Date: 2019-12-20

IAEA SAFETY STANDARDS

for protecting people and the environment

Step 8
For submission to MS for comments

Instrumentation and Control Systems and Software Important to Safety for Research Reactors

DS509H

DRAFT SAFETY GUIDE

A revision of Safety Guide SSG-37

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Requirements for the safety of research reactors, with particular emphasis on their design and operation, are established in IAEA Safety Standards Series No. SSR-3, Safety of Research Reactors [1].

1.2. This Safety Guide provides recommendations on design and operation of instrumentation and control systems for research reactors.

1.3. This Safety Guide was developed in parallel with seven other Safety Guides on the safety of research reactors, as follows:

- IAEA Safety Standards Series No. DS509A, Commissioning of Research Reactors [2];
- IAEA Safety Standards Series No. DS509B, Maintenance, Periodic Testing and Inspection of Research Reactors [3];
- IAEA Safety Standards Series No. DS509C, Core Management and Fuel Handling for Research Reactors [4];
- IAEA Safety Standards Series No. DS509D, Operational Limits and Conditions and Operating Procedures for Research Reactors [5];
- IAEA Safety Standards Series No. DS509E, The Operating Organization and the Recruitment, Training and Qualification of Personnel for Research Reactors [6];
- IAEA Safety Standards Series No. DS509F, Radiation Protection and Radioactive Waste Management in the Design and Operation of Research Reactors [7];
- IAEA Safety Standards Series No. DS509G, Ageing Management for Research Reactors [8];

1.4. Additional recommendations on the safety of research reactors are provided in IAEA Safety Standards Series Nos SSG-20, Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report [9] and SSG-24, Safety in the Utilization and Modification of Research Reactors [10].

1.5. The terms used in this Safety Guide are to be understood as defined and explained in the IAEA Safety Glossary [11].

1.6. This Safety Guide supersedes IAEA Safety Standards Series No. SSG-37, Instrumentation and Control Systems and Software Important to Safety for Research Reactors[1].

OBJECTIVE

1.7. The objective of this Safety Guide is to provide recommendations on instrumentation and control systems and software important to safety for research reactors, including instrumentation and

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems and Software Important to Safety for Research Reactors, IAEA Safety Standards Series No. SSG-37, IAEA, Vienna (2015).

control system architecture and associated components, from sensors to actuators, operator interfaces and auxiliary equipment, to meet the relevant requirements of SSR-3 [1].

1.8. The recommendations provided in this Safety Guide are aimed at operating organizations of research reactors, regulatory bodies and other organizations involved in a research reactor project, including suppliers of instrumentation and control systems.

SCOPE

1.9. This Safety Guide is primarily intended for use for heterogeneous, thermal spectrum research reactors having a power rating of up to several tens of megawatts. Research reactors of higher power, specialized reactors (e.g. homogeneous reactors, fast spectrum reactors) and reactors having specialized facilities (e.g. hot or cold neutron sources, high pressure and high temperature loops) may need additional guidance. For such research reactors, the recommendations provided in IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [12] might be more suitable.

1.10. Research reactors with a low hazard potential having a power rating of up to several tens of kilowatts and critical assemblies and subcritical assemblies might need a less comprehensive commissioning programme than that outlined here. While all recommendations in this Safety Guide are to be considered, some might not be applicable to these research reactors with low hazard potential and subcritical assemblies (see paras 2.15 – 2.17 and Requirement 12 of SSR-3 [1], and IAEA Safety Standards Series No. SSG-22, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors [13]).

1.11. In this Safety Guide, subcritical assemblies will be mentioned separately only if a specific recommendation is not relevant for, or is applicable only to, subcritical assemblies.

1.12. The recommendations and guidance apply to both the design and configuration management of instrumentation and control systems for new research reactors and the modernization of the instrumentation and control systems of existing research reactor facilities.

1.13. This Safety Guide provides recommendations and guidance on human factors engineering and human–machine interfaces for hardware, and for computer based systems and software for use in instrumentation and control systems important to safety.

STRUCTURE

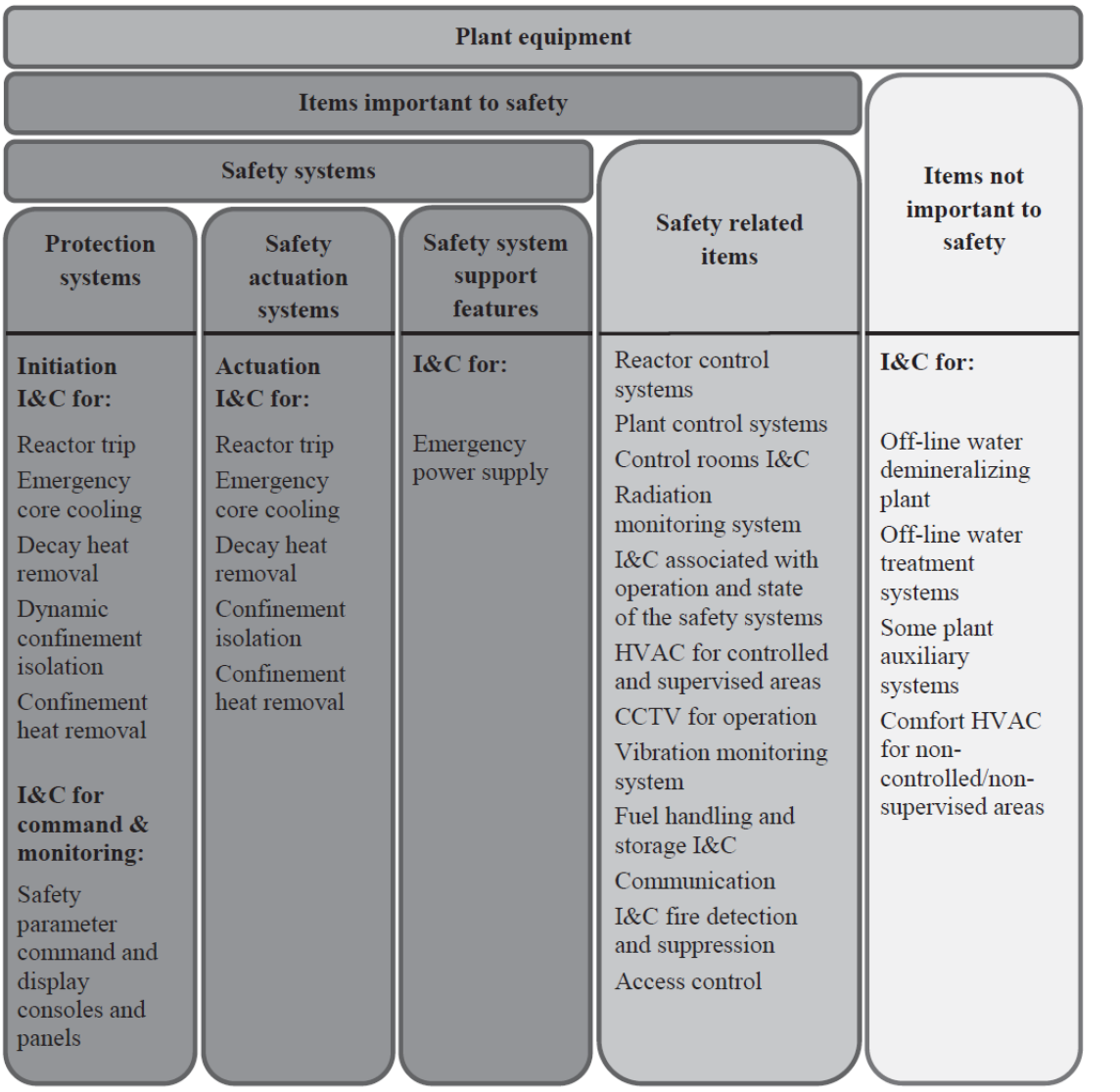
1.14. Section 2 discusses the identification of instrumentation and control functions and systems, the method and the basis for safety classification into safety functions and systems and safety related functions and systems. Section 3 gives guidance on how instrumentation and control systems are to be arranged into a hierarchy. Sections 4 and 5 provide an overview on meeting the general and specific design requirements for instrumentation and control systems. The operational aspects of instrumentation and control systems are presented in Section 6. Section 7 expands on the guidance given in Section 4 in

the area of human–machine interfaces. Section 8 provides guidance on design aspects and other aspects of computer based systems and software. Section 9 provides guidance on configuration management for instrumentation and control systems. Section 10 presents considerations in the modification and modernization of instrumentation and control systems. The Annex identifies instrumentation and control systems that can be used in a research reactor.

2. SAFETY CLASSIFICATION OF INSTRUMENTATION AND CONTROL SYSTEMS

GENERAL CONSIDERATIONS

2.1. Instrumentation and control functions, systems and components may be classified into two categories: items important to safety and items not important to safety (see Fig. 1 and the Annex). Functions, systems and components important to safety are those which ~~permit the safe operation of the facility research reactor and contribute toperform the following main safety functions~~contribute to:



~~**Note:** CCTV — closed circuit television; HVAC — heating, ventilation and air-conditioning; I&C — instrumentation and control.~~

~~*FIG. 1. Examples of instrumentation and control systems of a research reactor classified according to their importance to safety.*~~

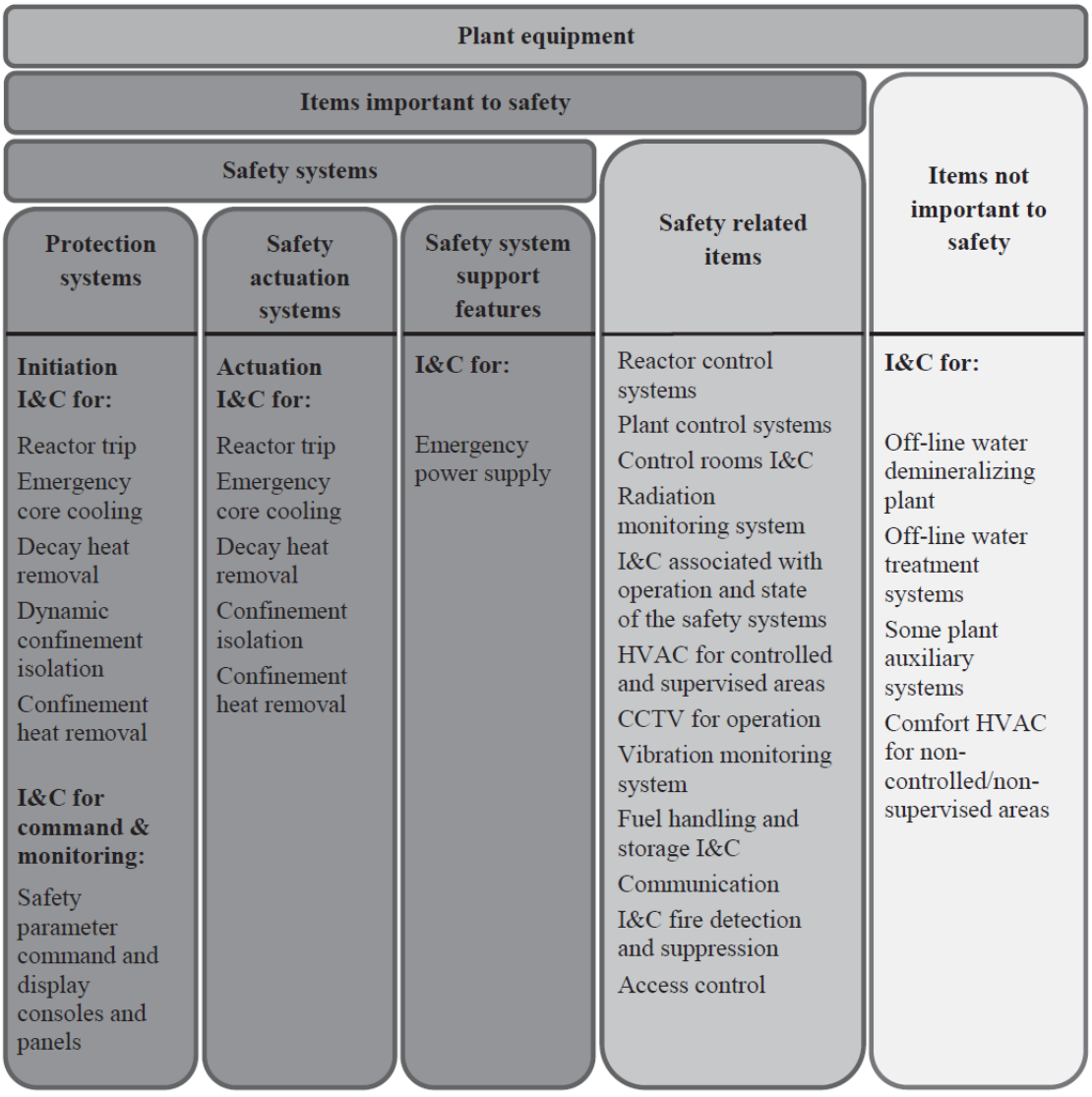
(a) ~~Control of reactivity~~Safely ~~shutting down the reactor and maintaining it in a safe shutdown condition in and after operational states and accident conditions;~~ Safely shutting down the reactor and maintaining it in a safe shutdown condition in and after operational states and accident conditions;

~~(a)~~(b) ~~Removing Removal of residual~~ Removing residual heat from the reactor core after shutdown, in all operational states and accident conditions. ~~core after shutdown, and from fuel storagein all operational states and accident conditions~~;

(c) ~~Confinement of the radioactive material, shielding against radiation and control of planned~~Preventing, ~~or reducing the potential for, radioactive~~ Preventing, or reducing the potential for, releases ~~of radioactive material and ensuring that any releases are within authorized limits in all operational states and within acceptable limits in and after accident~~ of radioactive material and ensuring that any releases are within authorized limits in all operational states and within acceptable limits in and after accidents~~as well as limitation of accidental radioactive releases~~;

(d) Assuring the safe operation of the reactor.

~~(d) Permitting the safe operation of the reactor.~~



Note: CCTV — closed circuit television; HVAC — heating, ventilation and air-conditioning; I&C — instrumentation and control.

FIG. 1. Examples of instrumentation and control systems of a research reactor classified according to their importance to safety.

~~(b)~~

2.2. Instrumentation and control systems not important to safety are those used to accomplish functions supporting the operation of the facility, while having no impact on the safety of the reactor.

2.3. Systems and components important to safety are further categorized into either safety systems or safety related systems:

(a) Safety systems consist of the protection system, the safety actuation systems and the safety system support features.

(b) Safety related systems are systems important to safety that are not part of a safety system, such as systems for monitoring the availability of safety systems.

2.4. For instrumentation and control systems important to safety, a graded approach to the application of the requirements of ~~NS-R-4~~SSR-3 [1] may be used, but the extent of grading should be clearly justified in the safety analysis report (the factors to be considered can be found in para. ~~1.14~~2.17 of ~~NS-R-4~~SSR-3 [1]). Additional recommendations and guidance on the application of the graded approach are provided in IAEA Safety Standards Series No. SSG-22, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors [13~~2~~].

METHODS OF CLASSIFICATION

2.5. Requirement 16, para. 6.29 of SSR-3 [1] states, "The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods (if available), with due account taken of factors such as~~The method for classifying the safety significance of a structure, system or component should be based primarily on deterministic methods, complemented by engineering judgement and where appropriate by probabilistic methods, if available. For instrumentation and control systems, the basis for such a classification should consider~~:

(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;

~~(a)~~(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.

