the roles, types, formats, ranges and constraints 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, and

f. A justification that the functions are suitable for the I&C system.

SOFTWARE TOOLS

9.98. Recommendations for software tools are given in 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 third party assessment is to provide a view on the adequacy of the system and its software that is independent of both the supplier and the operating organization. Such an assessment may be undertaken by the regulator or by a body acceptable to the regulator.

9.101. It is important that proper arrangements are made with the software originator to permit third party assessment.

9.102. The assessment should involve an examination of:

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).

[4] International Atomic Energy Agency, The Management System for Facilities and Activities, Safety Requirements No. GS-R-3, IAEA, Vienna (2006).

[5] International Atomic Energy Agency Safety Guide, Application for the Management System for Facilities and Activities, Safety Guides Series No. GS-G-3.1, IAEA, Vienna (2006).

[6] International Atomic Energy Agency, The Management System for Nuclear Installations, Safety Guide Safety Guide GS-G-3.5, IAEA, Vienna (2009).

[7] International Atomic Energy Agency, Safety Assessment for Facilities and Activities, General Safety Requirements No. GS-R-4, IAEA, Vienna (2009).

[8] International Atomic Energy Agency, Safety Glossary, IAEA, Vienna (2007).

[9] International Atomic Energy Agency, Design of Electric Power Systems of Nuclear Power Plants, Safety Guide Series DS-430, IAEA, Vienna (Draft August 2011).

[10] International Atomic Energy Agency, Modifications to Nuclear Power Plants, Safety Guide Series No. NS-G-2.3, IAEA, Vienna (2000).

[11] International Atomic Energy Agency, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (1999).

[12] International Atomic Energy Agency, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants: A Reference Book, NP-T-3.12, IAEA, Vienna, (2012).

[13] International Atomic Energy Agency, Computer Security at Nuclear Facilities, Nuclear Security Series No. 17, IAEA, Vienna (2011).

[14] International Atomic Energy Agency, Development and Application of Level 1 Probabilistic Safety Assessment for Power Plants, Safety Guide Series No. SSG-3, IAEA, Vienna (2010).

[15] International Atomic Energy Agency, Development and Application of Level 2 Probabilistic Safety Assessment for Power Plants, Safety Guide Series No. SSG-4, IAEA, Vienna (2010).

[16] International Atomic Energy Agency, Deterministic Safety Analysis for Nuclear Power Plants, Safety Guide Series No. SSG-2, IAEA, Vienna (2009).

[17] International Atomic Energy Agency, Commissioning for Nuclear Power Plants, Safety Guide Series No. NS-G-2.9, IAEA, Vienna (2003).

[18] International Atomic Energy Agency, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, Safety Guide Series No. NS-G-2.6, IAEA, Vienna (2001).

[19] International Nuclear Safety Group, Defence in Depth in Nuclear Safety, INSAG Report 10, IAEA, Vienna (1996).

[20] International Nuclear Safety Group, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1, INSAG Report 12, IAEA, Vienna

[21] International Atomic Energy Agency, Classification of Structures, Systems and Components in Nuclear Power Plants, Safety Guide DS 367, IAEA, Vienna (2013).

[22] International Atomic Energy Agency, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, Safety Guide Series No. NS-G-1.7, IAEA, Vienna (2004).

[23] International Atomic Energy Agency, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, Safety Guide Series No. NS-G-1.11, IAEA, Vienna (2004).

[24] International Atomic Energy Agency, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Reports Series No. 3, Vienna (1998).

[25] International Atomic Energy Agency, Seismic Design and Qualification for Nuclear Power Plants, Safety Guide Series No. NS-G-1.6, IAEA, Vienna (2003).

[26] International Atomic Energy Agency, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Guide Series No. NS-G-1.5, IAEA, Vienna (2003).

[27] International Atomic Energy Agency, Ageing Management for Nuclear Power Plants, Safety Guide Series No. NS-G-2.12, IAEA, Vienna (2009).

[28] International Atomic Energy Agency, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, Nuclear Security Series No. 4, IAEA, Vienna (2007).

