DS436 Draft 6~~5~~

Date: ~~19 Aug 2013~~9-Oct-2013

IAEA SAFETY STANDARDS

for protecting people and the environment

Status: SPESS Step 11

Member States comments incorporated,
NUSSC Members comments incorporated

Instrumentation and Control and Software Important to Safety for Research Reactors

DRAFT SAFETY GUIDE
DS 436

New Safety Guide

IAEA

International Atomic Energy Agency

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides.**

Safety Fundamentals (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

www.iaea.org/ns/coordinet

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related sales publications are the **Technical Reports Series,** the **Radiological Assessment Reports Series** and the **INSAG Series**. The IAEA also issues reports on radiological accidents and other special sales publications. Unprized safety related publications are issued in the **TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series,** the **IAEA Services Series** and the **Computer Manual Series**, and as **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**.

FOREWORD

This page has been left blank intentionally.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1 This safety guide supplements and elaborates upon the safety requirements for design and operation of the instrumentation and control system for research reactors that are established in Section 6 and 7 of Ref. [1].

1.2 During the lifetime of a research reactor one or more refurbishments of instrumentation and control system can be predicted. Different reasons are demanding instrumentation and control modernization projects such as obsolescence or ageing, improvement of maintainability and reliability, reactor reconstruction and upgrading, new utilization or experiments in research reactors and enhancement of safety.

OBJECTIVE

1.3 The objective of this safety guide is to provide guidance on the instrumentation and control systems important to safety of research reactors including instrumentation and control architecture and associated components, from the sensors to the actuators, operator interfaces and auxiliary equipment. This safety guide is intended for use by all organizations involved in the design and operation of research reactors including the operating organization, the regulatory body, instrumentation and control system suppliers and other organizations involved in a research reactor project.

SCOPE

1.4 This safety guide provides guidance on the safety classification, design, implementation, qualification and operation of instrumentation and control systems important to safety for research reactors to achieve compliance with Ref. [1]. This guide also addresses safety and security interface issues.

1.5 The guidance applies to both, the design and configuration management of instrumentation and control systems for new research reactors, and to the modernization of the instrumentation and control of existing facilities.

1.6 This safety guide also provides recommendations for human factor engineering and human-machine interface and for computer based systems and software for use in instrumentation and control systems important to safety.

STRUCTURE

Section 2 discusses the identification of instrumentation and control functions and systems, the method and the basis of safety classification into safety and safety related functions and systems. Section 3 describes how instrumentation and control systems are arranged into a hierarchy. Section 4 and 5 gives an overview of general and specific design requirements of instrumentation and control systems, while section 7 expands on the guidance given in section 4 in the area of human-system interfaces. The operation aspects of instrumentation and control systems are presented in section 6. Section 8 provides guidance on design, and other

aspects of computer based systems and software. Section 9 deals with instrumentation and control systems configuration management. Section 10 presents the modification and modernization aspects of instrumentation and control systems.

2. SAFETY CLASSIFICATION OF INSTRUMENTATION AND CONTROL SYSTEMS

GENERAL CONSIDERATIONS

2.1 Instrumentation and control functions, systems, and components may be classified to fit into one of two categories: items important to safety or items not important to safety (see Fig.1).

Functions, systems, and components important to safety are those which contribute to:

i. Safely shut down the reactor and maintain it in a safe shutdown condition during and after operational states and accident conditions;

ii. Remove residual heat from the reactor core after shutdown, in all operational states and accident conditions;

iii. Prevent or reduce the potential for the release of radioactive material and ensure that any releases are within prescribed limits in all operational states and within acceptable limits during and after accidents;

iv. Permit the safe operation of the reactor.

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 reactor safety.

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

- Safety systems consist of the protection system, the safety actuation systems and the safety system support features.
- Safety related systems are systems important to safety performing other safety functions not mentioned above, such as monitoring the availability of safety systems.

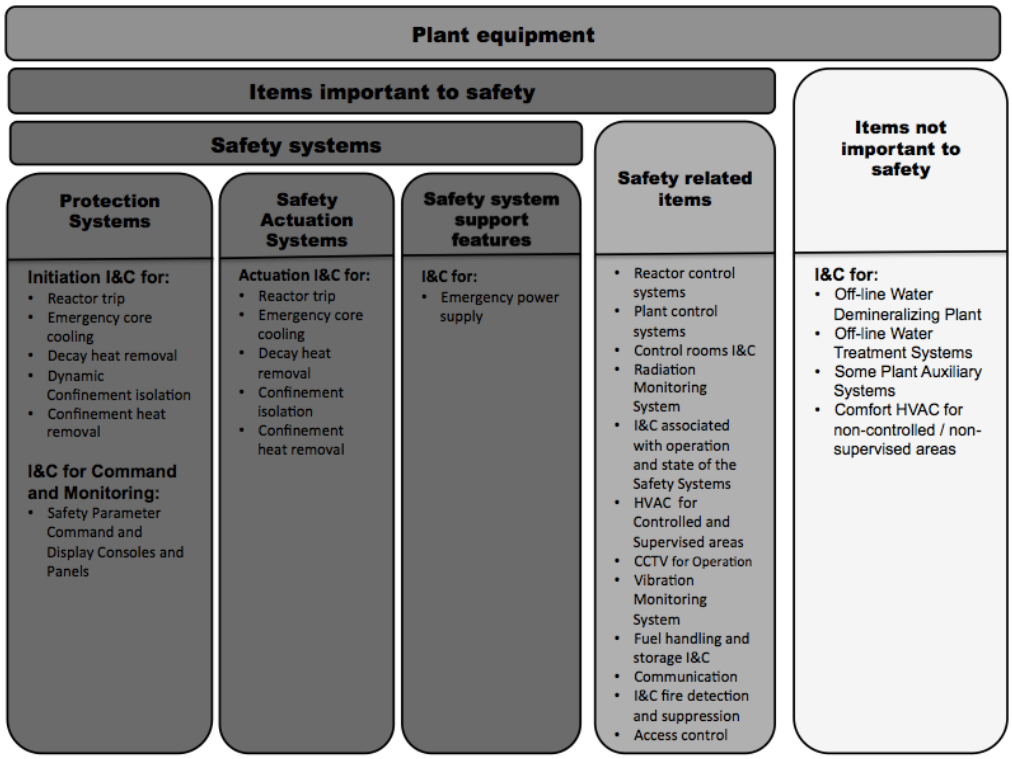

FIG. 1: Examples of instrumentation and control systems of a research reactor classified in connection to their importance to safety. See also Annex I.

2.4 For instrumentation and control systems important to safety, a graded approach to the application of requirements of Ref. [1] can 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 paragraph 1.14 of Ref. [1]). Additional guidance on the application of a graded approach can be found in Ref. [2].

METHOD OF CLASSIFICATION

2.5 The method for classifying the safety significance of a structure, system or component should be based primarily on deterministic methods and engineering judgment, complemented where appropriate by available probabilistic safety assessment. For instrumentation and control systems the basis for such classification should consider:

- The safety function(s) to be performed by the instrumentation and control system;
- The consequences of the instrumentation and control system's failure (failure or faulty performance of the function(s)). This includes potential of the instrumentation and control system itself to cause a postulated initiating event (i.e. the instrumentation and control system's fail-safe modes) and the combination of the probability and consequences of such a postulated initiating event (i.e. frequency of failure and radiological consequences);

- The estimated frequency or probability (if available) that the instrumentation and control system will be called upon to perform a safety function; and
- 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.~~, the potential of the instrumentation and control system itself to cause a postulated initiating event (i.e. the instrumentation and control system's fail-safe modes) and the combination of the probability and consequences of such a postulated initiating event (i.e. frequency of failure and radiological consequences).~~

2.6 The instrumentation and control functions needed to mitigate consequences of design extension conditions could be assigned to a lower safety class than functions needed to control anticipated operational occurrences and design basis accidents to reach a controlled state.