~~The safety function(s) to be performed by the instrumentation and control system.~~

~~The consequences of failure of the instrumentation and control system (failure or faulty performance of the function(s)). This includes the potential for the instrumentation and control system itself (i.e. the fail-safe modes of instrumentation and control systems) to cause an initiating event and the combination of the probability and consequences of such an initiating event (i.e. frequency of failure and the possible radiological consequences).~~

~~The estimated frequency or probability (if available) that the instrumentation and control system will be called upon to perform a safety function.~~

2.5. a. An I&C system where a spurious failure, or failure on demand, may cause an initiating event or make the consequences of a postulated initiating event worse, should be classified to a higher safety class. A similar approach should be applied to the I&C associated with reactivity control systems whose failure may lead to accident conditions. ~~With respect to the consequences of failure to perform a safety function, an I&C system whose failure or spurious operation may directly cause an initiating event, or that its failure on demand may make the consequences of a postulated initiating event worse, can be classified to a high safety class. This includes the I&C associated with reactivity control systems whose failure would result in accident conditions.~~ ~~Following a postulated initiating event, the time at which or the period for which the instrumentation and control system will be called upon to operate.~~

2.5.b. Instrumentation and control functions for all ~~facility~~ states of the research reactor should be identified. The instrumentation and control functions necessary to mitigate the consequences of design extension conditions could be assigned to a lower safety class than the functions necessary to control anticipated operational occurrences and design basis accident conditions to reach a controlled state of the research reactor.

DESIGN, CONSTRUCTION, COMMISSIONING, OPERATION AND MAINTENANCE OF INSTRUMENTATION AND CONTROL SYSTEMS

2.6. All instrumentation and control systems and equipment should be designed, constructed, commissioned, operated and maintained in such a manner that their specification, their verification and validation process, and their quality and reliability are commensurate with their safety classification. The specifications should consider sufficient margins for their safety system design. These margins should be verified at both component level and system level by testing and analysis.

2.7. All instrumentation and control systems and equipment performing functions important to safety should have appropriately designed interfaces with systems and equipment of different safety classes in order to ensure (e.g. by using isolation devices) that any failure in a system classified in a lower safety class (with less stringent requirements) will not propagate to a system classified in a higher safety class. Equipment that fulfils the function to prevent such a propagation of failure should be treated as being in the higher class.

2.8. The safety class of an instrumentation and control system should be the same as the highest safety class of the systems or equipment that it controls or monitors.

3. OVERALL INSTRUMENTATION AND CONTROL SYSTEM ARCHITECTURE

GENERAL

3.1. The research reactor should be provided with sufficient instrumentation and control systems for ensuring the safety of the facility in normal operation, including startup, operation at power, shutting down, refuelling and maintenance, and in accident conditions. In particular, the instrumentation and control systems should be able to automatically initiate reactor shutdown, emergency core cooling,

residual heat removal and the confinement of radioactive material, although manual operation action may be permitted as described in para. 5.14. The instrumentation and control system architecture should provide sufficient capabilities to cover all anticipated operational occurrences and post-event conditions.

3.2. The instrumentation and control system architecture ~~has to~~is required to fulfil the safety objectives and design requirements established in section 2, requirements 49–55, and paras 6.44, 6.55, 6.85, 6.94, 6.106, 6.154, and 6.159 ~~paras 2.2–2.7, 6.1–6.43, 6.61–6.65, 6.94–6.105 and 6.136–6.144~~ of ~~NS-R-4~~SSR-3 [1]. The instrumentation and control system architecture should support all the instrumentation and control functions necessary to ensure the safety of the facility.

3.3. The instrumentation and control system architecture provides high level definition of the instrumentation and control systems, the assignment of instrumentation and control functions to these systems, and the communications (interfaces) between instrumentation and control systems and the facility operators and users. ~~Modern instrumentation and control systems are more highly integrated than in the past.~~ The architecture of highly integrated systems should be carefully considered to ensure proper implementation of the defence in depth concept. A good architectural design is characterized by a rational allocation of functions, only in the systems where they are needed. The identification of the different and individual instrumentation and control systems that can be included in a particular research reactor facility depends on the type of reactor, its purpose and its operation modes. These different instrumentation and control systems are described in the Annex.

DEFENCE IN DEPTH

3.4. As stated in para. 2.11~~5~~ of ~~NS-R-4~~SSR-3 [1]:

> "Application of the concept of defence in depth throughout design and operation provides ~~a graded~~ protection against ~~a wide variety of transients,~~ anticipated operational occurrences and accidents, including those resulting from equipment failure or inappropriate human actions within the installation~~,~~ and events ~~that originate outside the installation~~induced by external hazards."

3.5. Requirement 10 of SSR-3. [1] states, "The design of a research reactor shall apply the concept of defence in depth. The levels of defence in depth shall be independent as far as is practicable". ~~The design of the instrumentation and control system should incorporate the defence in depth concept. The levels of defence should be independent as far as is practicable (see also Ref. [3]).~~

3.6. The instrumentation and control system architecture should:

(a) Implement a defence in depth concept. For instrumentation and control, defence in depth includes implementing successive instrumentation and control functions designed to limit the consequences of a postulated initiating event despite the failure of the instrumentation and control functions designed to respond first.

(b) Not compromise the strategy to meet the defence in depth concept of the facility design.

INDEPENDENCE

3.7. Independence is intended to prevent the propagation of failures from the item affected by the failure to other redundancies, or from one system to another system independent of the safety class to which they belong.

3.8. The instrumentation and control system architecture should not compromise the independence in effect at the different levels of defence in depth.

3.9. Safety systems should be independent of systems of lower safety classification to ensure that the safety systems can perform their safety functions during and following any postulated initiating event that requires these functions without any interference or degradation from systems of lower safety classification.

3.10. The failure of the support features of safety systems should not compromise the independence between redundant components of safety systems or between safety systems and systems of lower safety classification.

CONSIDERATION OF COMMON CAUSE FAILURE

3.11. A common cause failure is defined as the failure of two or more structures, systems and components due to a single event or cause Ref. [~~4~~113~~3~~]. Common cause failure might happen, for example, because of:

— Human errors in operation or maintenance;

— A design deficiency;

— A manufacturing deficiency;

— Inadequate specification;

— Inadequate qualification for or protection against internal or external hazards, a human induced event, high voltages, data errors, data communication errors, or failure propagation between systems or components.

3.12. Latent failures and common failure modes that could potentially result in a common failure of the redundancies should be identified. Justification should be provided for those sources of common cause failure between systems or individual components that the operating organization does not consider credible. Justification that a common cause failure may not need to be considered can be based, for example, on the assigned level of defence in depth of the instrumentation and control function, the dependability of the components or the technology applied.

3.13. An analysis should be conducted of the consequences of each postulated initiating event within the scope of the safety analysis in combination with common cause failures that will prevent a protection system from performing the necessary safety functions.

3.14. The design of systems and components should take due account of the potential for common cause failures of items important to safety to determine how the concepts of diversity, physical separation, and electrical and functional isolation have to be applied to achieve the necessary reliability.

ARCHITECTURAL DESIGN OF THE INSTRUMENTATION AND CONTROL SYSTEM

3.15. The instrumentation and control system architecture:

(a) Should provide all instrumentation and control functions necessary to ensure the safe operation of the facility and to manage anticipated operational occurrences and accident conditions.

(b) Should provide the systems necessary to support the defence in depth strategy of the facility.

(c) Should provide preferably a hierarchical system design where instrumentation and control systems that belong to safety systems keep the highest priority to perform the safety functions for which they have been designed. In this way, other systems of lower safety class are not able to prevent the actions initiated by safety systems (i.e. shutdown of the reactor).

(d) Should provide a suitable arrangement of systems and components so that they can be adequately tested and maintained at regular intervals in accordance with their importance to safety.

(e) Should divide the overall instrumentation and control system into individual systems as necessary:

  (i) To fulfil design basis requirements for independence between functions at different levels of the defence in depth concept;

  (ii) To adequately separate systems and functions of different safety classes;

  (iii) To establish the redundancy necessary to fulfil design basis reliability requirements;

  (iv) To support the compliance of safety systems or groups with the single failure criterion and the fail-safe criterion;

  (v) To provide the necessary information and operator controls in the main control room and the supplementary control room (if applicable) and other areas where information is needed for operation or for managing an accident;

  (vi) To provide the automatic controls necessary to maintain and limit the process variables important to safety within the specified normal operational ranges.

(f) Should define the human-machine interface as well as the interfaces and means of communication between the individual instrumentation and control systems.

(g) Should consider special precautions in relation to the utilization and modification of the research reactor to ensure that the configuration of the reactor, as well as the configuration of the instrumentation and control system, is known at all times throughout the lifetime of the reactor.

3.16. The inputs to the design process for the instrumentation and control system architecture should refer to the documents on the safety design basis for the facility, which should provide the following information:

(a) The defence in depth concept of the facility;

(b) The groups of functions to be provided to address postulated sequences of initiating events;

(c) The safety classification and the functional and performance requirements of the facility functions important to safety;

(d) The role of automation and prescribed operator actions in the management of anticipated operational occurrences and accident conditions;

(e) The assignment of functions to operators and to automatic means;

(f) The information to be provided to the operators;

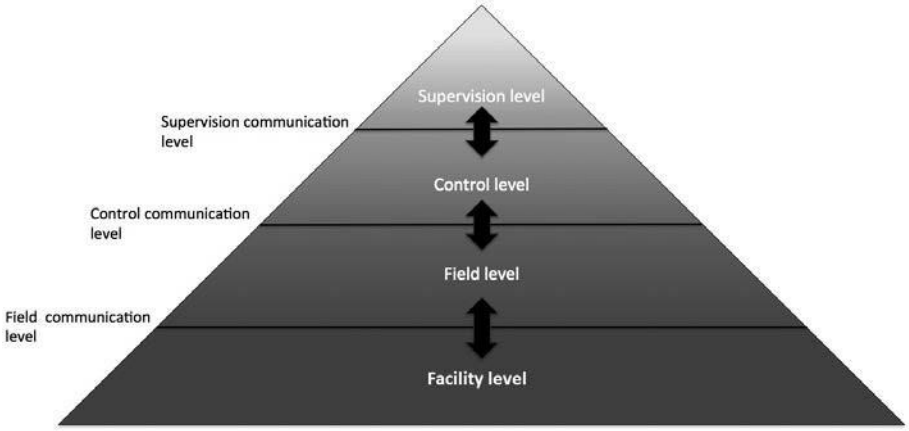
(g) The priority criteria between automatically initiated and manually initiated actions;

(h) National requirements, including those for licensing of instrumentation and control systems;

(i) Requirements on the operating organization with respect to operational features (i.e. the design of the instrumentation and control system as it affects the interface with facility operators) for systems important to safety.

~~3.17. The instrumentation and control systems should be designed in a 'top-down' architecture (see Fig. 2) having different levels of monitoring, processing, acquisition and actuation, sensors and actuator drivers. The monitoring functions should be allocated at the supervision level; the calculation, algorithms, and safety and process functions should be allocated at the control level; the acquisition and actuation functions should be allocated at the field level; and sensors and actuator drivers should be located at the facility level.~~

~~3.18.~~3.17. The use of diversity, redundancy and independence (i.e. physical separation, and electrical and functional isolation) in the architecture of the instrumentation and control systems should be consistent with the safety classification of each instrumentation and control system, and with the defence in depth concept, both for the overall facility and for the instrumentation and control system. In the case of redundancy, other factors such as reliability (i.e. the probability that a system or component will meet its minimum performance requirements when called upon to do so Ref. [113~~3~~4]) or the availability of instrumentation and control systems should be considered.



~~*FIG. 2. 'Top-down' architecture of the instrumentation and control systems.*~~

~~3.19.~~3.17. ~~The 'top-down' hierarchy architecture for the instrumentation and control systems requires the inclusion of three independent levels of communication to provide interfaces for communication between the different architectural levels and the reactor systems and facility systems, namely:~~

~~(a) Supervision level of communication; (b) Control level of communication; (c) Field level of communication.~~

~~3.20. The features mentioned in para. 3.19 should be used in the design of the different architectural levels to reduce the likelihood of dependent failures at these levels.~~

~~3.21.~~3.18 The instrumentation and control system should have a fail-safe design such that no malfunction within the system caused solely by variations of external conditions within the ranges detailed in the design basis would result in an unsafe condition or failure.

4. DESIGN GUIDELINES AND CRITERIA

GENERAL

4.1. Instrumentation and control systems should fully implement the requirements of their design bases. The origin of, and the objective for, every requirement should be specified and documented to facilitate verification and traceability to higher level documents and as a demonstration that all relevant design requirements have been accounted for.

4.2. The design of the instrumentation and control systems should be as simple as possible to fulfil their functions. Simplicity of design leads to fewer components, simpler interfaces, easier verification and validation, and easier maintenance of the hardware and software. ~~Adequate~~ Careful analysis of the design requirements is an effective means to achieve simplicity of design.

DESIGN BASIS

4.3. Each instrumentation and control system important to safety for the research reactor should have a design basis that specifies the following:

(a) The facility states (operational states and accident conditions) in which the system is required;

(b) The various configurations of the facility and experimental configurations that the instrumentation and control system is required to accommodate;

(c) Functionality requirements for each facility state, including extended shutdown;

(d) Performance requirements, including the guaranteed response time for safety functions including latency, precision and instrument error;

(e) The facility conditions during which manual control is allowed for each manual protective action;

(f) Postulated initiating events to which the system is required to respond;

(g) The variables, or combination of variables, to be monitored, the control actions required, and the identification of actions to be performed automatically, manually or both;

(h) The ranges, rates of change, and required accuracy of input and output signals of the system;

(i) Constraints on the values of process variables in all postulated conditions;

(j) Requirements for periodic testing, self-diagnostics and maintenance;

(k) System reliability levels, which may be specified using deterministic criteria, probabilistic criteria or both;

(l) Requirements for system availability;

(m) The range of transient and steady state environmental conditions under which the system is required to perform functions important to safety;

(n) The range of environmental conditions, including those hazards potentially arising from natural phenomena, under which the system is required to perform functions important to safety;

(o) Conditions with the potential to functionally degrade the performance of systems important to safety and the provisions to be made to retain their capability of performance;

~~The whole lifetime of the facility including accident conditions and conditions following an accident;~~

(p) ~~(q)~~ Operational constraints such as interface requirements with other systems.

4.4. In addition, for the design basis for reactor protection and shutdown systems, the following should be specified:

(a) The settings for the actuation of safety systems which should be derived from the assumptions of the safety analysis;

(b) Variables that are required to be displayed so that the operators can confirm the operation of protective system functions or to enable them to initiate manual actions;

(c) The conditions (including duration) under which a bypass of safety functions is to be permitted to allow for changes in operating modes, testing or maintenance.

DESIGN FOR RELIABILITY

4.5. Several measures should be used, if necessary in combination, to achieve and maintain the required reliability of the instrumentation and control system.

Redundancy and the single failure criterion

4.6. A single failure is a failure that results in the loss of capability of a component to perform its intended safety function(s) and any consequential failure(s) that results from this loss of capability of a component. The single failure could occur when the safety task is required or at any time prior to that.

4.7. The single failure approach is a deterministic method to determine the necessary degree of redundancy for items important to safety, and it is required to be applied (Requirement 25 of SSR-3 [1]).

4.8. The design is required to ensure, on the basis of analysis, that the redundancy will provide a backup to ensure that no single failure could result in a loss of the capability of a system to perform its intended safety function (Requirement 25 of SSR-3 [1]).

4.9. The criterion of redundancy should be considered to be the provision of alternative (identical or diverse) structures, systems or components such that any of these alternatives can perform the required function regardless of the state of operation or failure of any other structure, system or component performing the function. The criterion of redundancy is an important design principle for enhancing the safety and reliability of systems important to safety.

4.10. ~~Instrumentation and control systems important to safety are systems that play an important part in achieving the main safety functions: shutting down the reactor, providing cooling, in particular for the reactor core, and confining radioactive material. In the design of instrumentation and control systems that are~~For safety systems, the single failure criterion should be applied so that the system is capable of performing its intended safety function on the occurrence of any single failure. A single failure in the system should be considered together with: (a) other failures as a consequence of postulated initiating events; and (b) any credible undetected fault in the system.