[29] International Atomic Energy Agency, Preventive and Protective Measures against Insider Threats, Nuclear Security Series No. 8, IAEA, Vienna (2008).

[30] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), Nuclear Security Series No. 13, IAEA, Vienna (2007).

[31] International Atomic Energy Agency, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Safety Guide Series No. NS-G-2.2, IAEA, Vienna (2000).

[32] International Atomic Energy Agency, The Operating Organization for Nuclear Power Plants, Safety Guide Series No. NS-G-2.4, IAEA, Vienna (2002).

[33] International Atomic Energy Agency, Conduct of Operations at Nuclear Power Plants, Safety Guide Series No. NS-G-2.14, IAEA, Vienna (2008).

[34] International Atomic Energy Agency, Radiation Protection Aspects of Design for Nuclear Power Plants, Safety Guide Series No. NS-G-1.13, IAEA, Vienna (2005).

ANNEX I. BIBLIOGRAPHY OF INTERNATIONAL I&C STANDARDS

I-1. SSR 2/1 requirement 9 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 safety guide gives high-level recommendations that are widely accepted among the IAEA member states. Beyond 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 2/1. It is expected that designers, users, and regulators 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 nuclear power plant 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 2/1 and the recommendations of this guide. Consequently, either set of standards can be used to further interpret the recommendations of this guide.

I-4. This annex is intended to help readers understand the relationship between this 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 guide. Table I-1 is not a complete list of either set of standards, but it identifies the entry points into the IEC and IEEE standards sets.

I-5. Table I-2 shows how these entry standards relate to the major topic areas of this guide.

I-4. A concerted effort was made to avoid conflicts between the recommendations of this guide and the standards of IEEE and IEC. Members of both standards committees participated in the development of this guide and both standards organizations reviewed drafts to help identify and eliminate conflicts.

I-5. Users should nevertheless, recognize and account for the fact that there are important differences between the IEC and the IEEE standards.

I-6. IEC standards take the IAEA requirements and safety guides as fundamental inputs for the development of their standards. As a result, the IEC standards deal with items important to safety and take the IAEA I&C safety guide as the source of general recommendations.

I-7. IEEE standards focus largely on safety items, therefore, their guidance directly applies to a smaller set of functions, systems and equipment than this guide. Nevertheless, the guidance of IEEE can be applied to safety related items (items important to safety but not safety system items) using a graded approach.

I-8. IEEE standards do not take this guide as a reference. IEEE 603 is the equivalent of this guide in the IEEE framework of standards. Nevertheless, this 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 'IE' 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. [9], 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 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
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-431	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 and equipment	IEC 61226
6. General recommendations for all I&C systems important to safety	
- General	IEC 61513, IEC 60709, IEEE 379, IEEE 384
- Design for reliability	

DS-431	Internationally Used I&C Standards
- Equipment qualification - Design to cope with ageing	IEC 60780,IEC 980, IEC 62342, IEEE 344, IEEE 323, IEC 2003
- 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
- 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

DS-431	Internationally Used I&C Standards
- Accident monitoring	IEEE 497
- Operator communications systems	
- General HFE principles 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, ISO/IEC 12207

ANNEX II. CORRELATION BETWEEN THIS 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 safety guides, NS-G-1.1 and NS-G-1.3, are located in this guide.

Table II.1 Correspondence Between NS-G-1.1 and D-431

NS-G-1.1	DS-431
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
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

NS-G-1.1	DS-431
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

NS-G 1.3	DS-431
1. Introduction	1. Introduction
2. Instrumentation and control systems important to safety	See NS-T-3.12, Ref. [9]
- 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	
- 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)

NS-G 1.3	DS-431
- 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)
- 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

NS-G 1.3	DS-431
	important to safety (Maintainability)
- Documentation	2. Management systems for I&C design (Activities common to all life-cycle phases - 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)

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 I&C safety design criteria are not widely accepted by all member states. This annex discusses areas where such differences were identified during the development of this Safety Guide. It may be expected that the practices of member states will evolve over time.

RELIABILITY DETERMINIATION 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 ~~both~~ 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 member states, 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 members states consider numerical estimates of digital system reliability to be a necessary element of reliability demonstration.