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

2.7 All instrumentation and control systems and equipment should be designed, constructed, commissioned, operated and maintained in such a way that their specification, verification and validation process, 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

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

2.9 The safety class of the instrumentation and control system should have the same safety class as the system or equipment 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 safety of the facility during normal operation, including shut down, refueling, maintenance, and accident conditions. In particular, instrumentation and control systems should ~~en~~be able to automatically initiate[1] reactor shutdown, emergency core cooling, residual heat removal, and the confinement of radioactive

[1] Manual operator action is permitted according to paragraph 5.14

materials. The architectural design of the instrumentation and control systems should provide sufficient capabilities to cover all anticipated operational occurrences and post-event conditions.

3.2 Instrumentation and control system architecture should fulfill safety objectives and design requirements described in paragraphs 2.2 to 2.7; 6.1 to 6.43; 6.61 to 6.65; 6.94 to 6.105 and 6.136 to 6.144 of Ref. [1]. Instrumentation and control system architecture should support all instrumentation and control functions needed to ensure the safety of the facility.

3.3 The overall 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 with the facility operators and users. Modern instrumentation and control systems are more highly integrated than were the past generations. The architecture of highly integrated systems should be carefully considered to ensure proper implementation of the defence in depth concept. A well designed architecture 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. They are shown and described in Annex I.

DEFENCE IN DEPTH

3.4 As it is stated in Ref. [1], paragraph 2.5 "*...the 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 human action within the installation, and events that originate outside the installation*".

3.5 The instrumentation and control system design should incorporate the defence in depth concept. The levels of defence should be independent as far as is practicable. See also Ref. [36].

3.6 The overall instrumentation and control architecture should:

- 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 instrumentation and control functions designed to respond first.
- Not compromise the defence in depth strategy of the facility design.

INDEPENDENCE

3.7 The independence is intended to prevent the propagation of failures from the item affected by the failure to other redundancies, or from a one system to other systems independent of~~ly to~~ the safety class that they belong.

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

3.9 Safety systems should be independent from systems of lower safety classification as far as practicable 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 those 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 or components due to a single event or cause. Common cause failure might happen, for example, because of human errors, errors in the manufacturing process, inadequate specification, qualification for, or protection against internal or external hazards, high voltages, data errors, data communication errors, or failure propagation between systems or components.

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

3.13 An analysis should be done of the consequences of each postulated initiating event within the scope of safety analysis in combination with common cause failures that will prevent a protection system from performing the needed safety functions.~~The consequences of a postulated initiating event in combination with a common cause failure that prevents necessary safety system response to the postulated initiating event should be not greater than those tolerated for design basis accidents. The accident sequences and consequences resulting from the combination of a postulated initiating event and common cause failure of the safety systems may be analysed using best estimate methods. Often it is necessary to provide a diverse actuation system to limit the consequences of the postulated initiating event in conjunction with common cause failure in one or more safety system functions.~~

3.14 The design of ~~equipment~~ system and component 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, electrical and functional isolation have to be applied to achieve the necessary reliability.

OVERALL ARCHITECTURAL DESIGN OF THE INSTRUMENTATION AND CONTROL SYSTEM

3.15 The overall instrumentation and control architecture should:

- Provide all instrumentation and control functions needed to ensure the safe operation of the facility and manage anticipated operational occurrences and accident conditions;
- Provide systems necessary to support the defense in depth strategy of the facility;
- 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);
- 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;
- Divide the overall instrumentation and control system into individual systems as necessary to:
    a) Fulfill design basis requirements for independence between functions in different levels of the defense in depth concept;
    b) Adequately separate systems and functions of different safety classes;
    c) Establish the redundancy needed to fulfill design basis reliability requirements;
    d) Support the compliance of safety systems with the single failure and fail safe criteria;
    e) Provide necessary information and operator controls in the main control room and supplementary control room (if applicable); and
    f) Provide automatic controls necessary to maintain and limit the process variables important to safety within the specified normal operational ranges.
- Define the interfaces between the individual instrumentation and control systems; and
- 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 in the life cycle of the reactor.

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

a) The defence in-depth concepts of the facility;
b) The groups of functions to be provided to address postulated initiating event sequences;
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 principles between automatically and manually initiated actions;

h) National requirements including those for instrumentation and control licensing; and

i) Research reactor operating organization requirements with respect to operational features (i.e., the instrumentation and control design as it affects the interface with facility operators) for systems important to safety.

3.17 The instrumentation and control systems should be architecturally designed in a top-down approach (see Figure 3.1) having different monitoring, processing, acquisition/actuation and sensor/actuator driver levels. The monitoring functions should be allocated at the supervision level; the calculation, algorithms, safety and process functions should be located 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 The use of diversity, redundancy, and independence (i.e. physical separation, electrical and functional isolation)~~,~~ in the overall architectural design of the instrumentation and control system, should be consistent with the safety classification of each instrumentation and control system and the defence in depth concept, both for the overall facility and for the instrumentation and control system. In case of redundancy, other factors such as reliability (i.e. probability of failure on demand) or availability of instrumentation and control systems should be considered.

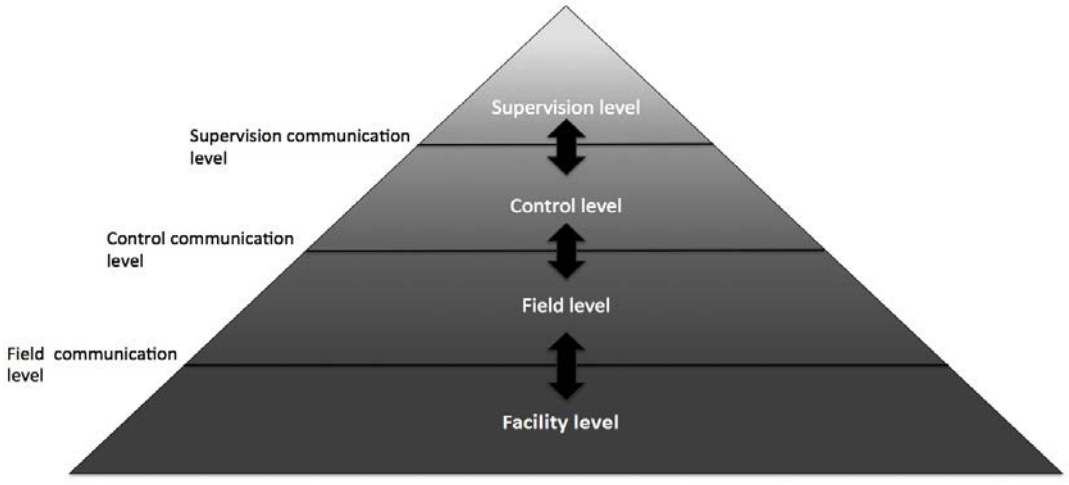

Figure 3.1: Top-down architectural approach design

3.19 The ~~instrumentation and control system~~ top-down hierarchy architecture of the instrumentation and control system ~~approach~~ requires the inclusion of three independent communication levels namely:

a) Supervision communication level;

b) Control communication level; and

c) Field communication level

to establish a communication interface between the different architectural levels and the reactor and facility systems.