4.11. The degree of redundancy should depend on the potential for failures that could degrade reliability. For all instrumentation and control systems important to safety, redundancy should be applied to the extent necessary to meet the requirements of the design basis for reliability and availability. For instrumentation and control systems that are safety systems, redundancy should also be applied to the extent necessary to comply with the single failure criterion when equipment is removed from service for planned surveillance or testing.

4.11. a. 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.

Common cause failure

4.12. The design of instrumentation and control systems important to safety should minimize the possibility of common cause failures by applying the criteria of independence and diversity. Safety systems should be designed in such a manner that common cause failures are prevented or mitigated.

4.13. As far as possible, redundant safety systems should be physically and electrically separate from each other and from systems of lower safety classification. Moreover, the criterion of independence should be used for the entire safety system, for example between redundant trains within the same system and across diverse systems fulfilling the same function, such as first and second shutdown systems.

Independence

4.14. The criterion of independence (e.g. functional independence, electrical isolation, physical separation by means of distance, barriers or a special layout, as well as independence of data transfer) should be applied, as appropriate and to enhance the reliability of systems. For example, different safety functions should be performed by different modules, components or systems to avoid the effects on each other of the failure of these items.

4.15. Examples of events caused by common cause failures that may be avoided by physical separation include failures resulting from fire, flooding and other external events or accident conditions. Physical separation also reduces the likelihood of inadvertent human errors.

4.16. The extent to which independence might be lost after a postulated initiating event should be considered in the design of certain parts of the facility, such as confinement penetrations, cable spreading rooms, equipment rooms and control rooms.

4.17. Electrical connections and data connections between redundant divisions within a safety system should be designed so that no credible failure in one redundant division would prevent the other redundant division(s) from meeting their requirements for performance and reliability.

4.18. Electrical connections and data connections between safety systems and systems of a lower safety classification should be designed so that no credible failure in the system of lower safety classification would prevent the safety systems from meeting their requirements for performance and reliability.

4.19. Electrical isolation should be used to control or prevent adverse interactions between equipment and components caused by factors such as electromagnetic interference, electrostatic pickup, short circuits, open circuits, grounding and, among other things, the application of the maximum credible voltage (AC or DC). Examples of provisions for electrical isolation are electronic isolating devices,

optical isolating devices (including optic fibre), relays, shielding of cables or components, separation and distance, or combinations of these.

4.20. When isolation devices are used between safety systems and systems of a lower safety classification, the isolation devices should be part of the system having higher safety classification.

4.21. When it is not feasible to provide adequate physical separation or electrical isolation between safety systems and systems of a lower safety classification, the lower safety classification system:

(a) Should be identified as part of the safety system with which it is associated; (b) Should be independent of other lower safety classification systems;

(c) Should be analysed or tested to demonstrate that the association does not unacceptably degrade the safety system with which it is associated.

4.22. If data communication channels are used in safety systems, they should satisfy the recommendations for independence (functional isolation, electrical isolation and physical separation). The concept also includes independence from the effects of data communication errors.

Diversity

4.23. Diversity provides defence against common cause failures, increasing the likelihood that appropriate safety actions will be performed when necessary.

4.24. Diversity is 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. Examples include: different operating conditions, different working principles or different design teams (which provides functional diversity), different manufacturers using different designs, and types of equipment that use different physical methods to provide physical diversity.

4.25. The criterion of diversity in instrumentation and control systems is met through the concept of monitoring and processing parameters using different methods or technologies, different logic or algorithms, or different means of actuation in order to provide more than one way to detect and respond to a specific event.

4.26. In any application, it should be ensured that the required diversity is achieved in the implemented design and preserved throughout the lifetime of the facility.

4.27. Where independence is claimed between two systems (e.g. a research reactor with a main reactor protection system and a second diverse reactor protection system) through multiplying their failure probabilities within the probabilistic safety assessment, then their diversity should be substantiated in consideration of the full instrumentation and control chain from the sensors, signal conditioning devices, and signal processors and calculators to the actuator drivers.

4.28. Diversity applied to instrumentation and control systems should include:

(a) Functional diversity: This could be achieved by systems providing different physical functions or physical means, resulting in the same safety effects.

(b) Equipment diversity: This could be achieved by sensors and systems using different technologies or designed and produced by different manufacturers.

4.29. In assessing the claimed diversity, attention should be paid to the components of equipment to ensure that diversity actually exists. For example, different manufacturers might use the same processor or the same operating system, thereby potentially incorporating common failure modes. Claims for diversity that are based only on a difference in manufacturers' names are insufficient without these considerations.

Failure modes

4.30. The failure modes of instrumentation and control systems important to safety should be known and should be properly documented using methods of failure mode analysis and cause and effect analysis. The more probable failure modes should neither place the system in an unsafe state nor cause spurious actuation of safety systems.

4.31. The failure modes of instrumentation and control systems important to safety should consider equipment and human factors, and their interactions.

4.32. Failures of components of instrumentation and control systems should be detectable by means of periodic testing or should be self-revealed by alarm or anomalous indication.

4.33. The design of instrumentation and control systems important to safety should include provisions for detecting all postulated (identified) failure modes in the system, preferably by a combination of failure alarms, and testing the credibility of readings, as appropriate. This is usually in addition to periodic testing to demonstrate system performance.

Fail-safe

4.34. The criteria of fail-safe design should be considered and should be adopted as appropriate in the design of instrumentation and control systems to enter a safe state on failure, with no necessity for any action to be initiated by any system or by the operator.

DESIGN CONSIDERATIONS FOR AGEING

4.35. The service life of electrical and electronic systems and components might be considerably less than the lifetime of the facility. Ageing degradation that impairs the ability of a qualified safety system component to withstand and function under severe environmental conditions could occur well before the component's functional capabilities under normal conditions are noticeably affected.

4.35.a. Obsolescence management should be considered in the design of ~~computer-based~~I&C systems to plan and manage for reductions in service life, diminishing manufacturing sources and material shortages. Special attention should be given to the obsolescence of computer-based equipment. Further

guidance on obsolescence management can be found in IAEA Safety Standards Series No. SSG-10, Ageing Management for Research Reactors [84].

4.36. Ageing mechanisms that could affect instrumentation and control system components and means for following the effects of these mechanisms should be identified during design. Ageing is commonly due to heat and also to radiation exposure. Nevertheless, the possibility that other phenomena (i.e. mechanical vibration or chemical degradation) might be relevant to a specific component should be considered.

4.37. Potentially significant ageing effects (e.g. thermal ageing and radiation ageing) should be addressed to show that the required functionality is maintained up to the end of service life. Further conservatism should be provided, where appropriate, to allow for unanticipated ageing mechanisms.

4.38. Examples of means to address the impacts of ageing include:

(a) Replacement of a component before the end of its qualified service life;

(b) Adjustment of functional characteristics (e.g. recalibration) to account for the effects of ageing;

(c) Changes to maintenance procedures or environmental conditions that have the effect of slowing the ageing process;

(d) Monitoring of the condition of equipment for ageing characteristics.

CONSIDERATION OF THE SAFETY AND SECURITY INTERFACE IN THE DESIGN

4.39. The purpose of nuclear security applied to instrumentation and control systems of research reactors is to prevent, detect and, when detected, eliminate or reduce the vulnerabilities that could be exploited from either outside or inside the site area of the protected facility, material, equipment, software and data.

4.40. As the instrumentation and control system is, in general, a combination of hardware and software modules that fulfil the overall functional and performance requirements to keep the research reactor in a safe and secure status, the architectural and functional vulnerabilities and their consequences for the instrumentation and control system should be assessed.

4.41. The design of the instrumentation and control system needs to consider and include preventing malicious interventions or exploitations of the system.

4.42. Many design concepts and components in the overall architecture contribute to enhancing both safety and security; nonetheless, an assessment should be performed to identify when one objective can be detrimental to the achievement of the other. Where conflicts are identified, compensatory measures should be considered during the design, so as not to weaken the safety or security of the systems.

4.43. Neither the operation nor the failure of any computer security feature should adversely affect the ability of a system to perform its safety function and conversely.

4.44. If computer security features are included in the human–machine interface, they should not adversely affect the operator's ability to maintain the safety of the facility.

4.45. Where practicable, security measures that do not also provide a benefit for safety should be implemented in devices that are separate from instrumentation and control systems.

4.46. IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities [15], provides guidance on implementing computer security programmes at nuclear facilities.

4.47. The recommended guidelines for safety in the design of instrumentation and control systems should not create adverse effects on the security system.

4.48. Safety functions should not be adversely affected by elements of the design intended to enhance security, and conversely security functions should not be adversely affected by elements of the design intended to enhance safety.

4.49. Security provisions must be applied in the instrumentation and control system from the beginning of the design of the system. One of the primary security considerations from a design perspective is the potential for the failure or manipulation of an instrumentation and control system due to an external or internal malicious act.

4.50. Operating organizations and designers should consider nuclear and computer safety and security in all phases of the project, namely: specification of requirements; conceptual, preliminary and detailed design; and the procurement, fabrication, integration, installation, commissioning, operation and maintenance, and decommissioning of the instrumentation and control systems.

4.51. National requirements for the information technology and IAEA guidance on computer security also need to be considered Ref. [15] and Ref [16].

EQUIPMENT QUALIFICATION

4.52. Instrumentation and control systems and components important to safety should be qualified for their intended functions. The qualification should provide a degree of confidence commensurate with the safety classification of the system or component. The basis for qualification should be documented.

4.53. The design should provide qualification programme(s) addressing all topics affecting the suitability of the system or component for its intended functions important to safety, including:

(a) Suitability and correctness of functions and performance for systems and components.

(b) Environmental qualification for components (including a qualification for radiation resistance if applicable). Items important to safety should be environmentally qualified for the effects of the accidents to which they are required to respond.

(c) Seismic qualification for components.

(d) Qualification for electromagnetic compatibility for systems and components.

4.54. Qualification should be based upon a combination of methods, including:

(a) The use of engineering and manufacturing processes in compliance with recognized standards;

(b) A demonstration of reliability;

(c) Past experience in similar applications;

(d) The testing of the equipment supplied;

(e) Analysis to extrapolate test results or operating experience under pertinent conditions;

(f) Ageing analysis as applicable.

4.55. Traceability should be established between all installed structures, systems and components important to safety and the applicable evidence of qualification. This includes traceability not only to the component itself, but traceability between the tested configuration and the installed configuration.

4.56. The equipment qualification programme should demonstrate that the as built instrumentation and control systems and installed components correctly implement the qualified design.

Suitability and correctness

4.57. The design of instrumentation and control systems and components important to safety should meet all functional, performance and reliability requirements contained in the design basis and in the equipment specifications.

4.58. Examples of functional requirements include the functionality required by the application, a support system or equipment operability, by the operator interface and by requirements for the input and output range.

4.59. Examples of performance requirements include requirements for accuracy and response time.

4.60. Examples of reliability requirements include requirements for fail-safe behaviour, conformance with the single failure criterion, independence, failure detection, maintainability and service life.

Internal and external hazards

4.61. Instrumentation and control systems and components should be protected against, and/or should be designed and qualified to withstand and operate through, internal and external hazards, including seismic hazards that are required in the design basis and in the safety analysis.

Environmental qualification

4.62. In the context of this Safety Guide, environmental qualification means qualification for conditions of temperature, pressure, humidity, chemicals and radiation, and for ageing mechanisms that might affect the proper functioning of components under those conditions. Systems and components should be designed to withstand the effects of, and to operate under, the environmental conditions associated with

normal operation, anticipated operational occurrences and accident conditions if they are required to function in incidents.

4.63. Components should meet all design basis requirements when subjected to the range of environmental conditions specified in the design basis.

Qualification for electromagnetic compatibility

4.64. The unperturbed operation of electrical and electronic systems and components depends on their electromagnetic compatibility with components located nearby or with which they are connected. Significant origins of electromagnetic interference could include, for example, fault current clearance by the operation of switchgear or circuit breakers or fuses, electromagnetic fields caused by radio transmitters, natural origins such as lightning strikes and geomagnetically induced currents, and other human made sources internal or external to the facility.

4.65. Systems and equipment, including associated cables, should be designed, installed and tested to withstand the conditions of their electromagnetic environment.

4.66. The types of electromagnetic interference to be considered in the design of instrumentation and control systems and components should include:

(a) Emission and conduction of electromagnetic disturbances via cables;

(b) Electrostatic discharge.

4.67. Electromagnetic compatibility qualification of instrumentation and control systems and components depends upon a combination of design of systems and components to minimize the coupling of electromagnetic noise to electrical components. Testing should be conducted to demonstrate that electrical components can withstand the expected levels of electromagnetic interference and to demonstrate that electromagnetic emissions are within tolerable levels. Testing for electromagnetic emissions should be applied to systems and components both important to safety and not important to safety. Instrumentation and control systems and components that are already qualified should be accompanied by the corresponding qualification certificate.

4.68. The emission characteristics of wireless systems and devices used at the facility as well as those of devices used for repair, maintenance and measuring should be taken into consideration. Wireless systems and devices analysed could include, for example, mobile telephones, radio transmitters and receivers, and wireless data communications networks.

4.69. Any electrical or electronic equipment at the facility will contribute to the electromagnetic environment. Instrumentation and control systems important to safety should be capable of performing safety functions in such electromagnetic environment. The contribution of electromagnetic emissions from all equipment — not only equipment important to safety — should be evaluated as well as its impact on the performance of instrumentation and control systems important to safety.

4.70. Equipment and systems, including associated cables, should be designed and installed and qualified to appropriately limit the propagation (both by radiation and by conduction) of electromagnetic interference to equipment at the facility. National and international industry standards for electromagnetic emissions should be considered.

TESTING AND TESTABILITY

4.71. The design of all instrumentation and control systems important to safety should include provisions that allow the performance of the required testing during reactor operation, or, if justified, during shutdown only, thereby supporting the observance of the recommendations and guidance provided in IAEA Safety Standards Series No. NS-G-4.2, Maintenance, Periodic Testing and Inspection of Research Reactors [376]. Many research reactors are operated on relatively short operating cycles and therefore provisions for testing during operation may not be necessary for such research reactors.

Test provisions

4.72. Provisions for testing instrumentation and control systems and components important to safety:

(a) Should have appropriate test interfaces and status indications. Test interfaces should include, for example, the capability to introduce simulated process conditions or electrical signals.

(b) Should operate in such a manner that faults in the equipment are readily detectable.

(c) Should have features to prevent unauthorized access.

(d) Should be located so that test equipment and the components to be tested are readily accessible.

(e) Should be located so that neither the testing nor access to the testing location exposes staff to hazardous environmental conditions. Where equipment to be tested is located in hazardous areas, provisions for testing from outside the hazardous area should be considered in the design.

(f) Should have communications facilities as necessary to support the tests.

4.73. It should be ensured in the design that the system cannot be unknowingly left in a test configuration. Inoperability or bypassing of safety system components or channels should be indicated in the control room. For frequently bypassed items, such indications should be auto-announcing.

4.74. Self-checking features of instrumentation and control systems important to safety should be considered and should be applied in the design as appropriate. It is necessary to balance the provision of self-checking features with the need for simplicity.

4.75. Built-in test facilities should themselves be capable of being checked at regular intervals to ensure continued correct operation.

Preserving control functions for instrumentation during testing

4.76. Arrangements for testing include: interfaces with test equipment, installed test equipment, built-in test facilities and procedures. Testing should neither compromise the safety function nor introduce the

potential for common cause failures. Safety aspects should be considered prior to the testing of systems important to safety during operation.

4.77. Test facilities that are permanently connected to safety systems should be considered part of the safety systems. Installed test facilities should be tested independently on a regular basis against another calibrated source.

Considerations for tests

4.78. Considerations for the tests should include:

(a) The location and installation of sensors such that their testing and calibration can preferably be performed at their location, including at facilities for draining, drying, decontamination, isolation and ventilation where applicable;

(b) The location of test devices and test equipment in areas convenient to the equipment to be tested;

(c) The features of the layout and administrative aspects;

(d) The convenience of the indications of component status and the test connections.