III-4. For the Member States who apply numerical reliability to software, ~~Claims~~ claims of high software reliability are not demonstrable at the present time. Hence, designs requiring 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 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 of technology, 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 of the extent to which the strategies described in section 7 (e.g., redundancy) are employed.

III-6. ~~Some member states use a qualitative approach for determining SW reliability.~~ Some member states use a qualitative approach for determining SW reliability. Such qualitative approach is typically based on strong requirements on the deterministic behaviour of the software to allow a full verification and validation. Such combination of strong design requirements that allow full V&V gives a high confidence in the reliability of the software.

III-7. Paragraph 4.32 recommends that an analysis should be done of the consequences of each PIE in combination with 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 PIE together with a 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 expect for the analysis described in paragraph 4.32 include the following examples.

- Analysis of safety system CCF in conjunction with PIE that are considered to be Anticipated Operational Occurrences and Design Basis Accident conditions.
- Analysis of safety system CCF in conjunction with PIE with an occurrence frequency greater than 10^{-3} per year.

Accepted consequences

III-9. Examples of the consequences that regulatory authorities may accept in the event that a PIE occurs in conjunction with a common cause failure of safety systems include:

- 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 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 primary coolant system or containment design limits.
- Following a design basis accident occurring in conjunction with a common cause failure a reactor protection system the remaining safety systems are to be capable of:
  - Dose limits agreed between the regulator and the licensee,
  - 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 common cause failure ensure a sufficiently high reliability of system function.
- The consequences of a DBA do not exceed acceptable dose limits if a safety system fails.

Analytical approaches

III-10. In making consequence determinations as part of the analysis described in paragraph 4.32, some regulatory authorities expect the use of conservative methods; others allow the use of best estimate methods. NS-G-1.2, Ref. [10] discusses conservative, and best estimate analysis methods.

DIVERSE ACTUATION SYSTEMS

III-11. When digital systems are used to implement Protection System functions it is not uncommon for the analysis described in paragraph 4.32 to find that common cause failures within the digital protection system might result in unacceptable consequences for certain combinations of CCF and PIEs. When this situation is encountered a Diverse Actuation System is often provided to backup the Protection System.

III-12. There is general agreement that Diverse Actuation Systems may effectively mitigate the consequences of specific PIEs in conjunction with postulated CCF of a Protection System. There are, however, different approaches to the safety classification, the use of digital Diverse Actuation Systems to back up digital Protection System, and use of manual actuation to mitigate the consequences of Protection System CCF.

Safety classification

III-13. Some regulatory authorities expect that Diverse Actuation Systems will be classified as safety systems. Some regulatory authorities allow them to be systems of lower safety classification. Some regulatory authorities base the expected level of safety classification upon the reliability claims made for the Diverse Actuation System.

Diverse Actuation System technology

III-14. Some regulatory authorities expect that Diverse Actuation Systems will be hardwired systems. Some regulatory authorities discourage, but do not prohibit, the use of digital systems. Some regulatory authorities 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 but the conditions under which manual actuation may be credited vary. The range of accepted practices include:

- 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 engineered safety feature 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, a regulator may take a different approach based upon the specific situation proposed.

LIST OF DEFINITIONS

(The following definitions are not given or are different from those given in the IAEA Safety Glossary [7].*

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 that the required 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 event or cause.

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 specification 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.

diversity.* Presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure.

NOTE 1 - When “Diversity” is used with an additional attribute, the term diversity indicates the general meaning “Existence of two or more different ways or means of achieving a specified objective”, where the attribute indicates the characteristics of the different ways applied, e.g. functional diversity, equipment diversity, signal diversity.

NOTE 2 - See also “functional diversity”

division. The collection of items, including their interconnections, that form one redundancy of a redundant system or safety group. Divisions may include multiple channels.

failure.* Loss of the ability of a structure, system or component to function within acceptance criteria

NOTE 1 - 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). Integrated circuit that can be programmed in the field by the I&C manufacturer. It includes programmable logic blocks (combinatorial and sequential), programmable interconnections between them and programmable blocks for input and/or outputs. The function is then defined by the I&C designer, not by the 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). HDL-Programmed Device can be an integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and related software tools.

hazard analysis. A process that explores and identifies conditions that are not identified by the normal design review and testing process.