3.20 The use of the same ~~features~~ levels (~~those mentioned in~~refer to 3.19) should be applied in the design of the different architectural levels to reduce the probability of dependant failures of the levels.

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

4. DESIGN GUIDELINES

GENERAL

4.1 Instrumentation and control systems should fully implement the requirements of their design bases. The origin of and the ~~rationale~~ objective for every requirement should be defined and documented, to facilitate verification, 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 achieve its imparted goals. Simplicity leads to fewer components, simpler interfaces, easier verification and validation and easier maintenance for the hardware and software. Adequate analysis of the design requirements is an effective means to achieve design simplicity.

~~4.3 Provisions to strengthen safety culture should be considered in the design and implementation of the instrumentation and control system.~~

DESIGN BASIS

~~4.4~~4.3 Each research reactor instrumentation and control system important to safety should have design basis that specify the ~~following~~:

a) F~~The f~~acility states (operational states and accident conditions) in which the system is required;

b) ~~The v~~Various facility and experimental configurations that the instrumentation and control system must accommodate;

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

d) Performance requirements including the guaranteed response time for safety functions;

e) Facility conditions during which manual control is allowed f~~F~~or each manual protective action ~~the facility conditions during which manual control is allowed~~;

f) Postulated initiating events to which the system must respond;

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

h) R~~The r~~anges, rate of change, required accuracy of input and output signals of the system;

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

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

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

l) System availability requirements;

m) R~~The r~~ange of transient and steady state environmental conditions under which the system is required to perform functions important to safety;

n) R~~The r~~ange of environmental conditions, including those arising from natural phenomena hazards 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 the capability;

p) ~~To serve the w~~Whole life cycle of the facility including accident and post-accident conditions; and~~.~~

q) Security regulatory requirements and operational constraints.~~;~~

~~4.5~~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 report;

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

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

DESIGN CRITERIA

DESIGN FOR RELIABILITY

~~4.6~~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 single failure criterion

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

4.7 The single failure criterion is a deterministic method to determine the necessary degree of redundancy for items important to safety and it should be applied.

~~4.7~~

4.8 The design should ensure, on the basis of analysis that the redundancy will provide a backup to assure that no single failure could result in a loss of the capability of a system to perform its intended safety function.

~~4.8~~4.9 The principle of redundancy should be considered as the provision of alternative (identical or diverse) structure, system or components, such that any of them can perform the required function regardless of the state of operation or failure of any other structure, system or components performing the function. The principle of redundancy is an important design principle for improving the safety and reliability of systems important to safety.

~~4.9 The single failure approach is a deterministic method to determine the necessary degree of redundancy for items important to safety and it should be applied.~~

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

~~4.11 The design should ensure, on the basis of analysis that the redundancy will provide a backup to assure that no single failure could result in a loss of the capability of a system to perform its intended safety function. The design of instrumentation and control systems important to safety should include provisions for detecting all postulated (identified) failure modes in the system by, preferably a combination of failure alarms, testing the credibility of readings, as appropriate. This is usually in addition to periodic testing to demonstrate system performance.~~

~~4.12~~4.11 Instrumentation and control systems important to safety have a critical role 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 safety systems the single failure criterion should be applied so that the system is capable of performing its intended safety function in the presence of any single failure. A single failure in the system should be considered along with: a) failures as a consequence of postulated initiating events and b) any credible and undetected fault in the system.

Formatiert: Einzug: Links: 1,2 cm, Keine Aufzählungen oder Nummerierungen

4.134.12 The degree of redundancy should depend upon 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 reliability and availability requirements of the design basis. For instrumentation and control safety systems redundancy should also be applied to the extent needed to comply with the single failure criterion when equipment is removed from service for planned surveillance or testing.

Common cause failure

4.144.13 The design of instrumentation and control system important to safety should minimize the possibility of common cause failures by applying principles of independence, and diversity. ~~Especially, s~~Safety systems should be designed in such a way that common cause failures are prevented or mitigated.

4.154.14 As far as practicable, redundant safety systems should be physically and electrically separated from each other and from systems of lower safety classification. Moreover, the principle of independence should be used for the entire safety system e.g. between redundant trains within the same system and across diverse systems providing the same function, such as first and second shutdown systems.

Independence

~~4.16~~ The principle 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 as far as reasonably practicable, to enhance the reliability of systems. ~~For example, different safety functions should be performed by different modules, components or systems to avoid the effect of the failure of these items on each other.~~

4.15

4.174.16 Examples of events caused by common cause failures which may be avoided by physical separation should include failures resulting from: fire, flooding, and other abnormal, or accident environments. Physical separation also reduces the likelihood of inadvertent human errors.

4.184.17 Design of certain areas of the facility such as confinement penetrations, cable spreading rooms, equipment rooms, control rooms etc. should consider the extent to which independence might be lost after a postulated initiating event.

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

4.204.19 Electrical 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 will prevent the safety systems from meeting their performance and reliability requirements.

4.214.20 Electrical isolation should control or prevent adverse interactions between equipment and components caused by factors such as electromagnetic interference, electrostatic pick-up, short circuits, open circuits, grounding, and among others application of the maximum credible voltage (alternating or direct current). Examples

of provisions for electrical isolation are electronic isolating devices, optical isolating devices (including optical fibre), relays, cable or component shielding, separation, distance, or combinations thereof.

~~4.22~~4.21 When isolation devices are used between safety systems and systems of a lower safety classification, the isolation devices should be part of the safety system having higher classification.

~~4.23~~4.22 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 should be:

a) Identified as part of the safety system which it is associated;

b) Independent from other lower safety classification systems; and

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

~~4.24~~4.23 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

~~4.25~~ Diversity provides defence against common cause failures, increasing the probability that appropriate safety actions will be performed when necessary.

4.24

~~4.26~~4.25 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 of such attributes are: different operating conditions, different working principles or different design teams (which provide functional diversity), different manufacturers using different designs, and types of equipment that use different physical methods which provide physical diversity.

~~4.27~~4.26 Diversity in instrumentation and control systems is the principle 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.

~~4.28~~4.27 ~~Diversity provides defence against common cause failures, increasing the probability that appropriate safety actions will be performed when necessary.~~

~~4.29~~4.28 In any application, it should be ensured that required diversity is achieved in the implemented design and preserved throughout the life of the facility.

~~4.30~~4.29 Where independence is claimed between two systems (for example 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 considering the full instrumentation and control chain from the sensors, signal conditioning devices, signal processors/calculators to the actuators drivers.

~~4.31~~4.30 Diversity applied to instrumentation and control systems should include:

- Functional diversity: could be achieved by systems providing different physical functions or means resulting in the same safety effects; and
- Equipment diversity: achieved by sensors and systems using different technology or designed and produced by different manufacturers.

~~4.32~~4.31 In assessing claimed diversity, attention should be paid to the equipment's components to ensure that actual diversity exists. For example, different manufacturers might use the same processor or the same operating system, thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers' names are insufficient without the considerations mentioned above.