4.79. Communications facilities are necessary to support the tests. The design of instrumentation and control systems important to safety should include provisions to automatically alert operators that channels or components are in test mode. The notification of operators that channels or components are in test mode is often accomplished by alarms.

4.80. Channels of safety systems being tested should automatically be placed in trip condition during the testing.

4.81. The impact of the channel under test on assumptions made in the safety analysis should be considered.

4.82. Administrative controls should be considered prior to performing on-line tests on safety systems.

Test programme

4.83. The design of instrumentation and control systems should include the specification of a test and calibration programme. The scope and frequency of testing and calibration should be designed to be, and should be justified as, consistent with functional requirements and availability requirements. In determining the frequency of testing, the requirements for the accuracy and the stability of the instruments chosen should be taken into account. Stable instruments with low drift may need to be tested less frequently.

4.84. The test programme should include:

(a) A description of the programme objectives;

(b) An identification of systems and channels to be tested;

(c) The master test schedule;

(d) The reasons and justification for the tests to be conducted and the

test intervals;

(e) A description of the required documentation and reports;

(f) The requirements for periodic review of the effectiveness of the programme; (g) A specification of the individual test procedures to be used in the conduct of tests.

4.85. The tests defined in the test programme should ensure by means of clear procedures that during the tests and after their completion:

(a) The overall functional capabilities of the systems are not degraded.

(b) The instrumentation and control systems continue to meet their design basis requirements of functionality and performance and are returned correctly to operation.

4.86. The test programme should arrange tests into a sequence such that the overall condition of the system or component under test can be assessed without, as far as practicable, further testing of other components or systems.

4.87. The test programme should define processes for periodic tests and calibration of systems that:

(a) Specify overall checks of all functions, from the sensors to the actuators, that are capable of being performed in situ and with a minimum of effort;

(b) Confirm that functional and performance requirements [2] for the design basis are met by documenting the success of a test showing compliance with tolerance requirements;

(c) Test all inputs and output functions, such as alarms, indicators, control actions and the operation of actuation devices;

(d) Provide post-maintenance testing to ensure that systems are returned correctly to operation;

(e) Ensure the safety of the facility during the conduct of the test;

(f) Minimize the possibility of spurious initiation of any safety action and minimize any other adverse effect of the tests on the availability of the research reactor.

4.88. Conduct of the test programme should not cause deterioration of any system or component.

[2] Requirements for testing of the response time should be strictly based on the assumptions made in the safety analysis report and should be limited to parameters that require special consideration for testing of the response time because their timely response is important to the safety of the facility.

4.89. Where temporary connections of equipment are required for periodic testing or calibration, the operator should be alerted by alarms and/or warning lights of the presence of the temporary connection and use of such equipment should be subject to appropriate administrative controls.

4.90. Temporary modification of computer codes in systems and components for testing purposes should not be allowed.

4.91. The time interval for which equipment is removed from service should be minimized and each sensor should be individually tested to the extent practicable.

4.92. Tests of safety system channels should preferably be single on-line tests. When a single on-line test is not practicable, the test programme may combine overlapping tests to achieve the test objectives. For tests of safety system channels, documented justification for the use of overlapping tests should be provided.

4.93. Tests of a safety system should independently confirm the functional requirements and the performance requirements of each channel of sensing devices, and of command, execution and support functions.

4.94. Tests of a safety system should include as much of the function under test as practicable (including sensors and actuators), with due consideration of the wear on actuators when tested excessively.

4.95. Wherever possible, tests of a safety system should be accomplished under actual or simulated operating conditions, including the sequence of operations. Precautions should be taken in testing safety systems that are sensitive and important.

4.96. After a failed test, the reasons for the failure, its root causes and the actions taken afterwards should be evaluated and documented before the results of a repeated test can be used to demonstrate the operability of the system or the component involved.

4.97. Corrective actions may include, for example, maintenance or repair of components, or changes to test procedures. If corrective actions are determined to be unnecessary, the reasons should be documented.

MAINTAINABILITY

4.98. Provision of means for the maintenance of instrumentation and control systems should be considered in the design. The design of instrumentation and control systems should include maintenance plans for all systems and components.

4.99. Instrumentation and control systems and components should be designed to minimize radiological and other risks to maintenance personnel and to facilitate preventive maintenance, troubleshooting and timely repair.

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

(a) Avoiding locating equipment in areas of extreme temperature or humidity, and possible high radiation levels;

(b) Considerations of human factors in performing the required maintenance activities;

(c) Leaving sufficient space around the equipment to ensure that the maintenance staff can perform their tasks with their supporting tools;

(d) The provision of test panels, instrument isolation and draining and test connections.

4.101. If components have to be located in inaccessible areas, other solutions should be considered in the design. Examples include:

(a) The installation of spare redundant devices in cold or hot standby;

(b) The provision of facilities for remote replacement, repair and return to service.

DESIGN ANALYSIS

4.102. Safety analysis is used to support the design of a new instrumentation and control system or the modification of an existing system. Design analyses, including the following specific activities, should be performed to confirm that instrumentation and control systems fulfil their design basis requirements (more guidance is available in IAEA Safety Standards Series No. SSG-20, Safety Assessment for Research Reactors and Preparation of the Safety Analysis Report, [98~~7~~]):

(a) Confirmation that all known and predictable failure modes are either self-revealing or detectable by planned testing and that the system is fail-safe.

(b) Verification that the overall instrumentation and control system supports the defence in depth concept of the facility.

(c) Verification that the vulnerabilities of instrumentation and control systems important to safety to common cause failures are known and have been adequately addressed. Vulnerabilities to common cause failures may be dealt with by eliminating the vulnerabilities, by providing diverse means of achieving the safety functions that are subject to the common cause failures, or by justifying acceptance of the vulnerability.

(d) Verification that design basis reliability requirements are met. This demonstration may be based on a balance of application of deterministic criteria and quantitative reliability analysis in which design features such as redundancy and testability, failure modes, mean time between failures and rigour of qualification are considered. For complicated systems, a combination of qualitative analysis, quantitative analysis and testing is usually needed to verify compliance with design basis reliability requirements.

(e) Verification that the design of instrumentation and control systems includes adequate provisions for testing.

(f) In determining system availability, test facilities that are part of the safety system should be regarded as permanently installed test equipment.

(g) Confirmation of functional requirements for various operational modes of instrumentation and control systems. This includes analysis of correct system behaviour in commissioning, in first startup when the facility is not operating under normal conditions (e.g. following trips due to low flux with fresh core), and in normal operation, following power interruptions and restart or reboot after the execution of tests.

(h) Verification that the effects of failures of automatic control systems will not exceed the acceptance criteria established for anticipated operational occurrences.

4.103. The methodology for any analysis that is conducted should be thoroughly specified and should be documented, together with the inputs for the analysis, its results and the details of the analysis itself. Typically, traceability analysis is used to confirm implementation and validation requirements.

4.104. Each assumption made for an analysis should be justified and such justification should be documented.

SAFETY SYSTEM SETTINGS

4.105. The requirements and operational limits and conditions established in the design for the facility should include safety system settings for instrumentation and control systems.

4.106. The following values are usually considered in the determination of settings for instrumentation and control systems that are safety systems:

(a) Safety limits: Limits on certain operational parameters within which operation of the reactor has been shown to be safe;

(b) Analytical limits (of safety system settings): Limits of a measured or calculated variable established by the safety analysis to ensure that a safety limit is not exceeded;

(c) Allowable values: The limiting values of safety system settings, beyond which appropriate action is required to be taken. The allowable value for a particular safety system setting specifies the value at which it is acceptable to find that a trip would occur when periodically testing the corresponding channel. If the point at which a protective action would be initiated is found to be beyond the allowable value, corrective action should be taken.

Figure 23 illustrates the relationship between these terms and the types of measurement uncertainty that are normally considered in establishing the basis for safety system settings for trips and the allowable values.

4.107. The adequacy of the safety classification should be verified by using deterministic safety analysis, which should be complemented by insights from probabilistic safety assessment and/or supported by engineering judgement. Expert groups providing engineering judgement should include knowledgeable personnel from design and operating organizations of a research reactor facility.

4.108. A consistent and coherent method of naming and identifying all instrumentation and control components should be determined and followed throughout the design, construction, installation, commissioning and operation stages of the reactor facility as well as for the labelling of controls, displays and indications. Clear identification of components should be used to reduce the likelihood of inadvertently performing installation, modification, maintenance, tests, repair or calibration on an incorrect channel. Components or modules mounted in equipment or an assembly that is clearly identified may not themselves need identification.

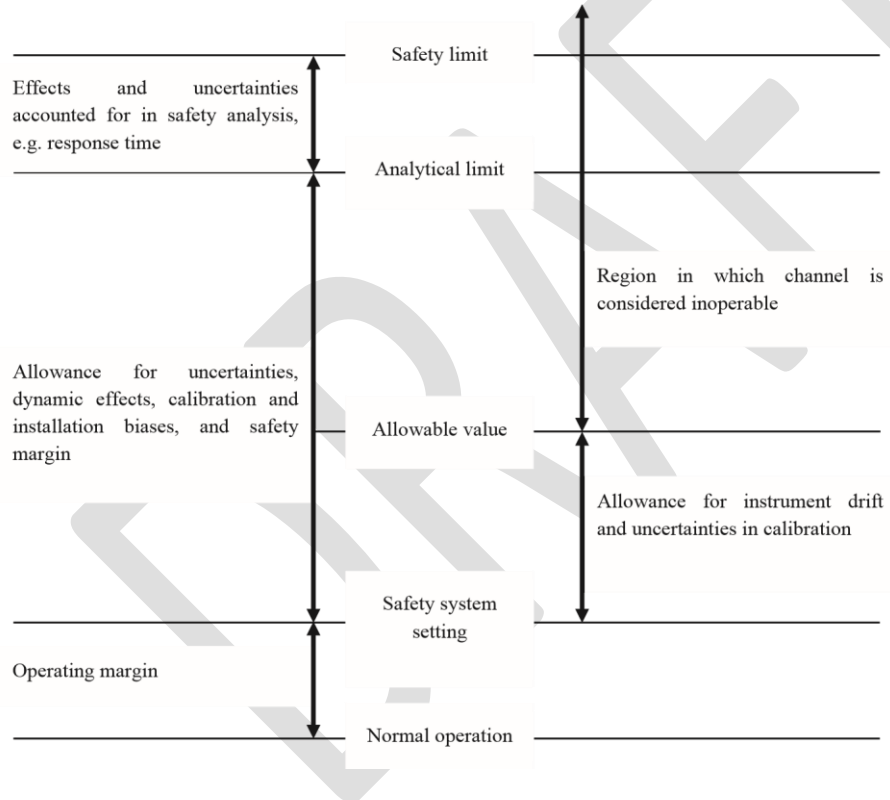


FIG. ~~3~~2. Safety system setting terminology and errors to be considered in determining safety system settings.

CONSIDERATION FOR DESIGN EXTENSION CONDITIONS

4.109. SSR-3 [1] para 6.65 states " The design extension conditions shall be used to define the design specifications for safety features and for the design of all other items important to safety that are necessary for preventing such conditions from arising, or, if they do arise, for controlling them and mitigating their consequences."

4.110. The I&C systems and equipment provided for additional safety features for design extension conditions should be subjected to the requirements for equipment qualification, reliability, testability, maintainability, and inspectability, as well as ageing management. This equipment should be considered as items important to safety.

5. SYSTEM SPECIFIC DESIGN GUIDELINES

SENSING DEVICES

5.1. Measurements of variables for a research reactor should be consistent with the requirements of the design basis. These measurements include both detection of the present value of a variable within a range and detection of a discrete state such as is detected by limit switches or on/off switches (i.e. temperature, pressure, flow or level limit switches and switches for availability of the main supply or for normal operation of the control system, or interlock on/off switches).

5.2. The measurements of variables may be made directly or indirectly, such as calculation of the value by performing multiple measurements, or by measuring other data having a known relationship to the desired variable.

5.3. To the extent practicable, the reactor conditions should be monitored by direct measurements rather than being inferred from indirect measurements.

5.4. 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 normal operation and in accident conditions.

5.5. Vulnerability of sensing devices to common cause failure should be identified (e.g. saturation of radiation monitors), as they have a potential to deny operators the information and parameters necessary to control and mitigate accident conditions.

5.6. If more than one sensor is necessary to cover the entire range of the reactor parameter being monitored, a reasonable amount of overlap from one sensor to another should be provided. Examples include source range, intermediate range and power range of neutron flux monitors.

5.7. If the monitored variables have a spatial dependence (i.e. if the measured value of a parameter depends upon the location of the sensor), the minimum number and locations of sensors, such as flow measurement elements, should be identified by the design and justified. The final locations also need to be tested to verify the design assumptions and to determine whether associated set points, limiting conditions and allowable values should be reassessed.

REACTOR PROTECTION SYSTEM

5.8. Where applicable, the reactor protection system should comply with all the general guidance in Section 4 for the design of instrumentation and control systems.

5.9. The design of the reactor protection function should include provisions to bring the reactor into a safe condition and to maintain it in a safe condition, even if the primary reactor protection system is subjected to a credible common cause failure (e.g. hardware failure or failure due to human factors).

5.10. The reactor protection system should include, as a minimum, a function to initiate shutdown of the reactor. In case of subcritical assemblies, the shutdown may be achieved by withdrawing the neutron source. The reactor protection system may also provide other safety functions such as initiation of emergency core cooling, confinement functions and maintaining of the reactor in a safe and stable condition (the features of the reactor protection system acting in this case as extended engineered safety features of the instrumentation and control system).

5.11. The appropriate protective actions should be initiated automatically for the full range of postulated initiating events to terminate the event safely.

5.12. As part of defence in depth and to cope with a potential common mode failure of the primary protection system, the need for a second protection system with all or some of the functions of the primary protection system should be considered. Where two reactor protection systems are provided, these two systems should be independent and diverse from one another.

5.13. The action initiated by the reactor protection system should be latched so that once an action is initiated, it should continue until its completion even if the initiating state is terminated. Functions added to latch safety actions should not reduce the reliability of the safety action below an acceptable level.

5.14. In some cases, manual operator action to initiate a protective action may be considered to be sufficient provided that the diagnosis is simple and the action is clearly defined:

(a) The operator has sufficient and clearly presented information to make valid judgements on the need to initiate the required safety actions.

(b) The operator is allowed sufficient time to evaluate the status of the reactor facility and to complete the required actions.

(c) The operator is provided with sufficient means of control of the reactor to perform the required actions.

5.15. In addition to any automatic actions, means should be provided to manually initiate reactor trip and any other safety actions of the reactor protection system. The manual actuation function should act directly on the final actuation devices (e.g. reactor trip breakers) rather than being an input to the reactor protection system logic.

5.16. Functions that inhibit tripping of the protection system, including the means for activating and deactivating these functions, should be part of the protection system. Sometimes, it is necessary to inhibit the action of protection system functions to enable changes in reactor conditions. For example, the trips that limit reactor power during startup have to be inhibited at some point to enable power increase.

Another example would be the necessity to inhibit certain functions in the case of pulsed operation of a research reactor. In this Safety Guide, such inhibit functions of the reactor protection system are called operational interlocks and are classified as components and/or functions of safety systems.

5.17. The protection system should prevent enabling of an operational interlock when the applicable enabling conditions are not met. If conditions change so that an enabled operational interlock is no longer permissible, the protection system should automatically accomplish one of the following: disable the operational interlock; or initiate appropriate protective actions.

5.18. ~~Paragraph 4.89 provides a recommendation on temporary connections used for maintenance and testing. This recommendation should be strictly applied to the reactor protection system~~Where temporary connections of equipment are required for periodic testing or calibration of the reactor protective system, the operator should be alerted by alarms and/or warning lights of the presence of the temporary connection and use of such equipment should be subject to appropriate administrative controls.