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

human-machine interface (HMI). The interface between operating staff and I & C system and computer systems linked with the plant. The interface includes displays, controls, and the Operator Support System interface.

non-functional requirements. Requirements that specify required characteristics of an item, other than the required functions and behaviours. Characteristics specified in non-functional requirements include, for example, auditability, availability, compatibility, documentation, integrity, maintainability, reliability, and usability.

pre-developed block. pre-developed functional block usable in a HDL description. Pre-developed blocks might be, for example, libraries, macros, or Intellectual Property cores. A pre-

developed block may need significant work before incorporation in a HDL programmed device.

pre-developed item. Item which 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 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. an engineering process, which includes the activities involved in discovering, 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: analysis 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 as intended (functionality, response time, fault tolerance, robustness).

type test. Conformity test made on one or more items representative of the production.

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

CONTRIBUTORS TO DRAFTING AND REVIEW

Alpeev, A	Scientific-Technical Center on Nuclear and Radiation Safety	Russia
Alvarado, R.	US Nuclear Regulatory Commission	USA
Asikainen, S.	Teollisuuden Voima Oyj	Finland
Babcock, B.	Ontario Power Generation	Canada
Benitez-Read, J.	National Nuclear Research Institute of Mexico	Mexico
Bicer, C.	Turkish Atomic Energy Authority	Turkey
Boeva, T.	Kozloduy NPP	Bulgaria
Bouard, J-P,	EDF	France
Bowell, M.	Office of Nuclear Regulation	United Kingdom
Curtis, D.	Private Consultant	United Kingdom
Debor, J.	Private Consultant	USA
Duchac. A	IAEA	
Edvinsson, H.	Vattenfall	Sweden
Eriksson, K-E.	Oskarshamn NPP	Sweden
Faya, A.	FANR	UAE
Fichman, R.	Ontario Power Generation	Canada
Furieri, E-B.	Comissao Nacional de Energia Nuclear	Brazil
Gassino, J.	IRSN	France
Gonchukov, V.	Rostechnadzor	Russia
Göring, M.	Vattenfall	Germany
Harber, J.	AECL	Canada
Hohendorf, R.	Ontario Power Generation	Canada
Johnson, G.	IAEA	
Karasek, A.	CEZ	Czech Republic
Kawaguchi, K.	Japan Nuclear Energy Safety Organization	Japan
Kim, B-Y.	Korea Institute of Nuclear Safety	ROK
Klopkov V.	Rostechnadzor	Russia
Lee, J-S.	Korea Atomic Energy Research Institute	ROK

Li, H.	US Nuclear Regulatory Commission	USA
Lindskog, U.	Oskarshamn NPP	Sweden
Mangi, A.	Pakistan Nuclear Regulatory Authrority	Pakistan
Ngo, C.	Candesco	Canada
Odess-Gillett, W.	Westinghouse	USA
Park, H-S.	Korea Institute of Nuclear Safety	ROK
Parsons, A.	AMEC	United Kingdom
Poulat, B.	IAEA	
Piljugin, E.	GRS	Germany
Régnier, P.	IRSN	France
Santos, D.	US Nuclear Regulatory Commission	USA
Seidel, F.	Federal Office for Radiation Protection	Germany
Shumov, S.	SNIIP	Russia
Stattel, R.	US Nuclear Regulatory Commission	USA
Sjövall, H.	Teollisuuden Voima Oyj	Finland
Svensson, C.	Oskarshamn NPP	Sweden
Takala, H.	STUK	Finland
Takita, M.	Japan Nuclear Energy Safety Organization	Japan
Tate, R.	Office of Nuclear Regulation	United Kingdom
Thuy, N.	EDF	France
Welbourne, D.	Private Consultant	United Kingdom
Yastrebenetsky, M.	SSTC	Ukraine
Yates, R.	Office of Nuclear Regulation	United Kingdom
Zeng, Z-C.	Canadian Nuclear Safety Commission	Canada