Failure modes

~~4.33~~4.32 The failure modes of instrumentation and control systems important to safety should be known and properly documented using failure mode and cause- effect analysis methods. The more probable failure modes should neither place the system in an unsafe state nor cause spurious actuation of safety systems.

~~4.34~~4.33 The failure mode of instrumentation and control systems important to safety should ~~include~~ consider equipment aspects, and human aspects, and their interaction.

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

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

~~4.35~~

Formatiert: Keine Aufzählungen oder Nummerierungen

Fail-safe

4.36 The principle of fail-safe design should be considered and adopted as appropriate in the design of instrumentation and control systems to go into a safe state, with no necessity for any action to be initiated for any system or by the operator.

DESIGN TO COPE WITH AGEING

4.37 The service life of electrical and electronics systems and components might be considerably less than facility life. Ageing degradation that impairs the ability of a qualified safety component to withstand and function under severe environmental conditions may exist well before the functional capabilities under normal conditions are noticeably affected.

4.38 Ageing mechanisms that could significantly affect instrumentation and control components and means for following the effects of these mechanisms should be identified during design. Ageing is most commonly due to heat, and 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.

4.39 Potentially significant ageing effects (e.g., thermal 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.

4.40 Examples of means to address ageing impacts include:

- Component replacement before the end of its qualified service life;
- Adjustment of functional characteristics (e.g., recalibration) to account for ageing effects;
- Changes to maintenance procedures or environmental conditions that have the effect of slowing the ageing process; and
- Monitoring of equipment condition for ageing characteristics.

DESIGN FOR SECURITY

4.41 The purpose of security applied to instrumentation and control systems of research reactors is to prevent, detect and, in case of detection, eliminate or mitigate vulnerabilities that could be exploited either from outside or inside of the area of the protected equipment, software and data.

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

4.43 The design of the instrumentation and control system should include a security perspective to prevent malicious interventions or exploitations of the system.

4.44 Many design principles and components in the overall architectural design contribute to enhance both safety and security simultaneously, nonetheless an assessment should be performed to identify when one objective can be detrimental to the achievement of the other.

4.45 The recommended safety design guidelines of the instrumentation and control design should not create adverse effects to the security system.

4.46 Safety functions should not be adversely affected by elements of design intended to enhance security.

4.47 Security provisions should be implemented into the instrumentation and control system from the beginning of the system design. One of the primary security considerations from a design perspective is the potential of an instrumentation and control system failure or manipulation due to an adverse external or internal malicious act.

4.48 The operating organizations and designers should consider principles of security and computer security in all phases of the project, namely, requirements specifications, conceptual, preliminary and detailed design, procurement, fabrication, integration, installation, commissioning, operation and maintenance of the instrumentation and control systems.

4.49 Regulatory bodies should verify that the principles of security and computer security were applied during all phases of the project (whole project life cycle).

4.50 National information technology (IT) security requirements and IAEA guidance on computer security should also be considered.

EQUIPMENT QUALIFICATION

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

4.52 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 radiation endurance qualification if applicable). Items important to safety should be environmentally qualified for the effects of the ~~design basis~~ accidents to which they must respond;

c) Seismic qualification for components; and

d) Electromagnetic compatibility qualification for systems and components.

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

a) Use of engineering and manufacturing processes in compliance with recognized standards;

b) Reliability demonstration;

c) Past experience in similar applications;

d) Testing of supplied equipment;

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

f) Ageing analysis as applicable.

4.54 Traceability should be established between each installed system, structure and component 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.

4.55 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

4.56 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 equipment specifications.

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

4.58 Examples of performance requirements include: accuracy and response time requirements.

4.59 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

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

Environmental qualification

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

4.62 Systems and components should be designed to withstand the effects of, and be compatible with the environmental conditions associated with normal operation, anticipated operational occurrences and accidents when they are required to function.

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

Electromagnetic compatibility qualification

4.64 The unperturbed operation of electrical and electronic systems and components depends upon their electromagnetic compatibility with components located nearby or with which they are connected. Significant sources of electromagnetic interference could include for example fault current clearance by switchgear or circuit breaker or fuse operation, electromagnetic fields caused by radio transmitters, natural sources such as lightning strikes, geo-magnetically induced currents and other man-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 electromagnetic environment in which they are located.

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

- Emission and conduction of electromagnetic disturbances via cables; and
- Electrostatic discharge.

4.67 Electromagnetic compatibility qualification of instrumentation and control systems and components depends upon a combination of system and component design to minimize the coupling of electromagnetic noise to electrical components. Testing should be done to demonstrate that components can withstand the expected levels and ~~testing~~ to demonstrate that electromagnetic emissions are within tolerable levels. The electromagnetic emission test should be applied to systems and components both important and not important to safety. Instrumentation and control systems and components 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 repair, maintenance and measuring devices should be taken into consideration. Wireless systems and devices analysed could include, for example, mobile phones, radio transceivers, and wireless data communication networks.

4.69 Any electrical or electronic equipment in the facility will contribute to the electromagnetic environment. Instrumentation and control systems important to safety must be capable to perform safety functions in such 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 conduction) of electromagnetic interference among facility equipment. National and international 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 performance of the required testing during reactor operation, or, if justified, during shutdown only, supporting implementation of the guidance given in Ref. [~~11~~4][2].

Test provisions

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

a) Have appropriate test interfaces and status indication. Test interfaces should include, for example, the capability to introduce simulated process conditions or electrical signals;

b) Operate such that faults in the equipment are readily detectable;

c) Have features to prevent unauthorized access;

[2] Many of the research reactors are operated on relatively short operating cycles therefore provisions for testing during operation on those research reactors may be not necessary.

d) Be located such that test equipment and the components to be tested are readily accessible;

e) Be located such that neither the testing nor access to the testing location exposes staff to hazardous environments. Where equipment to be tested is located in hazardous areas, the design should consider provisions for testing from outside the hazardous area;

f) Have communications facilities as needed to support the tests.~~; and~~

~~g) Document the results of the testing following quality assurance procedures.~~

4.73 The design should ensure that the system cannot be unknowingly left in a test configuration. Inoperability or bypass of safety system components or channels should be indicated in the control room. For frequently bypassed items these indications should be auto-announcing.

4.74 Self-checking features of instrumentation and control systems important to safety should be considered and applied by the design as applicable. It is necessary to balance the provision of self-checking features and 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 instrumentation control functions during testing

4.76 Arrangements for testing include: test equipment interfaces, installed test equipment, built in test facilities and procedures. Testing should neither compromise the safety function nor introduce the potential for common cause failures. Testing of a ~~safety critical~~ system during operation should consider the safety aspect.

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

Test considerations

4.78 Considerations for the test should include:

- Location and installation of sensors such that testing and calibration can be performed preferably at their location including facilities for draining, drying, decontamination, isolation and ventilation where applicable;
- Location of test devices and test equipment in areas convenient to the equipment to be tested;
- Layout or administrative features;
- Convenience of component status indication and test connections.

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

Formatiert: Nummerierte Liste + Ebene: 1 + Nummerierungsformatvorlage: 1, 2, 3, ... + Beginnen bei: 1 + Ausrichtung: Links + Ausgerichtet an: 0 cm + Tabstopp nach: 0,3 cm + Einzug bei: 1,2 cm

Formatiert: Guidance list, Block

4.80 Channels under test of safety systems should automatically be placed in trip condition during the test.

4.81 The impact of the channel under test on safety assumptions should be considered;

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

Test programme

4.83 The design of instrumentation and control systems should include identification of a testing and calibration programme. The scope and frequency of testing and calibration should be designed and justified as consistent with functional and availability requirements. The test frequency should take into account the requirements for accuracy and the stability of the instruments chosen. Stable instruments with low drift can be tested less frequently.