5.19. The design should ensure that safety system settings can be established with a margin between the initiation point and the safety limits where the action initiated by the reactor protection system will be able to control the ~~process~~ parameter before the safety limit is reached. In addition, the following should be taken into account in selecting such margins:

(a) Inaccuracy of instrumentation;

(b) Uncertainty in calibration;

(c) Instrument drift;

(d) Instrument and system response time.

5.20. If a computer based system is intended to be used in a reactor protection system:

~~(a) Hardware and software of high quality should be used and best practices should be employed;~~

~~(b)~~(a)The ~~whole~~ life cycle of the system should be systematically documented and reviewed;

~~(c)~~(b)Independent verification and validation processes should be applied.

5.21. Where the necessary reliability of a computer based system that is intended for use in a reactor protection system cannot be demonstrated to a high level of confidence, diverse means of ensuring fulfilment of the protection functions should be provided. The diversity may be provided:

(a) Internally to the reactor protection system or by a separate and independent system, provided that the design bases are met;

(b) By a diverse independent system, which may be hard wired or computer based as long as adequate diversity can be justified.

It is usually easier to justify diversity between computer based and hardware based systems than between two computer based systems.

5.22. ~~As stated in para. 6.104(c) of NS-R-4~~Para 6.180 (c) of SSR-3 [1] states:

> "In order to~~To~~ confirm the reliability of the computer based systems, ~~an~~ a systematic, fully documented and reviewed assessment ~~of the computer based systems~~ shall be undertaken by expert personnel who are independent of the designers and the suppliers."

5.23. For computer based reactor protection systems and equipment, the ~~system~~ design needs to consider and include computer security features (see paras 4.39–4.51) for the whole lifecycle of the reactor protection system.

OTHER INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY

5.24. The reactor operator should be provided with sufficient instrumentation for monitoring the operation of the reactor systems during normal operation (including shutdown, refuelling and maintenance) and accident conditions, including recording all variables important to safety.

5.25. The requirements for startup neutron sources and dedicated startup instrumentation for the conditions in which they are needed should be taken into account in the design.

5.26. The safe operation of a research reactor, intended to cover all ~~normal~~ modes of operation, should be considered in the design process. The design process should establish a set of requirements and limitations on the normal operation of the instrumentation and control systems as necessary for the safe operation of the facility. These requirements and limitations should cover:

(a) The information necessary to establish the safety limits and safety system settings;

(b) Control system constraints and procedural constraints on process variables and other important parameters;

(c) Maintenance, testing and inspection of the facility to ensure that systems, structures and components function as intended;

(d) Clearly defined operating configurations, including operational restrictions in the event of safety system outages;

(e) Considerations for research related tasks.

These requirements and limitations are the bases for establishing the operational limits and conditions under which the reactor is authorized to operate.

CONTROL ROOMS

5.27. In the main control room, supplementary control room (if required) and other areas where staff are expected to monitor and control facility systems, the necessary provisions should be implemented to ensure satisfactory conditions in the working environment and to protect against hazardous conditions.

Task analysis factors, ergonomic factors and human factors should be considered in the design of control rooms.

5.28. The design of control rooms should include adequate provisions for preventing unauthorized access and use.

5.29. The control rooms should be designed and constructed to resist internal and external hazards in particular fires and one control room (main, supplementary or emergency) should be designed and constructed to resist design basis earthquakes.

Main control room

5.30. The principal location for safety actions and safety related control actions is the main control room. A control room should be provided from which the reactor facility can be safely operated in all its operational states and from which measures can be taken to maintain the research reactor in a safe state or to bring it back into a safe state after the onset of anticipated operational occurrences and accident conditions.

Supplementary control room

5.31. A remote capability for reactor shutdown should be provided if the safety analysis identifies events that could inhibit the operator's ability to shut down the reactor and to maintain it in a safe condition from the main control room. A supplementary control room or emergency control console should be provided if operators are required to perform safety actions and the safety analysis identifies events where the main control room could be unavailable or operations from the main control room could be inhibited. Events that could inhibit the operator's ability to shut down the reactor from the control room include, for example, a fire in the control room or a fire in a location that affects connections between the control room and devices elsewhere in the facility.

5.32. The instrumentation and control systems of the supplementary control room should be appropriately independent of the main control room to avoid common cause failures diminishing the operability of the systems of the supplementary control room. For example, the design of control system networking should be such that there is minimal chance of being unable to use the system from either of the two control rooms. Another example is the separation of power supplies for the control rooms.

5.33. A suitable provision outside the main control room should be considered and applied as appropriate for transferring priority control to a new location and for isolating the equipment in the main control room whenever the main control room is abandoned.

5.34. The design of the supplementary control room should take into account ergonomic factors and should include suitable provisions for preventing unauthorized access and use.

CONTROL SYSTEMS FOR IRRADIATION FACILITIES AND EXPERIMENTAL DEVICES

5.35. In many research reactors, there are special control consoles for irradiation facilities and experimental devices, which may be located in the main control room and/or in other rooms. The operator of experimental devices should have communications links with the reactor operator to share information on experiments and on the reactor status and to make each other aware of expected actions (e.g. situations that require shutdown of the reactor).

5.36. The control consoles for irradiation facilities and experimental devices should be devoted exclusively to the irradiation facilities and experimental devices if the safety analysis identifies events that show an independent I&C system is required for irradiation facilities to keep a functional separation from the other activities at the research reactor.

5.37. Parameters important to the operation of the reactor should be covered by the alarm system. ~~Other a~~Alarms of experimental devices, with no reactor safety implications, should be presented with a functional separation from the reactor alarms.

VOICE COMMUNICATION SYSTEM

5.38. Communication systems should be provided for staff to have secure interfaces between the main control room, the supplementary control room (if applicable) and other locations within the facility, the operators of experimental devices, associated facilities, the on-site emergency centre and off-site response organizations without having to leave the control room.

5.39. Both the main control room and the supplementary control room should have at least two diverse communications links with:

(a) Areas where communications are needed in anticipated operational occurrences and accident conditions;

(b) Off-site emergency response organizations;

(c) Associated facilities.

5.40. The diverse communications links should be routed so that they will not both be affected by loss of the primary communications links, whatever its origin (including external events), and they should be capable of operating independently of both the facility power systems and the off-site power systems. Requirement 55 from SSR-3 [1] requires the provision of relevant information and means of communication from the control room(s) to the emergency response facility on site. The emergency response facility should also use environmental monitoring information from sources outside the research reactor. The information and communication links should be designed for operation during accident conditions.

PROVISIONS FOR FIRE DETECTION AND EXTINGUISHING

5.41. The nature of the fire alarm system, its layout, the necessary response time and the characteristics of its detectors should be determined on the basis of the fire hazard analysis. The detection system should provide a warning by means of audible and visual fire alarms in the control room of the detailed location of the fire.

5.42. Local audible and visual fire alarms, as appropriate, should also be provided in areas of the facility that are usually occupied. Fire alarms should be distinctive to avoid confusion with any other alarms at the facility.

5.43. The fire detection and alarm system should be operational at all times and should be provided with non-interruptible emergency power supplies, including fire resistant cables where necessary.

5.44. Fire detectors should be located so that the flow of air due to ventilation or pressure differences that are required for contamination control will not cause smoke or heat energy to flow away from the detectors and thus unduly delay actuation of the detector alarm.

5.45. If the environment does not allow detectors to be placed in the area to be protected (e.g. owing to increased radiation levels or high temperatures), alternative methods should be considered, such as the sampling of the gaseous atmosphere by remote detectors with automatic operation.

5.46. When items such as fire pumps, water spray systems, ventilation equipment, fire dampers and the corresponding power supplies are controlled or used by fire detection systems, and where spurious operation would be detrimental to the facility and the personnel, operation should be controlled by two diverse means of fire detection operating in series. The design should allow the operation of the system to be stopped if the actuation is confirmed to be spurious. The potential effects on the facility of the spurious operation of the items should also be considered, for example gas suppression systems may be a good alternative to water sprinkler systems for rooms containing power systems and instrumentation and control systems.

5.47. Wiring for fire detection systems, alarm systems or actuation systems should be:

(a) Protected from the effects of fire by a suitable choice of cable type, by proper routing or by other means;

(b) Protected from mechanical damage;

(c) Constantly monitored for integrity and functionality.

5.48. Requirements for periodic testing should be considered.

5.49. National requirements for fire protection as inputs for the design should be considered.

POWER SUPPLIES OF INSTRUMENTATION AND CONTROL SYSTEMS

5.50. The power supplies for instrumentation and control systems should be classified and have reliability provisions, qualification, isolation, testability, maintainability and indication of removal from service, consistent with the design basis reliability requirements of the instrumentation and control systems that they serve. In addition, failure modes for power supplies should be considered.

5.51. Instrumentation and control systems that are required to be available for use at all times, in operational states or in accident conditions, should be connected to uninterruptible power supplies that provide the instrumentation and control systems with power within the tolerances specified by the design basis for the systems. These tolerances should be specified for the instrumentation and control systems to withstand failures in the normal power supply as well as a facility blackout considered an external event in the safety analysis.

5.52. Power supplies can provide a transmission path for electromagnetic interference that might originate outside the instrumentation and control systems or might arise from other instrumentation and control systems that are connected directly or indirectly to the same power supply. Such origins of interference include electrical fault clearance associated with other equipment on the same supply. These interferences should be analysed and should be avoided to the extent possible.

6. OPERATION

OPERATIONAL LIMITS AND CONDITIONS

6.1. ~~Paragraphs 7.29 and 7.30 of NS-R-4~~Requirement 71 of SSR-3 [1] state~~s~~ that:

"The operating organization for a research reactor facility shall ensure that the research reactor is operated in accordance with the operational limits and conditions."~~"7.29. A set of OLCs [operational limits and conditions] important to reactor safety, including safety limits, safety system settings, limiting conditions for safe operation, requirements for inspection, periodic testing and maintenance and administrative requirements, shall be established and submitted to the regulatory body for review and assessment.~~

~~"7.30. The OLCs shall be used to provide the framework for the safe operation of the research reactor...."~~

6.2. The design of the instrumentation and control systems of the reactor should ensure that, for the operational states of the reactor, the instrumentation and control systems contribute to keeping the reactor's operating parameters within the operational limits and conditions. A~~-~~dditional guidance is provided in IAEA Safety Standards Series No. NS-G-4.4, Operational Limits and Conditions and Operating Procedures for Research Reactors [59~~8~~].

Safety limits

6.3. The instrumentation and control systems should include those safety functions and safety related functions that prevent the exceeding of safety limits in operational states of the reactor by means of the selected safety system settings, in design basis accidents and, as far as practicable, in ~~beyond design basis accidents~~design extension conditions.

Safety system settings

6.4. For each parameter for which an analytical limit is required and for other important safety related parameters, an instrumentation and control system should monitor the parameter and, where appropriate, should provide a signal that can be utilized in an automatic mode to prevent that parameter from exceeding the set limit. ~~The required instrumentation and control systems that are to provide these functions should have the capability of storing and recovering these safety system settings.~~

Limiting conditions for safe operation

6.5. Acceptable margins between normal operating values and the safety system settings should be considered in the functions of the instrumentation and control systems to ensure safe operation of the reactor, while avoiding the frequent actuation of safety systems. Acceptable margins should be allowed for instrument accuracy, expected drift and allowable margin or error in measured signals and for all expected variations in normal operation.

CONTROL OF ACCESS TO SYSTEMS IMPORTANT TO SAFETY

6.6. All reasonable precautions should be taken to prevent persons from carrying out unauthorized actions that could jeopardize safety when accessing instrumentation and control systems or performing tasks on instrumentation and control systems Ref. [10~~8~~9].

6.7. Instrumentation and control systems classified as important to safety should be controlled to prevent unauthorized access. Access control methods should include physical restrictions or barriers, special embedded devices and restrictions on access to functions important to safety by means of hardware or software access keys, access alarms and administrative controls.

6.8. Access to the safety system settings and calibration adjustments should be restricted by physical and administrative means.

6.9. The protection of computer based components of instrumentation and control systems needs to be addressed in appropriate security procedures. National regulations, standards and IAEA guidance may be used to specify the requirements for control system security Ref [15] and Ref. [16].

6.10. Secure storage arrangements and procedural controls should be used to ensure that only authorized software versions are loaded into the equipment of the facility. The correct performance of the computer based system should be demonstrated before it is returned to service.

6.11. Electronic access to software and data of computer based systems via external network connections should be prohibited.

6.12. Access control methods should be used to allow users access to only those data and commands for which they have been authorized.

6.13. The security policy needs to apply suitable measures to prevent unauthorized access, use or corruption of the software or data, the introduction of malicious code, unauthorized connections to external networks or other computer based attacks.

MAINTENANCE, TESTING, SURVEILLANCE AND INSPECTION OF INSTRUMENTATION AND CONTROL SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY

6.14. Inspection, periodic testing, surveillance and maintenance of instrumentation and control systems should be conducted to ensure that all their components function in accordance with the design intent and with the requirements, in compliance with the operating limits and conditions, and in accordance with requirements for the long term safety of the reactor. The frequency or periodicity for such activities should be consistent with the reliability requirements for such systems or components. Additional guidance is provided in NS-G-4.2 [~~7~~3].

6.15. The instrumentation and control systems should include~~, where applicable, on-line testing functions and~~ the capability~~ies~~ to facilitate periodic testing and, where applicable, on-line testing functions to reduce the time such testing takes, improving the availability of the reactor.

PROVISIONS FOR REMOVAL FROM SERVICE FOR TESTING OR MAINTENANCE

6.16. Removal from service of any single safety system, component or channel should not result in loss of the required minimum redundancy unless the acceptably reliable operation of the system can be adequately demonstrated.

6.17. If use of equipment for testing or maintenance can impair an instrumentation and control 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.

6.18. For safety systems, design features should ensure that during periodic tests of part of a safety system, those parts remaining in service can perform the required safety task. For example, tripping the redundancy during the testing of a ‘two out of three’ logic leaves the system in a ‘one out of two’ logic arrangement. Administrative controls on the availability of safety systems should keep them in operation within the design basis.

EXTENDED SHUTDOWN

6.19. A research reactor facility may have a period of extended shutdown when decisions are pending on its future or for any other reason. The operating organization should assess and define the minimum

instrumentation and control systems required for safety to be kept operational during such an extended shutdown.

7. HUMAN FACTORS ENGINEERING AND THE HUMAN–MACHINE INTERFACE

GENERAL CONSIDERATIONS

7.1. An effective process for human factors engineering should be embedded into the overall design process for every aspect of the design.

7.2. Appropriate design standards and guidelines should be identified and should be used throughout the design process.

7.3. Verification and validation of human factors should be included throughout the design process to confirm that the design adequately accommodates all necessary operating actions and administrative arrangements of the operating organization.

7.4. In the case where only a part of the instrumentation and control system is modernized, careful consideration should be given to the design of the modernized part of the system and to its compatibility with and human interaction with the existing systems, such as task analysis and consideration of factors such as timing and human cognition and perception (operator overload and available indications for the operator response), to ensure proper and continued operation following the recommendations given in paras 7.1 and 7.2.

CRITERIA FOR HUMAN FACTORS ENGINEERING AND DESIGN FOR THE HUMAN–MACHINE INTERFACE

7.5. The design for human–machine interfaces should retain useful features and should avoid the problems and issues with human factors engineering that were experienced in previous designs. Such design considerations should be included in architectural considerations in new projects as well as in modification projects. The design for the human–machine interface should emphasize the incorporation of human features and machine features and the advantages of applying both.

7.6. Instrumentation and control functions necessary to achieve the safety objectives for the facility should be identified and allocated to human resources and system resources in accordance with a specified methodology and should be included in architectural considerations at the design stage.

7.7. All human–machine interfaces should be designed in accordance with ergonomic criteria. The operational philosophy should determine which information is convenient to display using conventional displays (e.g. panel instruments and alarm annunciators) and which information is convenient to display using video screens. In the establishment of design criteria for information displays and controls, the different roles of the operating personnel such as operators, maintenance staff, systems managers and personnel with responsibilities in an emergency should be taken into account.

7.8. Requirements for design for the human–machine interface should be specified on the basis of all the tasks to be supported by the human–machine interface, including normal operation and anticipated operational occurrences and accident conditions, for the operators as well as for the maintenance staff, the experimenters and personnel with responsibilities in an emergency.

7.9. The specification of requirements for the design of human–machine interfaces should include the instrumentation and control requirements necessary to assess the general state of the facility, in whatever condition it may be, and requirements for confirmation that automatic safety actions are taken as intended in the design.

7.10. The instrumentation and control system should provide operators with the information necessary to detect changes in the status of systems, to diagnose the situation and to verify manual actions or automatic actions.

7.11. During operation of the facility, the operator should be provided with suitable warnings or alarms when the facility is approaching a state in which operational interlocks should be enabled or should be disabled.

7.12. The reactor operator should be provided with sufficient indicators and recording instrumentation to be able to monitor relevant reactor parameters in, and following, anticipated operational occurrences and accident conditions.

7.13. Audible and visual alarm systems should be used to provide an early indication of changes in the operating conditions of the reactor if these changes in the operating conditions could affect its safety.

7.14. Careful attention should be paid in the design of human–machine interfaces to ensure that the operator would not be overwhelmed by large amounts of data that could be difficult to assimilate owing to the inherent limitations on human perception, cognition and memory. This is particularly important in the case of the treatment of alarms.

7.15. In the design of the instrumentation and control system, due account should be taken of the time periods necessary for operators to perform their expected tasks.

7.16. The instrumentation and control system should protect against operator errors by implementing range limits, interlocks or trips to protect the facility from unsafe operation.

7.17. Where a function is carried out automatically, the instrumentation and control system should provide operators with the necessary information to monitor the function. The information should be provided at a rate and to a level of detail that the operator can monitor effectively.

7.18. The instrumentation and control system should alert the operator of a failure of an automatic control system.

7.19. The presentation of information should be harmonized to facilitate the operator’s understanding of the facility’s status and of the activities necessary to control the facility.

7.20. The operation and appearance of the human–machine interfaces should be consistent among the various locations for information and control, should reflect a high degree of standardization and should be fully consistent with procedures and training.

7.21. The human–machine interfaces should provide the capability to display recorded information where such information will help operators to identify patterns and trends, to understand the past or present state of the system, or to predict its future progression.

CONTROL ROOMS

7.22. Requirements for functional isolation and physical separation as well as ergonomic criteria should be taken into account in the design of the control rooms.

7.23. In the design of control rooms, aspects of human factors engineering such as workload, possibility of human error, operator response time and minimization of the physical and mental effort of the operator should be taken into account in order to facilitate the execution of the necessary operating procedures to ensure safety in all operational states and accident conditions.

7.24. Acceptable working environments in control rooms should be ensured in terms of radiation exposure, lighting, temperature, humidity, noise, dust and vibration, for normal operation, anticipated operational occurrences and accident conditions. The design of the main control room and the supplementary control room (if required) should take into account conditions resulting from internal hazards (e.g. fire or smoke, or toxic substances in the atmosphere) and external hazards (e.g. earthquakes, flooding, extreme meteorological conditions and hazards due to human error).

7.25. The layout of instrumentation and the means of presenting information to operating personnel, with both an adequate overall summary of the status and performance of the facility and detailed information, where necessary, on the status and performance of particular systems or equipment, should be considered in the design.

7.26. The information displayed in the control rooms should allow operators:

(a) To take specific manually controlled actions for which no automatic control is provided;

(b) To confirm the availability of important safety functions and the performance of automatic safety actions;

(c) To determine the potential for the breach of a fission product barrier or to detect such a breach;

(d) To confirm the performance of safety systems, auxiliary supporting features and other systems necessary for the mitigation of accident conditions or for maintaining safe shutdown;

(e) To determine the magnitude of any releases of radioactive material and to continually assess such releases.

7.27. For a supplementary control room, sufficient instrumentation and control equipment should be available so that the reactor can be placed and maintained in a safe shutdown state, residual heat can be removed, confinement functions can be performed and the essential facility variables can be monitored in the event of a loss of ability to perform essential safety functions from the main control room. The instrumentation and control equipment in the supplementary control room should be physically and electrically separate from the equipment in the main control room.

7.28. The parameters displayed in the supplementary control room may differ from those displayed in the main control room if the supplementary control room does not need to be used to respond to the same range of anticipated operational occurrences and accident conditions as the main control room. In any case, the information available in the supplementary control room or at the emergency control console should be sufficient for putting the facility into a safe condition in, and after, accident conditions, and for mitigating the consequences of the accident.

8. COMPUTER BASED SYSTEMS AND SOFTWARE

GENERAL CONSIDERATIONS

8.1. Computer based systems are of increasing importance to safety in research reactors as their use is increasing in both new and older facilities. Such systems are used both in safety related applications, such as some functions of the process control systems and the monitoring systems, and in safety applications, such as the reactor protection system.

8.2. The reliability of computer based systems should be evaluated with a systematic, fully documented and reviewed engineering process. This process should include the evaluation of new software and operating experience with pre-existing software.

8.3. Since software faults are systematic in nature and not random, potential common mode failure of computer based safety systems employing redundant hardware subsystems using identical copies of the software should be systematically considered.

8.4. Depending on the complexity of experimental devices in the research reactor, consideration should be given to having separate computer based instrumentation and control systems for the reactor and for the experiments. In this way, each system could be provided with its own set of requirements and objectives.

8.5. Obsolescence management should be considered in the design and operation of computer based systems to plan and manage for reductions in service life, diminishing manufacturing sources and material shortages.

COMPUTER BASED SYSTEMS AND SOFTWARE DESIGN CONSIDERATIONS

8.6. For safety systems, complexity should be avoided both in the functionality of the system and in its implementation by complying with a structured design that follows a programming discipline.

8.7. For safety systems, the functional requirements that have to be fulfilled by a computer system should all be essential to the fulfilment of safety functions. Functions not essential to safety should be isolated to avoid any impact on safety functions.

8.8. For applications of computer based systems, 'top-down' decomposition, levels of abstraction and modular structure are important concepts for coping with complexity. The logic behind the system modularization and the definition of interfaces should be made as simple as possible.

8.9. A 'top-down' design process (essentially breaking the system down to gain insight into its subsystems) for the system and its associated software should be used to facilitate the assessment of whether design objectives are being achieved.

8.10. When the use of a computer system involves two or more components that fall into different safety classes, the computer system should meet the requirements of the higher safety class.

8.11. The use of diverse functions and system components at different levels of the design should be considered. The reliability of computer based systems can be enhanced by using diversity to reduce the potential for common cause failures of software. Diversity of methods, languages, tools and personnel should also be taken into consideration. However, although diverse software may provide improved protection against common mode failures of software, coincident errors may still occur. The choice of type of diversity or the decision not to use diversity should be justified at the system design stage.

8.12. System fail-safe features, supervision and fault tolerant mechanisms should be incorporated into the software, but only to the extent that the additional complexity is justified by design basis functional requirements and performance requirements important to facility safety and necessary protection for anticipated operational occurrences and design basis accidents.

8.13. Fault detection and self-supervision features should not adversely affect the ability of a computer system to perform its safety function or cause spurious actuations of the safety function.

8.14. It should be demonstrated that measures have been taken to protect a computer based system throughout its entire life cycle against physical attack, unauthorized access, fraud, computer viruses and other such threats. Safety systems should not be connected to external networks.

8.15. The connections for external storage devices should be locked to prevent unauthorized use.

8.16. A computer based system should be designed for maintainability to facilitate the detection, localization and diagnosis of potential or actual failures so that the system can be repaired or replaced efficiently. Software that has a modular structure may be easier to repair, review and analyse, since the design may be easier to understand. Maintainability of software also includes the concept of making changes to the functionality. The design of a computer based system should allow, as far as practicable, that changes are confined to a small part of the software.

8.17. Computer systems that perform safety functions should have deterministic behaviour with regard to functions and timing.

8.18. Sample rates and processing speed should be consistent with requirements for accuracy and timing.

8.19. Data communications channels important to safety should satisfy the recommendations for independence from one another.

8.20. The design should ensure that errors and failures of transmission equipment and data communications equipment are detected and that suitable alarms are provided for the operators and records are made for the analysis of performance.

8.21. The communications technology should be chosen and should be suitably configured to ensure that it is capable of meeting the requirements for timely response under all possible conditions of data loading.

8.22. Appropriate consideration should be given to the use of redundancy in data communications.

8.23. The topology and network interface of the data communications network should be designed and implemented to avoid common cause failures of independent systems or subsystems.

8.24. Data flow from lower classified to higher classified safety systems should be avoided unless a decoupling device is installed.

8.25. The selection of pre-developed items to be included in the final product should follow a defined and documented process to guarantee their suitability.

8.26. Software tools can be used to support the life cycle of the instrumentation and control systems where benefits result from the use of software tools and where they are available. These tools should be verified and assessed consistently with the reliability requirements, the type of tool and the potential for the software tool to introduce errors.

PROJECT PLANNING

8.27. The project development process should be carefully planned and clear evidence should be provided that the process has been followed to facilitate the independent assessment of systems important to safety.

8.28. The development plan should identify and define the process that will be used on the particular project. Other aspects of the project that should be considered and planned are quality management, verification and validation, configuration management, installation and commissioning.

8.29. All phases of the development process should be identified. The design activity of one phase provides the inputs for the next phase. Verification should be performed across each phase of the development process and before starting the next phase.

8.30. The methods to be used in the development process should be identified. The selection of methods should be related to a description of the quality management programme, in which standards and procedures are established.

8.31. The quality management programme should be prepared and implemented before the project begins. A software quality management plan should be available at the start of the project.

Verification and validation plan

8.32. Verification and validation activities should be performed to demonstrate that the computer system achieves its overall safety requirements and functional requirements. Techniques and explicit validation procedures should be specified in the verification and validation plan.

8.33. Verification and validation planning should include the listing and collection of applicable standards, procedures and conventions that guide the verification process.

8.34. The teams performing verification and validation should be independent of the development team. Independence is usually ensured by having a different line management for the verification and validation teams and for the development teams. A different organization could be used to complete the verification and validation activities.

8.35. The verification and validation plan should include a mechanism for recording all instances of non-compliance found during the analysis and ensuring that they are properly resolved by means of an approved change control process.

Configuration management plan

8.36. All items of software development, such as compilers, development tools, configuration files and operating systems, should be under control for configuration management. All identifiable items, such as documents, components of the software or data structures, should be given a unique identification, including the version number. These items should include both developed items and existing items that are being reused or reapplied.

8.37. A procedure for change control should be established. This procedure should provide for maintaining records of any problems identified during the development process, or during the operation of the research reactor, that required changes. It should also provide for documenting problem analysis, items that were affected, changes that have been made to solve the problems, and which versions (such as version numbers of software or components of software) and which baseline database of systems and components of the instrumentation and control systems were produced in order to resolve the problems.

8.38. The change control procedure should specify responsibilities for approving changes.

Installation and commissioning plan

8.39. The installation and commissioning plan should cover the following:

(a) The sequence of steps for proper integration of the system into the reactor facility and the corresponding facility states necessary for the safe introduction of the new or changed system;

(b) The required interactions with the regulatory body, including approvals, hold points and reports, that should be respected before the system can be put into operation;

(c) The commissioning test cases and sequence and the corresponding facility states necessary to confirm proper functioning of the system in the environmental conditions of the facility;

(d) A description of the records and reports that will be necessary to describe the results of commissioning.

SPECIFICATION OF REQUIREMENTS FOR COMPUTER BASED SYSTEMS

8.40. The specification of requirements for a computer system should specify, as a minimum, the functional and non-functional properties of the computer system that are necessary and sufficient to meet the requirements for the facility.

8.41. Safety analyses (e.g. facility safety analyses, transient analyses and accident analyses, based on postulated initiating events and safety criteria) should be an essential part of specifying functional safety requirements. In addition to safety requirements, some additional requirements not directly associated with safety are included at this stage of the design, such as requirements for reliability and availability.

8.42. A safety analysis should be made for safety systems and safety related systems to determine functional safety requirements.

8.43. Non-functional requirements should specify the following:

(a) The relevant dependability attributes, such as reliability, availability and safety required of the system behaviour;

(b) The security requirements derived from the security policy that has been defined for the environment of the computer based systems, including security procedures;

(c) Performance requirements (e.g. response time of software modules for safety functions);

(d) Environmental qualification requirements, such as temperature and radiation;

(e) Whether and where physical separation is needed (e.g. between safety functions and control functions);

(f) That requirements not directly associated with safety (e.g. requirements for availability or security) will not adversely affect the ability to perform a safety function when required.

8.44. An accurate and clear description of these requirements should be formulated before starting the next stage of the project, and this description should be subject to independent review.

SOFTWARE REQUIREMENTS

8.45. The software requirements should include the description of the allocation of system requirements to software, with attention to safety requirements and potential failure conditions, functional and operational requirements in each mode of operation, performance criteria, timing and constraints, detection of failures, self-supervision, requirements for monitoring of safety and security requirements.

8.46. Wherever safety system settings are configurable by the user, only the authorized user should be allowed to change these settings, and these settings should be checked for their integrity.

SOFTWARE DESIGN

8.47. In the software of systems important to safety, unnecessary complexity should be avoided at all levels of design. The simpler the design is, the easier it is to achieve and demonstrate all other attributes. It also gives greater confidence that the software is fully understood.

8.48. To facilitate the tracing of requirements, each design element, such as a software module, a procedure, a subroutine or a file, should have a unique identifier.

8.49. The design should contain no contradictions and no ambiguities. The description of the interfaces between modules should be complete. In addition to internal interfaces between modules of the software, the design should explicitly specify the external interfaces of the software, such as system calls, hardware interfaces and libraries. The design and its description should demonstrate that each software requirement has been met and should verify that the implementation is correct with respect to the detailed design.

8.50. The documentation on software design should provide technical information on the software architecture and on the detailed design of all software modules and their concurrence, with synchronization to prevent unpredictable results in terms of response time. Relevant constraints on implementation should also be specified.

8.51. Each software module identified in the software architecture should be described in the detailed design.

8.52. Diagrams and flow charts could be used provided that the meaning of the elements of the diagrams is well defined. Common techniques used for describing design should include data flow diagrams, structure diagrams or graphics.

SOFTWARE IMPLEMENTATION

8.53. The production of software code should be verifiable against the software specifications. The code should be readable, adequately commented and understandable. Validated software tools could be used to facilitate the code verification process. The software code could be verified using formal methods.

8.54. Peer review should be conducted at the software design stage to avoid potential errors and to improve software quality.

8.55. A formal system for requesting changes and controlling modifications should be in place at the implementation phase to deal with omissions and inconsistencies. Up to date records of changes should be kept available for reviews and audits.

8.56. The code of each program should be kept simple and easy to understand, both in its general structure and in its details.

8.57. Data structures and their naming conventions should be used uniformly throughout the whole computer based system.

VERIFICATION AND ANALYSIS

8.58. Techniques for verification and analysis should be used to provide assurance of ~~product~~ a software quality.

8.58.a. A software verification plan should be produced that documents:

(a) The verification techniques to be used;

(b) Details of, or references to, the procedures to be used in applying each technique, including its scope and depth;

(c) How non-functional requirements and constraints will be demonstrated to be met;

(d) Criteria for determining when sufficient verification has taken place, including targets for completeness with respect to the outputs of the previous phase and for structural coverage of the functional tests, and how these will be demonstrated;

(e) The means by which results will be recorded;

(f) The means by which non-compliances and faults will be recorded and resolved;

(g) The team or teams performing the verification and their independence from the designers of the software;

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

~~(a)~~(i) The rationale for each of the elements listed in items (a)–(h) above, and justification that the verification will be sufficient for software in the system of the safety class to which it is applied.