4.84 A test programme should include:

- Description of programme objectives;
- Identification of systems and channels to be tested;
- Master test schedule;
- The reasons and justification for the tests to be conducted and test intervals;
- Description of required documentation and reports;
- Requirement for periodic review of programme effectiveness; and
- Specification of the individual test procedures that will be used during the conduct of tests.

4.85 The tests defined in the test programme, through clear procedures should ensure that, during and after completion of the tests:

- The overall functional capabilities of the systems are not degraded; and
- The instrumentation and control systems continue to meet their design basis requirements of functionality and performance and are returned to operation correctly.

4.86 The 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:

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

- Confirm that design basis functional and performance requirements[3] are met by documenting the success of a test showing compliance with tolerance requirements;
- Test all inputs and output functions, such as alarms, indicators, control actions, and operation of actuation devices;
- Provide post maintenance testing to ensure that systems are returned to operation correctly;
- Ensure the safety of the facility during the conduct of the test; and
- Minimize the possibility of spurious initiation of any safety action and 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.

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

4.90 For testing purpose, temporary modification of computer codes in systems and components ~~is~~ should not be allowed.

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

4.92 Test of a safety system channels should preferably be single online. When a single online test is not practicable, the test programme may combine overlapping tests, to achieve test objectives. For safety system channels tests it is necessary to provide documented justification for the use of overlapping tests.

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

4.94 Test of a safety system should include as much of the function under test as practical (including sensors and actuators) with consideration for the wear on actuators when tested excessively.

4.95 Wherever possible, test of a safety system should be accomplished under actual or simulated operating conditions, including sequence of operations. Precaution should be taken in testing sensitive and critical safety system.

4.96 It is necessary to evaluate and document the reasons for, root causes of, and actions taken after a failed test before the results of a repeated test can be used to demonstrate operability of the system or component involved.

[3] Requirements for response time testing should be strictly based on the assumptions in the SAR and limited to parameters that require special consideration for response time because their timely response is critical to facility safety.

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

MAINTAINABILITY

4.98 The design should consider provision of means for the maintenance of instrumentation and control systems. 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 so as to minimize risks to maintenance personnel and to facilitate necessary preventive maintenance, troubleshooting, and timely repair.

4.100 Design to facilitate maintenance, troubleshooting and repair includes:

- Avoiding locating equipment in areas of extreme temperature or humidity, and where risk of high radiation levels exist;
- Considerations of human factors in performing the required maintenance activities;
- Leaving sufficient room around the equipment to ensure that the maintenance staff, with his supporting tools, can perform their tasks; and
- Provision of test panels, instrument isolation and draining and test connections.

4.101 If components must be located in inaccessible areas other solutions should be considered by the design. Examples include:

- Installation of spare redundant devices in cold or hot standby; and
- 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 modifications of an existing one. Design analyses, including the following specific activities, should be performed to confirm that instrumentation and control systems fulfil their design basis requirements, Ref. [5~~3~~]:

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 facility defence-in-depth concept;

c) Verification that common cause failure vulnerabilities of instrumentation and control safety systems are known and have been adequately addressed. Common cause failure vulnerabilities may be addressed by eliminating the vulnerability, providing diverse means of achieving the safety functions subject to the common cause failure, or 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 that considers design features such as redundancy, testability, failure modes, mean time between failures and rigour of qualification. 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 test provisions;

f) When determining system availability test facilities that are part of the safety system must be considered as permanently installed test equipment;

~~g) Typically traceability analysis is used to confirm implementation and validation of requirements;~~

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

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

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

4.104 Each assumption of an analysis should be stated, and justified.

SAFETY SYSTEM SETTINGS

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

4.106 Determination of instrumentation and control safety system setting usually considers the following values:

- Safety limits – limits on certain operational parameters within which the operation of the reactor has been shown to be safe;
- Analytical limit (of safety system setting) – limit of a measured or calculated variable established by the safety analysis to ensure that a safety limit is not exceeded; and
- Allowable value – the limiting value of a safety system setting, beyond which appropriate action must be taken. The allowable value for a specific 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 is necessary.

Figure 4.1 illustrates the relationship between these terms and the types of measurement uncertainties that are normally considered in establishing the basis for trip safety system setting and allowable values.

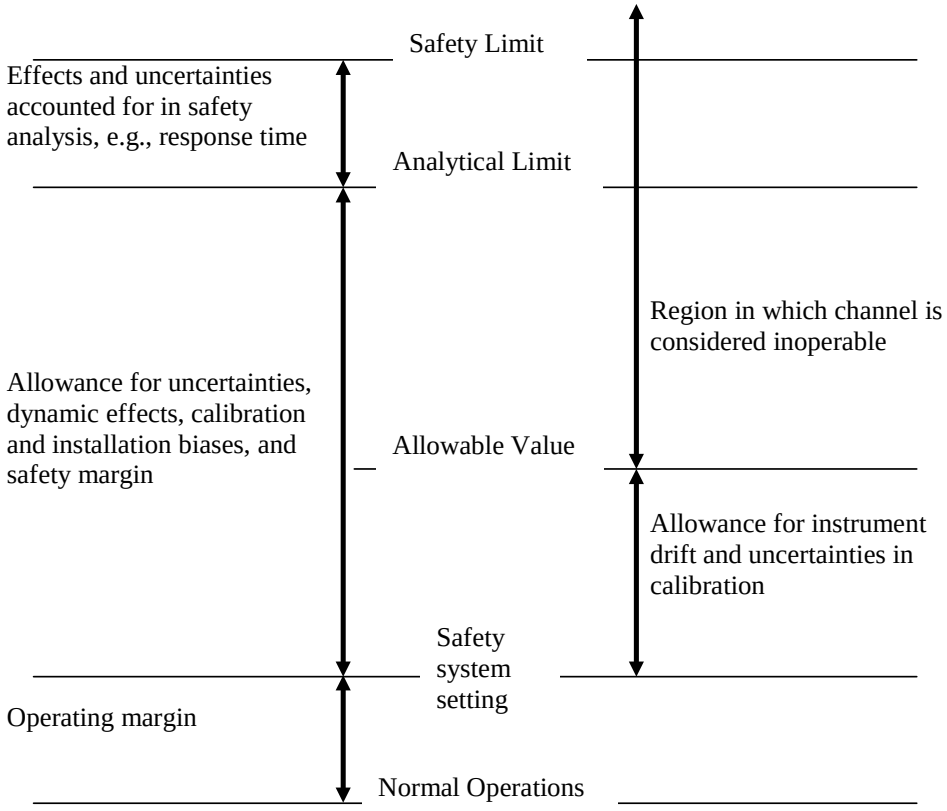

FIG. 4.1 Safety system setting terminology and errors to be considered in safety system setting determination

IDENTIFICATION OF ITEMS IMPORTANT TO SAFETY

4.107 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 phases of the reactor facility as well as for the labelling of controls, displays and indications. Clear identification of components is necessary 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 assemblies that are clearly identified may not themselves need identification.