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

8.58.c. The code should be reviewed to check for software security vulnerabilities, using automated software tools and complemented by manual review of the critical sections of the code (e.g. input/output handling, exception handling).

8.58.d. All outputs of the I&C system should be monitored during the verification and any deviation from the expected results should be investigated and documented.

8.58.e. Any shortfall in the verification results against the verification plan (e.g. in terms of the test coverage achieved) should be documented and resolved or justified.

8.58.f. Any errors detected should be analysed for cause and should be corrected by means of agreed modification procedures, and regression tested as appropriate, to ensure that previously developed and tested software still performs after a change.

8.58.g. The error analysis should include an evaluation of applicability to other parts of the I&C systems.

8.59. Records of the numbers and types of anomaly should be maintained. These records should be reviewed to determine whether or not any lessons could be learned and appropriate process improvements should be made.

8.60. Techniques such as reviews, inspections or audits should be applied to the verification of all phases in the life cycle of computer based systems. The means by which the verifiers record the results of their reviews should be stated in the verification plan together with a justification of the method used. The verification and validation team should be independent of the development team.

8.61. Review of the documentation on software design and software implementation should be undertaken prior to the design of the software test cases. The test case specifications should be fully documented and reviewed.

8.62. Test plans should be designed to facilitate regression testing by ensuring that tests are repeatable and require minimal human intervention.

8.63. Any anomalies in the performance of testing should be reviewed and, if it is determined that there is a need for a modification to the test procedure, an appropriate procedure for change control should be applied.

8.64. Each anomaly in the software test performance should be documented in a problem report to include the nature of the problem, the identified fix, the retest requirements and ultimate completion of a satisfactory retest. In addition, a cross-reference record of software fixes and software builds should be maintained for configuration management of the installed software.

THIRD PARTY ASSESSMENT

8.65. A third party assessment of safety system software should be conducted concurrently with the software development process.

8.66. The objective of such a third party assessment is to provide a view on the adequacy of the system and its software that is independent of both the supplier of the system and/or software and the operating organization. Such an assessment may be undertaken by the regulatory body or by a body acceptable to the regulatory body.

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

8.68. The assessment should involve an examination of the following:

— The development process (e.g. through quality assurance audits and technical inspections, including examination of life cycle documents, such as plans, software specifications and the full scope of test activities);

— The final software (e.g. through static analysis, inspection, audit and testing), including any subsequent modifications.

COMPUTER SYSTEM INTEGRATION

8.6965. The software version integrated into the computer system should be the latest version to have been verified and validated.

8.7066. The computer system integration phase should encompass at least three sequenced activities: software tests; hardware testing and integration; and hardware–software integration.

8.7167. The hardware–software integration should consist of three parts: loading of all software into the hardware system; testing that the software–hardware interface requirements are satisfied; and testing that all the software can operate in the integrated software–hardware environment.

8.7268. During the verification process of the computer system, evidence should be generated to demonstrate that the system integration has been properly checked and verified.

8.7369. A traceability analysis should be performed and documented as part of the verification activity to demonstrate that the system integration requirements are complete with respect to the design specification for the computer system.

Integrated computer system tests

8.7470. A software test plan should be developed covering all testing to be done, including unit level tests, integration tests, factory acceptance tests and installation tests.

8.7571. The integrated computer system tests should be performed before the system is transferred to the site and installed. The final integrated computer system test is often combined with the factory acceptance test to form a single test activity.

8.7672. In constructing test cases, special consideration should be given to the following:

(a) Coverage of all requirements (including robustness tests and features);

(b) Coverage of the full ranges of values for input signals;

(c) Handling of exceptions (e.g. demonstration of acceptable behaviour when input failure occurs);

(d) Timing related requirements (e.g. response time, input signal scanning and synchronization);

(e) Accuracy;

(f) All interfaces (e.g. the hardware–software interface in system integration and external interfaces during validation);

(g) Stress testing and load testing;

(h) Functionality requirements for security (e.g. logging of user activities);

(i) All modes of operation of the computer system, including transition between modes and recovery after failure of the power supply.

8.7773. A traceability analysis should be performed to demonstrate that the validation requirements (for test or evaluation) are complete with respect to the computer system requirements.

Validation and commissioning tests

8.7874. Validation and commissioning tests should be carried out to verify that the computer system has been connected correctly and to confirm the correct functioning of the system.

8.7975. The validation and commissioning tests should usually be combined with the site acceptance test, which includes verification of the operation of the equipment.

8.8076. Strict configuration control of the computer system (both hardware and software) should be maintained during the commissioning programme. Any changes required in this phase should be subject to a formally documented change process.

8.8177. Sufficient documentation should be produced to demonstrate the adequacy of the commissioning programme for the installed computer based safety system.

Operation, maintenance and modification

8.8278. The following main activities should be considered in the operation, maintenance and modification phases:

(a) Periodic tests, performed to verify that the system is not degrading;

(b) Regression testing because of modifications, performed to enhance

or change the functionality or to correct errors;

(c) Change of operating parameters;

(d) Diagnostic activities, for example the execution of special diagnostic programmes;

(e) Replacement of hardware components because of failures.

8.83. All software tools used in software development, testing, installation, integration, operation and maintenance should be qualified.

8.84. The life cycle of the systems should include the processes for implementing modifications. This life cycle should include the main phases of the development, including verification and validation.

These activities, together with an impact analysis and regression testing, will be necessary to ensure that the modifications have been correctly implemented and no new errors have been introduced.

8.85. After failure of a hardware component, corrective actions should be limited to one by one replacements of hardware and to the reloading of the existing software modules. These actions should not include any modification unless analysis of the failed components reveals a need for modification.

8.86. The failure modes of computer safety and security features and the effects of these failure modes on instrumentation and control functions should be known and documented, and should be considered in a hazard assessment of the system.

9. CONFIGURATION MANAGEMENT

9.1. A full set of documentation reflecting the configuration and status of instrumentation and control systems at the facility should be available prior to the commissioning of the facility. The documentation should be maintained up to date throughout the lifetime of the facility.

9.2. A baseline database of systems and components of the instrumentation and control systems should include the following information:

(a) General information (e.g. system identification, serial number, manufacturer, supplier support, location and safety class);

(b) System summary (e.g. functionality, configuration, impacts of the system on safety, current performance, loss of operational availability in the event of unavailability of the system, interfaces and documentation);

(c) Physical characteristics (e.g. number of cabinets, detailed component inventory and operational limits);

(d) Boundaries (e.g. environmental conditions, power supply, grounding, margins necessary in the cabinets and rooms for power supply and the amount of information exchanged with other systems);

(e) System constraints (e.g. licensing conditions, technical specifications, design constraints and operating characteristics);

(f) Obsolescence issues (e.g. maintenance costs, replacement parts and performance degradation);

(g) Measures for improvements (e.g. functionality, configuration, performance and maintenance); (h) References.

9.3. Operators and maintenance staff should collaborate in the improvement and the updating of documentation on configuration control for instrumentation and control systems. Information of the documentation and database, described in paras 9.1 and 9.2, should be protected according to requirements on security of information.

10. MODIFICATION AND MODERNIZATION OF INSTRUMENTATION AND CONTROL SYSTEMS

10.1. The main reasons to modernize an instrumentation and control system at a given facility are obsolescence of the present instrumentation and control system, the unavailability of spare parts and an increased failure rate of the instrumentation and control system. These developments can lead to frequent reactor shutdowns and long repair periods, resulting in increasing unavailability of the facility. Recommendations and guidance on ageing management for research reactor systems are given in ~~IAEA Safety Standards Series No.~~ SSG-10, ~~Ageing Management for Research Reactors~~ [~~10~~48].

10.2. Additional aspects supporting a decision to modernize are the technological progress in instrumentation and control systems, leading to their greater reliability, improvement of the human–system interface, and extensive and fast data collection and data processing. Besides such technically based decisions, other factors (i.e. new regulatory requirements) may also influence the final decision for modernization of the instrumentation and control system.

10.3. Before entering such a modernization project, information on needs and limitations should be collected using the current instrumentation and control system. Such information from past failures and incidents could be collected by event recording systems used at the facility. Other weaknesses could be identified from regular self-assessment of operational performance, including analysis of even small deviations from normal operation.

10.4. In addition to identifying current problems and limits of the current instrumentation and control system, the decision maker should attempt to foresee and assess possible future problems and limits of the current instrumentation and control system.

10.5. Upgrading and modifying instrumentation and control systems should be performed in accordance with the guidance provided in IAEA Safety Standards Series No. SSG-24, Safety in the Utilization and Modification of Research Reactors ~~[11~~[1~~1~~0], on planning, organizational aspects, safety assessment, implementation and post-implementation aspects, training and documentation of modifications to the facility. Vigorous independent verification and validation should be performed for every change associated with modification and modernization.

10.6. A modification to a reactor system may or may not include a complete replacement of the components of the system. Modifications to existing systems should account for any considerations that were addressed by the original equipment. Typical considerations in designing instrumentation and control systems are discussed in Section 4.

10.7. Modification of instrumentation and control equipment is expected over the lifetime of the facility. Regardless of the reason, consideration should be given to the function of the equipment being modified, for example in changing from one technology to another (e.g. in changing from an analogue

system to a digital system or in the event of obsolescence of the existing instrumentation and control system leading to a lack of spare parts).

10.8. When a decision is made to implement a modification to existing instrumentation and control equipment, the possible effects on reactor safety should be considered and assessed.

10.9. Special attention is necessary to verify that every modification has been properly assessed, documented and reported in terms of its potential effects on safety, and that the reactor is not restarted without formal approval after the completion of modifications to instrumentation and control systems.

10.10. The design documentation for older legacy 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. A full set of documentation reflecting the present states of the instrumentation and control systems at the facility should be made available.

10.11. A process of verification and updating of the existing documentation should be undertaken prior to commencing any activities for modernization. Operators and maintenance staff should collaborate on the updating of existing documentation to ensure that all modernization activities are completely captured in the documentation on configuration control for the instrumentation and control systems.

10.12. A baseline database of systems and components of the existing instrumentation and control systems should be updated or should be created following the recommendations of para. 9.2.

10.13. Verification and updating of existing documentation should start at a high level functional description of the instrumentation and control system architecture, preferably in the form of a diagrammatic representation with an accompanying list of all instrumentation and control systems.

10.14. A designated designer should be responsible for the activities for design, integration, documentation and maintenance as well as for training facility personnel in the use of the new equipment. ~~Reference~~ Ref. [~~12~~1219] provides details on the responsibilities that the designated designer should assume.

10.15. In modifications to any instrumentation and control system, the duties and the responsibilities of the operating personnel (i.e. the operators as well as the maintenance staff, the experimenters and personnel with responsibilities in an emergency) should be taken into consideration so as to achieve an effective interface between the operating personnel and the research reactor systems.

10.16. The effects of modifications on the interactions of personnel of the facility with the research reactor systems should be taken into consideration. Particular requirements for the operating personnel should be taken into account from the early stages of the project (see Section 7 for details on considerations of human factors).

10.17. The reliability of the new or modified equipment should be taken into consideration, as well as the effects of the modification on overall system reliability. Performance of a qualitative analysis (e.g. analysis of failure modes and their effects) may be helpful in determining which parts of the system may be affected by the modifications and what are the implications for the ability of the system to perform its safety function.

10.18. In modifying an existing safety system, the effect on the implementation of defence in depth should be considered.

10.19. Safety systems are required to be independent, as far as practicable, of other reactor systems. In modifying an instrumentation and control system, the development of design guidelines should be considered.

10.20. In modifying any system, the complexity of the modification generally plays a major role in the difficulty of analysing the effects on the overall system. In particular, careful consideration should be given to the addition of any new functions and to the ability to expand the capabilities of the existing safety systems in the future.

10.21. The requirement for qualification of modifications of the system for the expected environmental conditions of the system should be considered. Modifications should be qualified for the service conditions (including operational environment), and the qualification programme should be based on the safety analysis of the proposed modifications.

10.22. Procedures for change control should be put in place, including appropriate procedures and organizational structures for the review and approval of the safety aspects of the modification.

10.23. The following should be considered in the design of upgrades and modifications for instrumentation and control systems:

(a) The limitations due to the physical characteristics of the installed facility, which effectively restrict the design options for instrumentation and control systems;

(b) The possible need to maintain consistency between the design of replacement equipment and that of existing instrumentation and control equipment (e.g. to reduce the complexity of the overall operator interface and the maintenance tasks of the facility);

(c) Practical considerations with regard to the equipment or technology commercially available when required according to the project programme and the prospects for securing technical support for such equipment and technology by manufacturers or third parties for the installed life of the equipment.

10.24. The benefits of changes should be weighed against potential negative consequences for safety, and this assessment should be documented as part of the justification for the changes. For instance,

enhancements to the operator interface features might lead to increases in the number of errors made by operators and maintenance staff for some time after the change.

10.25. As required, sufficient and appropriate training programmes should be developed and implemented to minimize or to eliminate the potential for such errors, if modifications are made.

10.26. The consequences of updating or changing a software tool may be significant and should be subject to an impact assessment (e.g. the upgrade of a compiler could invalidate the results of previous analysis or verification concerning the adequacy of the compiler).

10.27. Installation of equipment should be performed by qualified personnel under the supervision of the designer and with the authorization of the reactor manager.

10.28. Once complete, and before startup of the research reactor, the installation should be functionally tested following the recommendations of SSG-10 [~~10~~48].

10.29. When an instrumentation and control system is modified or is part of an upgrade, the level of rigour applied in justifying and executing the change should be established on the basis of the role and function of the system in ensuring the safety of the facility, in association with the existing systems and with any systems that will remain in operation after the modification or the upgrade. This also applies to software based systems.

10.30. When an instrumentation and control system is replaced, the new instrumentation and control system may, where appropriate, be run in parallel with the old system for a probationary period, until sufficient confidence has been gained in the adequacy of the new system. In this configuration, only the previous instrumentation system should be able to control the reactor. Meanwhile, the response of the drivers of the new instrumentation and control system should be registered in an independent acquisition system to provide the possibility to assess and compare their responses against the responses of the previous system.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Safety Standards Series No. SSR-3, IAEA, Vienna (2016).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Commissioning of Research Reactors, IAEA Safety Standards Series No. DS509A, IAEA, Vienna (in preparation; revision of NS-G-4.1).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Periodic Testing and Inspection of Research Reactors, IAEA Safety Standards Series No. DS509B, IAEA, Vienna (in preparation; revision of NS-G-4.2).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Management and Fuel Handling for Research Reactors, IAEA Safety Standards Series No. DS509C, IAEA, Vienna (in preparation; revision of NS-G-4.3).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Research Reactors, IAEA Safety Standards Series No. DS509D, IAEA, Vienna (in preparation; revision of NS-G-4.4).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, The Operating Organization and the Recruitment, Training and Qualification of Personnel for Research Reactors, IAEA Safety Standards Series No. DS509E, IAEA, Vienna (in preparation; revision of NS-G-4.5).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and Radioactive Waste Management in the Design and Operation of Research Reactors, IAEA Safety Standards Series No. DS509F, IAEA, Vienna (in preparation; revision of NS-G-4.6).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management for Research Reactors, IAEA Safety Standards Series No. DS509G, IAEA, Vienna (in preparation; revision of SSG-10).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report, Safety Standards Series SSG-20, IAEA, Vienna (2012). (A revision of this publication is in preparation.)

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety in the Utilization and Modification of Research Reactors, Safety Standards Series No. SSG-24, IAEA, Vienna (2012). (A revision of this publication is in preparation.)

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2019).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series No. SSG-22, IAEA, Vienna (2012). (A revision of this publication is in preparation.)