5. SYSTEM SPECIFIC DESIGN GUIDELINES

SENSING DEVICES

5.1 Measurements of research reactor variables 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 it is detected by limit or on/off switches (i.e. temperature, pressure, flow or level limit switches and main supply availability, control system normal operation or interlock on/off switches).

5.2 The measurements of variables may be made directly or indirectly such as calculation of the value 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 measurement 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, and accident conditions.

5.5 No identified common cause failure vulnerability of sensing devices should have the potential of denying operators the information and parameters that they need to control and mitigate accident conditions. An example is the saturation of radiation monitors.

5.6 If more than one sensor is necessary to cover the entire range of the monitored reactor parameter, 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., the measured value of a parameter depends upon sensor location), the minimum number and locations of sensors, such as flow measurement elements, should be identified by the design and justified. The final location also needs to be tested to verify the design assumptions and whether associated set points, limiting conditions and allowable values should be reassessed.

REACTOR PROTECTION SYSTEM

5.8 The reactor protection system where applicable should comply with all of the general guidance for design of instrumentation and control systems given in the section 4.

5.9 The design of the reactor protection ~~system~~ 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 human factors).

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

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

5.12 As part of the 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 part 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 each other.

5.13 The action initiated by the reactor protection system should be latched so that once an action is started, it will continue until its completion even if the initiating state ceases to be present. 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 may be considered to be sufficient provided that the diagnosis is simple and the action is clearly defined:

- The operator has sufficient and clearly presented information to make valid judgements on the need to initiate the required safety actions;
- The operator is allowed sufficient time to evaluate the status of the reactor facility and to complete the required actions;
- The operator is provided with sufficient means of reactor control to perform the required actions., ~~and;~~
- ~~The diagnosis is simple and the action is clearly defined.~~

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. It is preferable that the manual actuation function 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 protection system trip, 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 allow changes in reactor conditions. For example, the trips that limit reactor power during start-up must be inhibited at some point to allow power increase. Another example would be the necessity for inhibition of certain functions in case of pulsed operation of a research reactor. In this guide such reactor protection system inhibit functions are called safety interlocks and are classified as components/functions of safety systems.

5.17 The protection system should prevent enabling of an operational interlock when the applicable permissive conditions are not met. If conditions change such that an enabled operational interlock is no longer permissible the protection system should automatically accomplish one of the following:

- Disable operational interlock; or

- Initiate appropriate protective actions.

5.18 Paragraph 4.88 gives recommendations on temporary connections used for maintenance and testing. This recommendation should be strictly applied to reactor protection systems.

5.19 The design should ensure that safety system settings can be established with such 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 before the safety limit is reached. In addition, these margins should take in account the following:

- Inaccuracy of instrumentation;
- Uncertainty in calibration;
- Instrument drift; and
- Instrument and system response time.

5.20 If a computer based system is intended to be used in reactor protection system the following requirements should be applied:

- Hardware and software of high quality and best practices should be used;
- The whole life cycle of the system should be systematically documented and reviewed; and
- Independent verification and validation process 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 with a high level of confidence, diverse means of ensuring fulfilment of the protection functions should be provided. The diversity[4] may be provided:

- Internally to the reactor protection system or by a separate and independent system; as long as the design bases are met; and
- By a diverse independent system which may be hardwired or computer-based as long as adequate diversity can be justified.

5.22 "To confirm the reliability of the computer based systems, an assessment of the computer based systems should be undertaken by expert personnel who are independent of the designers and the suppliers." Ref. [1], para. 6.104, (c)

5.23 For computer based reactor protection systems, the system design should include computer security.

---

4 - Normally, it is easier to justify diversity between computer-based and hardware-based systems than between two computer-based systems.

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 shut-down, refuelling and maintenance), accident conditions including the recording all variables important for safety.

5.25 The design should take into account the requirements of start-up neutron source and dedicated start-up instrumentation, for conditions in which they are needed.

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 safe operation of the facility. These requirements and limitations should cover:

- The information necessary to establish the safety limits and safety system settings;
- Control system constraints and procedural constraints on process variables and other important parameters;
- Maintenance, testing and inspection of the facility to ensure that systems, structures and components function as intended;
- Clearly defined operating configurations, including operational restrictions in the event of safety system outages; and
- Consideration 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. The design of control rooms should include task analysis, ergonomic, and human factors.

5.28 The design of the control rooms should include suitable 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 fire and one control room (main, supplementary or emergency) should be designed and constructed to resist the design base earthquake.

Main control room

5.30 The principal location for safety 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 safe state after the onset of anticipated operational occurrences and accident conditions.

Supplementary control room

5.31 A remote reactor shutdown capability should be provided if the safety analysis identifies events that could inhibit the operators' ability to shut down the reactor and keep it in 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 analyses identifies events where the main control room could be unavailable or operations from the main control room could be inhibited.[5]

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

5.33 ~~Events that could inhibit the operator's ability to shut down the reactor from the control room should include, for example, fire in the control room or fire in a location that affects connections between the control room and devices elsewhere in the facility.~~

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

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

Irradiation and experiment facility control systems

5.36 In many research reactors there are special control consoles for running irradiation and experimental devices. They are located in the main control room and/or in other rooms.

5.37 The operator of experimental devices should have communication links with reactor operator to share information on experiment and reactor status and make each other aware of the expected actions (e.g. situations that requires shutdown of the reactor).

5.38 The irradiation and experimental devices control consoles should be devoted exclusively to the experimental facilities to keep a functional separation with the reactor activities.

5.39 Parameters important to the operation of reactor should be covered by the alarm system. Other alarms of experimental devices should be presented with a functional separation from reactor's alarms.

Voice communication system

5.40 Communications systems should be provided for staff to securely interface between the main control room, supplementary control room, other locations within the facility,

[5] Events that could inhibit the operator's ability to shut down the reactor from the control room should include, for example, fire in the control room or fire in a location that affects connections between the control room and devices elsewhere in the facility.

Formatiert: Keine Aufzählungen oder Nummerierungen

Formatiert: Englisch (Großbritannien)

the operators of experimental devices, associated facilities, the on-site emergency centre, and to external emergency organizations without having to leave the control room.

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

- Areas where communications are needed during anticipated operational occurrences or accident conditions;
- Off-site emergency services; and
- Associated facilities.

5.42 The diverse communications links should be routed such that they will not both be affected by loss of the primary communications links, whatever it is its origin (including external events), and should be capable of operating independently of both the facility power systems and off-site power systems.

Provisions for fire detection and extinguishing

5.43 The nature of the fire alarm system, its layout, the necessary response time and the characteristics of its detectors should be determined by the fire hazard analysis.

5.44 The detection system should provide detailed warning in the control room about the location of the fire by means of audible and visual alarms.

5.45 Local audible and visual alarms, as appropriate, should also be provided in facility areas that are normally occupied. Fire alarms should be distinctive and should not be capable of being confused with any other alarms in the facility.

5.46 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.

5.47 Fire detectors should be located so that the flow of air due to ventilation or pressure differences 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.

5.48 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.

5.49 When items such as fire pumps, water spray systems[6], 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 detection operating

[6] Gas suppression systems are a good alternative to water sprinkler systems for rooms containing power and instrumentation and control systems.

in series. The design should allow the operation of the system to be stopped if the actuation is confirmed to be spurious.