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series No. SSG-22, IAEA, Vienna (2012).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. NSS 33-T, IAEA, Vienna (2018).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Periodic Testing and Inspection of Research Reactors, IAEA Safety Standards Series No. NS-G-4.2, IAEA, Vienna (2006).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[19] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, INSAG-19, IAEA, Vienna (2003).

ANNEX

INSTRUMENTATION AND CONTROL SYSTEMS THAT CAN BE USED IN A RESEARCH REACTOR

General

A–1. The instrumentation and control systems of a research reactor involve many systems that may differ depending on the type of reactor, the purpose and its modes of operation. Usually, it would include those systems identified in Section 2 as examples of instrumentation and control systems. ~~Typical sets of instrumentation and control systems and their interrelations are shown in Fig. A–1.~~

A–2. This Annex identifies instrumentation and control systems, and relevant architecture, that can be used in a research reactor. Some of these instrumentation and control systems might not be used in a particular research reactor if they are not required for that specific type of installation.

A-3. ~~The i~~Instrumentation and control systems can ~~should~~ be designed in a 'top-down' architecture (see Fig. ~~2~~A-1) having different levels of monitoring, processing, acquisition and actuation, sensors and actuator drivers. The 'top-down' hierarchy architecture for the instrumentation and control systems requires the inclusion of three independent levels of communication to provide interfaces for communication between the different architectural levels and the reactor systems and facility systems, namely:

(a) Supervision level of communication;

(b) Control level of communication;

(c) Field level of communication.

These features should be used in the design of the different architectural levels to reduce the likelihood of dependent failures at these levels.

~~The monitoring functions should be allocated at the supervision level; the calculation, algorithms, and safety and process functions should be allocated at the control level; the acquisition and actuation functions should be allocated at the field level; and sensors and actuator drivers should be located at the facility level.~~

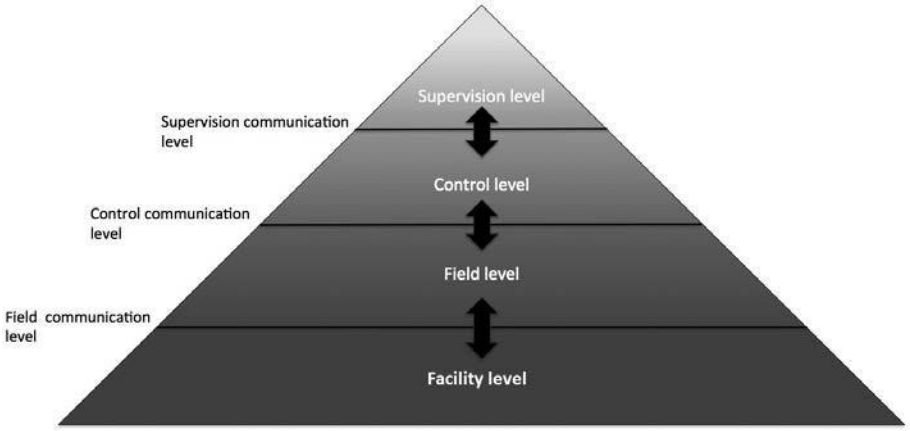


FIG. A-12. 'Top-down' architecture of the instrumentation and control systems.

A-4. In this architecture the monitoring functions are normally located at the supervision level; the calculation, algorithms, and safety and process functions are located at the control level; the acquisition and actuation functions are located at the field level; and sensors and actuator drivers are located at the facility level.

~~The 'top-down' hierarchy architecture for the instrumentation and control systems requires the inclusion of three independent levels of communication to provide interfaces for communication between the different architectural levels and the reactor systems and facility systems, namely:~~

~~(a) Supervision level of communication; (b) Control level of communication; (c) Field level of communication.~~

~~3.20. The features mentioned in para. 3.19 should be used in the design of the different architectural levels to reduce the likelihood of dependent failures at these levels.~~

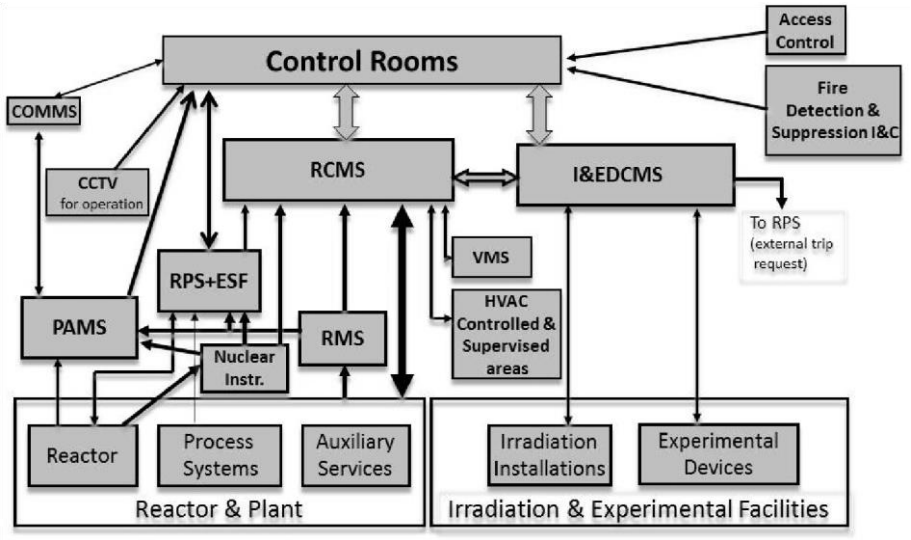
A-5. Typical sets of instrumentation and control systems and their interrelations are shown in Fig. A–2.

DESCRIPTION OF THE MAIN INSTRUMENTATION AND CONTROL SYSTEMS

Reactor protection system

A–6~~3~~. The reactor protection system is a set of components designed to monitor reactor operation parameters (e.g. neutron power and period, coolant flow rate, inlet and outlet temperatures and pressure drop in the reactor core), compare them with safety system settings and automatically initiate action of the reactor shutdown system when the parameters reach or exceed the safety system settings. Each parameter could be measured by two or more independent channels. The automatic actions are initiated on the basis that the logic arrangement for the initiation of protective actions complies with the single failure criterion. When three independent channels are available, the logic arrangement of two out of three channels could be used to prevent the initiation of protective actions by spurious signals. A reactor protection system could also be actuated manually by the operator, by the experimenters or by the control

and monitoring system for irradiation and experimental devices. A trip of the reactor protection system results in the shutdown of the reactor.



Note: CCTV — closed circuit television; COMMS — communication system;

ESF — instrumentation and control for initiation of other engineering safety features; HVAC — heating, ventilation and air-conditioning for controlled and supervised areas; I&C — instrumentation and control; I&EDCMS — control and monitoring system for irradiation facilities and experimental devices; Instr. — instrumentation; PAMS — postaccident monitoring system; RCMS — reactor control and monitoring system; RMS — radiation monitoring system; RPS — reactor protection system; VMS — vibration monitoring system.

FIG. A–~~1~~2. Research reactor instrumentation and control system.

Instrumentation and control system for the initiation of other engineering safety features

A–~~4~~7. The instrumentation and control system for the initiation of engineering safety features is a set of components designed to initiate, upon request, action of the emergency core cooling system, the decay heat removal system, the confinement isolation system and the confinement heat removal system. The system could also be actuated manually by the operator. A trip in the engineering safety features results in the initiation of one or more of the actions mentioned above. The functions of the engineering safety features could be included in the reactor protection system.

Post-accident monitoring system

A–~~8~~5. A post-accident monitoring system is an important feature of nuclear facilities. Its purpose is to provide the operators and their backup teams with information necessary for the purposes of accident management and to ensure that this information is, and remains, reliable. Under accident conditions, the operators require information in order:

(a) To perform those preplanned manual control actions for which no automatic control system is provided and which are necessary to prevent or to mitigate the consequences of the accident. Such

actions, specified in the safety analysis report, are compiled in the accident management procedures.

(b) To determine whether important safety functions relating to reactivity control, core cooling, integrity of the reactor coolant system, the heat sink, containment integrity and surveillance for radioactivity are challenged, and whether they are being accomplished by the reactor protection system, the engineered safety features and their essential support systems.

~~(b)~~(c) To relay information to, and to communicate effectively with, emergency response facilities on the site.

Nuclear instrumentation

A–~~9~~6. The nuclear instrumentation follows the value and evolution of the neutron flux of the reactor in all its operational states, since this parameter is of the highest relevance to ensuring the safe operation of the reactor. The nuclear instrumentation also provides the means to establish a suitable control strategy for starting up the reactor and keeping it in stable operation at different power levels.

Reactor control and monitoring system

A–10~~7~~. The process instrumentation (detectors, sensors and switches), which measure process parameters and the actual state (position) of actuators, and which are connected to the reactor control and monitoring system, reside at the lowest level of the instrumentation and control systems.

A–~~8~~11. The reactor control and monitoring system is intended for the reliable monitoring of the performance and the safe operation of the reactor. The reactor control and monitoring system provides startup and automatic adjustment of power, compensates for fuel burnup and provides interlocks for safe operation. The reactor control and monitoring system is built using fail-safe and redundant devices to receive and process signals from a large number of sensors, actuate the corresponding control drivers and present information on the reactor's status for the operator at the main control console of the reactor (main human– machine interface).

Radiation monitoring system

A–~~9~~12. The radiation monitoring system is designed for continuous radiation monitoring of nuclear facilities as well as of surrounding areas for detecting the possible release of radioactive material. Such releases may arise owing to failures of technical equipment, loss of integrity of protective barriers, loss of effectiveness of water purification systems, loss of confinement isolation, and failure of filters and ventilation systems, among the most relevant systems and components.

HEATING, VENTILATION AND AIR-CONDITIONING SYSTEM

A–1~~0~~3. Heating, ventilation and air-conditioning systems are used to ensure and maintain adequate environmental conditions for both personnel and equipment by providing temperature control and air quality control. The ventilation system also helps in maintaining the radiological conditions by means

of pressure gradients and the use of appropriate filters, for example. Modern electronic equipment generates much less heat than older types. Nevertheless, excess temperature can degrade performance. Air-conditioning, as a means of removing excess heat from instrumentation and control systems that are safety systems, needs to meet the requirements specified for safety system support features. In regions with a tropical climate or high levels of humidity, the proper design of ventilation systems (with physical separation, redundancy and a closed cycle) may be the only way to eliminate a source of potential common mode failure in instrumentation and control equipment. In some facilities, the reactor control and monitoring system has the capability to send commands remotely to the heating, ventilation and air-conditioning systems (i.e. a command for the remote trip of the emergency ventilation system).

VIBRATION MONITORING SYSTEM

A–141. The vibration monitoring system provides a means of monitoring and detecting abnormal vibration conditions on the main rotary equipment of the reactor. The reactor control and monitoring system is used to transmit information from the vibration monitoring system to the control room.

CONTROL ROOMS

A–152. Sufficient controls, indications, alarms and displays are provided in main control room to initiate, supervise and monitor normal reactor operation and reactor shutdown to a safe state and to provide assurance that a safe state has been reached and is being maintained.

A–163. The minimum set-up of the main control room, including the human– machine interfaces, has to consider the operator's needs to do the following:

(a) To operate the reactor safely in all its operational states;

(b) To monitor the safe operation of the reactor;

(c) To monitor the appearance of alarms;

(d) To perform and confirm a controlled shutdown;

(e) To actuate safety related systems;

(f) To perform and confirm a reactor trip;

(g) To perform and confirm the actuation of the engineering safety features;

(h) To monitor the status of fission product barriers;

(i) To keep the reactor in a safe shutdown mode; (j) To implement emergency operating procedures.

A–174. The alarm annunciators show the status of systems. Safety systems have audible and visual alarms on the operator's control console or control panel to provide a warning of any violation of the operational limits and conditions for safe operation. Operators can access all signals through the main

control console of the reactor control and monitoring system. Control consoles and displays for the irradiation facilities and experimental devices are usually located in the main control room.

A–185. The supplementary control room, where applicable, provides a possibility for remote shutdown of the reactor in the event that this cannot be done from the main control room. Sufficient controls, indications, alarms and displays need to be provided in the supplementary control room to be able to initiate, supervise and monitor a reactor shutdown to a safe state and to provide assurance that a safe state has been reached and is being maintained.

CONTROL AND MONITORING SYSTEM FOR IRRADIATION FACILITIES AND EXPERIMENTAL DEVICES

A–196. The primary use of a research reactor is for the production of neutrons, for research purposes and for the neutron irradiation of materials. Irradiation facilities include the equipment that is used to place, move and arrange samples. A dedicated and tailored instrumentation and control system is designed to control and monitor these operations. Irradiation facilities and experimental devices may have an impact on the safe operation of the research reactor. The parameters of the experimental devices that affect the safety of the reactor need to be displayed in the main control room. Trip signals from the control and monitoring system for irradiation facilities and experimental devices to the reactor protection system could also be provided as indicated by the safety analysis.

COMMUNICATION SYSTEM

A–2017. Communication systems are the link between the operators of the main control room and supplementary control rooms, the reactor hall and the process areas, the staff for the irradiation facilities and experimental devices and for other internal locations (e.g. alarm stations) within the facility, and for off-site response organizations. A voice announcement system is used for making announcements that can be heard by all personnel on the site and in the facility or to report an emergency or unforeseen circumstances requiring an immediate response.

CLOSED CIRCUIT TELEVISION

A–1821. Closed circuit television is a useful aid that allows the operator to monitor and supervise relevant operational or maintenance tasks or activities that are being executed by the operating personnel of the reactor and can be used for monitoring the security status of the facility.

INSTRUMENTATION AND CONTROL SYSTEMS FOR THE DETECTION AND SUPPRESSION OF FIRES

A–1922. The instrumentation and control system for the detection and suppression of fires is an independent system that has the capability to detect a fire at the facility and thereupon to initiate automatic fire suppression systems in the affected areas. Fire detection panels need to be located in the control rooms to provide the reactor operators with relevant information.

ACCESS CONTROL SYSTEM

A–~~20~~23. The access control system is part of the physical protection system and has the capability to supervise and manage the movement of the personnel at the facility. Access control panels may be located in the control rooms and/or in the central alarm stations to provide the reactor operators with relevant information.

CONTRIBUTORS TO DRAFTING AND REVIEW

Abou Yehia, H.	International Atomic Energy Agency
Böck, H.	Institute of Atomic and Subatomic Physics, Austria
Boogaard, J.	International Atomic Energy Agency
Busto, A.	International Atomic Energy Agency
D'Arcy, A.	Consultant, South Africa
Diakov, O.	International Atomic Energy Agency
Drexler, J.	INVAP, Argentina
Du Bruyn, J.F.	NECSA, South Africa
Hardesty, D.	Nuclear Regulatory Commission, United States of America
Hargitai, T.	International Atomic Energy Agency
Hirshfeld, H.	Israel Atomic Energy Commission, Israel
Johnson, G.	International Atomic Energy Agency
Kennedy, W.	International Atomic Energy Agency
Kim Hyung, K.	Korea Atomic Energy Research Institute, Republic of Korea
Lokantsev, A.	SNIIP, Russian Federation
McIvor, A.	International Atomic Energy Agency
Morris, C.	International Atomic Energy Agency

Muhlheim, M.D.	Nuclear Science and Technology Division, Oak Ridge National Laboratory, United States of America
Perrin, C.D.	Autoridad Regulatoria Nuclear, Argentina
Rao, D.V.H.	International Atomic Energy Agency
Rodriguez, L.	AREVA, France
Sears, D. F.	International Atomic Energy Agency
Shim, S.	International Atomic Energy Agency
Shirley, A.	Thermo Fisher Scientific, United States of America
Shokr, A.M.	International Atomic Energy Agency
Sumanth, P.	Bhabha Atomic Research Centre, India
Waard, J.	Nuclear Research and Consultancy Group, Netherlands
Winfield, D.	International Atomic Energy Agency