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

- Protected from the effects of fire by a suitable choice of cable type, by proper routing, or by other means;
- Protected from mechanical damage; and
- Constantly monitored for integrity and functionality.

5.51 Requirements for periodic testing should be considered.

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

POWER SUPPLIES OF INSTRUMENTATION AND CONTROL SYSTEMS

5.53 The power supply for instrumentation and control systems should have classification, 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 they serve. In addition failures modes for power supplies should be considered.

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

5.55 Power supplies can provide a transmission path for electromagnetic interference which 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 interference sources include electrical fault clearance associated with other equipment on the same supply. These interferences should be analysed and avoided to the extent possible.

6. OPERATION

OPERATIONAL LIMITS AND CONDITIONS

General

6.1 Paragraphs 7.29 and 7.30 of Ref. [1] respectively define:

- *"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

- *"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 assure that, during the operational states of the reactor, the instrumentation and control systems contribute to keep the reactor operating parameters within the operational limits and conditions, Ref. [610].

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 during the operational states of the reactor by means of the selected safety system settings, during design basis accident and, as far as reasonably practicable, during beyond design basis accident.

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, provides 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 to provide these functions should include the capability of storing and recovering these safety systems 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 assure safe operation of the reactor while avoiding frequent actuation of safety systems. Acceptable margins must be allowed for expected drift in measured signals and all expected variations during normal operation.

CONTROL OF ACCESS TO SYSTEMS IMPORTANT TO SAFETY

6.6 All reasonable precautions shall be taken to prevent persons from ~~deliberately~~ carrying out unauthorized actions that could jeopardize safety when accessing instrumentation and control systems or performing tasks on instrumentation and control systems.

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 limited access to functions important to safety using hardware or software access keys, access alarms and proper administrative controls.

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

6.9 When computer based systems are part of instrumentation and control systems, on the basis of the security policy that has been defined for the computer based system environment, appropriate security procedures - for instance access control - should be implemented. National regulations/standards and IAEA guidance may be used to define the requirements for control system security.

6.10 Secure storage arrangements and procedural controls should ensure that only authorized software versions are loaded into the facility equipment. 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 (implemented) allowing users access to only that data and commands for which they have been authorised.

6.13 The security policy should implement suitable measures in place to prevent intentional or unintentional intrusion or corruption of the software or data, the introduction of malicious code, incorrect connection 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 the 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 the long term safety of the reactor. Frequency ~~or periodicity~~ for such activities should be consistent with the reliability requirement of such systems or components.

6.15 The instrumentation and control systems should include, when reasonably applicable, on-line testing functions and capabilities to facilitate and reduce the time of periodic testing ~~preserving~~ 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 In safety systems it is important that design features 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 test of a 2 out of 3 logic leaves the system in 1 out of 2 logic arrangement. Administrative controls on availability of safety systems should keep them in operation within 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 minimal instrumentation and control systems required for safety to be kept operational during that extended shutdown.

7. HUMAN FACTORS ENGINEERING AND HUMAN- MACHINE INTERFACE

GENERAL CONSIDERATIONS

7.1. An effective human factors engineering process 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 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 in the design, compatibility and human interaction of the modernized part and 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 within the considerations given in paragraphs 7.1 and 7.2.

PRINCIPLES FOR HUMAN FACTORS ENGINEERING AND HUMAN MACHINE INTERFACE DESIGN

7.5 The human-machine interfaces design should retain useful features and avoid human factors engineering problems and issues experienced in previous designs and should be part of architecture considerations in new projects as well as in modification projects. The human-machine interface design should emphasize the incorporation of human and machine features and the advantages of applying both.

~~7.6 Design requirements for human-machine interface should be specified based on all of the tasks to be supported by the human-machine interface, including normal and abnormal operations, for operators as well as maintenance staff, experimenters and emergency response staff.~~

~~7.7~~7.6 Instrumentation and control functions necessary to achieve facility safety objectives should be identified and allocated to human and system resources according to a defined methodology and should be part of architectural considerations during the design stage.

~~7.8~~7.7 All human-machine interfaces should be designed according to ergonomic principles. The operational philosophy should determine which information is convenient to be displayed using conventional displays (e.g. panel instruments, alarm annunciators, etc.) and which information is convenient to be displayed using video screens. To assist in the establishment of design principles for information display and controls the different roles of the operating personnel such as operator, maintenance staff, systems manager and accident response staff should be taken into account.

~~7.9~~7.8 R~~Design r~~equirements for human machine interface designs should be specified based on all of the tasks to be supported by the human machine interface, including normal and abnormal operations, for operators as well as the maintenance staff, experimenters and emergency response staff.

~~7.10~~7.9 The requirements specification for human-machine interfaces design should include the instrumentation and control requirements necessary ~~the information~~ to assess the general state of the facility, in whichever condition it may be, and confirmation that the designed automatic safety actions are being taken.

~~7.11~~7.10 The instrumentation and control system should provide operators with the information necessary to detect changes in system status, diagnose the situation, and verify manual or automatic actions.

~~7.12~~7.11 During facility operation, the operator should be provided with suitable warnings or alarms when the facility is approaching a state where operational interlocks should be enabled or disabled.

~~7.13~~7.12 The reactor operator should be provided with sufficient indicating and recording instrumentation to monitor relevant reactor parameters during and following anticipated operational occurrences and accident conditions.

~~7.14~~7.13 Audible and visible alarm systems should provide an early indication of changes in the operating conditions of the reactor if these conditions could affect its safety.

~~7.15~~7.14 Careful attention should be paid during the design of the human-machine interfaces to ensure that the operator should not be overwhelmed by large amounts of data that could be difficult to grasp owing to the limitations on human perception, cognition and memory. This is particularly important in the case of the treatment of alarms.

~~7.16~~7.15 The instrumentation and control system design should take due account of the time needed by operators to perform their expected tasks.

~~7.17~~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.

~~7.18~~7.17 Where a function is carried out automatically, the instrumentation and control system should provide operators with information necessary to monitor the function. The information should be provided at a rate and level of detail that the operator can monitor effectively.

~~7.19~~7.18 The instrumentation and control system should alert the operator of the failure of an automatic control system.

7.207.19 The presentation of information should be integrated into a harmonized arrangement that optimizes the operator's understanding of the facility's status and the activities necessary to control the facility.

7.217.20 The operation and appearance of the human-machine interfaces should be consistent across information and control locations, reflect a high degree of standardization, and be fully consistent with procedures and training.

7.227.21 The human-machine interfaces should provide the capability to display recorded information where such displays will help operators to: identify patterns and trends, understand the past or current state of the system, or predict future progressions.

Control Rooms

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

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

7.257.24 Normal working environments in control rooms should be ensured concerning lighting, temperature, humidity, noise, radiation dose, dust and vibration, for normal, abnormal and accidental conditions. The design of the main control room and supplementary control room (if required) should take into account conditions resulting from internal hazards (e.g. fire smoke or toxic substances in the atmosphere) and external hazards (e.g. earthquakes, flooding, extreme meteorological conditions, man-made hazards).

7.267.25 The design should consider the layout of instrumentation and the mode of presenting information to operating personnel with both, an adequate overall picture of the status and performance of the facility, and detailed information, where necessary, on specific systems or equipment status or performance.

7.277.26 The information displayed at the control rooms should allow operators to:

- Take specific manually-controlled actions for which no automatic control is provided;
- Confirm facility critical safety functions availability and performance of automatic safety actions;
- Determine the potential for or actual breach of a fission product barrier;
- Confirm performance of safety systems, auxiliary supporting features, and other systems necessary for mitigation of accident conditions or maintaining of safe shutdown; and
- Determine the magnitude of any release of radioactive materials and continually assess such releases.

~~7.28~~7.27 In case of a supplementary control room, sufficient instrumentation and control equipment should be available, physically and electrically separate from the main control room, 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 these essential safety functions in the main control room.

~~7.29~~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 respond to the same range of anticipated operational occurrences and accident conditions as the main control room. In any case the information available at the supplementary control room or emergency control console should allow for putting the facility in a safe condition during and after accident conditions and mitigate 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 in both new and older facilities is increasing. They are used both in safety related applications, such as some functions of the process control and monitoring systems, as well as in safety applications, such as reactor protection systems.

8.2 Computer based systems reliability 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 and not random in nature, 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 ~~made~~ given to have separate computer based instrumentation and control systems for the reactor and the experiments. In that way, each system could be treated with its own set of requirements and objectives.

8.5 ~~For computer based systems, shorter life cycles and earlier O~~obsolescence management should be considered in the design and operation of computer based systems to plan and manage for diminishing manufacturing sources and material shortages.

COMPUTER BASED SYSTEMS AND SOFTWARE DESIGN CONSIDERATIONS

8.6 In the implementation of safety systems, complexity should be avoided both in the functionality of the system and in its implementation, by complying with a structured design, following 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 achievement of safety functions. Functions not essential to safety should be isolated to avoid any impact to safety functions.

8.8 For computer based system applications, 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 ~~and development~~ process[7] for the system and its associated software should be used to facilitate the assessment of whether design objectives are achieved.

8.10 When the use of a computer involves two or more functions 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 software common cause failures. Diversity of methods, languages, tools and personnel should also be taken into consideration. However, it should be noted that although diverse software may provide improved protection against common mode software failures, it does not guarantee the absence of coincident errors. The choice of type of diversity or the decision not to use diversity should be justified in the system design stage.

8.12 System fail-safe features, supervision and fault tolerant mechanisms should be added into the software, but only to the extent that the additional complexity is justified by design basis functional and performance requirements critical to facility safety and needed protection for anticipated operational occurrences and design basis accidents~~a demonstrable global increase in safety~~.

8.13 Fault detection and self-supervision features should not adversely affect the ability of 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 lifetime against physical attack, unauthorized access, fraud, viruses and so on. Safety systems should not be connected to external networks.

8.15 The connections for external storage devices should be locked to prevent their 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 can be

[7] In a top-down design ~~and development~~ process is essentially the breaking down of a system to gain insight into its sub-systems.

easier to repair, to review and analyse, since the design can be easier to understand. Software maintainability 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 ~~(real-time)~~ behaviour with regard to functions and timing.

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

8.19 Data communication channels important to safety should satisfy the recommendations for independence from each other.

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

8.21 The communication technology should be chosen and 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 the data communication.

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

8.24 Data flow from lower to higher classified safety systems should be ~~prevented~~ avoided unless decoupling device is inserted.

~~8.25 The design should explicitly handle all possible cases of logic and timing, and all operating modes of the system such as reset, power-on and normal operation.~~

~~8.26~~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.

~~8.27~~8.26 Software tools could be used to support all aspects of the instrumentation and control life cycle where benefits result through their use and where such tools are available. These tools should be verified and assessed consistent with the reliability requirements, the type of tool, and the potential of the software tool to introduce errors.

PROJECT PLANNING

~~8.28~~8.27 The project development process should be carefully planned and clear evidences should be provided that the process has been followed in order to facilitate the independent assessment of systems important to safety.

~~8.29~~8.28 The development plan should identify and define the process that will be used on the particular project. Other aspects of the project which should be considered and planned are quality assurance, verification and validation, configuration management, installation and commissioning.

8.308.29 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 and before starting the next phase.

8.318.30 The methods to be used in the development should be identified. The selection of method should be related to the quality assurance programme description, in which standards and procedures are established.

8.328.31 A quality assurance programme should be prepared and implemented before the project begins. A software quality assurance plan should be available at the start of the project.

Verification and validation plan

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

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

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

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

Configuration management plan

8.378.36 All items of software development, such as compilers, development tools, configuration files and operating systems, should be under configuration management control. 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.

8.388.37 A procedure for change control should be defined. The change control procedure should maintain records of the problems that were identified during the development process or during the operation of the research reactor, which required changes, how the problems were analysed, which items were affected, which specific changes were made to correct the problem and which versions and baseline were produced to resolve the problems.

8.398.38 The change control procedure should also identify responsibilities for approving changes.

Installation and commissioning plan

8.408.39 The installation and commissioning plan should cover the following:

- The sequence of steps for proper integration of the system into the reactor facility and the corresponding facility states needed for safe introduction of the new or changed system;
- The interactions with the regulatory body, including approvals, hold points and reports that should be respected before the system can be put into operation;
- The commissioning test cases and sequence and the corresponding facility states needed to confirm proper functioning of the system in the facility environment; and
- A description of the records and reports that will be generated to describe the results of commissioning.

COMPUTER BASED SYSTEM REQUIREMENTS

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

8.428.41 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 for defining functional safety requirements. In addition to safety requirements, some additional requirements not directly associated with safety are added at this stage of the design, such as: requirements for reliability and availability.

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

8.448.43 Non-functional requirements should specify the following:

- The relevant dependability attributes, such as reliability, availability and security, required of the system behaviour;
- The security requirements derived from the security policy that has been defined for the computer based system environment including security procedures;
- Performance requirements (e.g. response time of software modules for the safety functions);
- Environmental qualification requirements such as temperature and radiation;
- Whether and where physical separation is needed (for example between safety and control functions); and
- That requirements not directly associated with safety (such as availability or security) will not adversely affect the ability of a safety function to be performed when required.

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

Software requirements

~~8.46~~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 under each operation mode, performance criteria, timing and constraints, failure detection, self-supervision, safety monitoring requirements and security requirements.

~~8.47~~8.46 Wherever safety system settings are user configurable, changes to these settings should be allowed only to authorized user and these safety system settings should be checked for their integrity.

Software design

~~8.48~~8.47 In systems important to safety, unnecessary complexity should be avoided at all levels of design. The simpler the design is, the easier is to achieve and to demonstrate all other attributes. It also gives greater confidence that the software is fully understood.

~~8.49~~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.

~~8.50~~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, libraries, etc. The design and its description should demonstrate that each software requirement has been met and to verify that the implementation is correct with respect to the detailed design.

~~8.51~~8.50 The documentation on software design should provide technical information on the overall architecture of the software and on the detailed design of all software modules and their concurrencies with synchronization to prevent unpredictable results in terms of response time. Relevant implementation constraints should also be specified.

~~8.52~~8.51 Each software module identified in the software architecture should be described in the detailed design.

~~8.53~~8.52 Diagrams and flow charts could be used as long as the meaning of the elements of the diagrams is well defined. Other 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 can be verified using formal methods.

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

8.55 A system for requesting formal change and controlling modifications should be in place in the implementation phase to deal with omissions and inconsistencies. Up to date records of these 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 system.

VERIFICATION AND ANALYSIS

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

8.59 Records of the numbers and types of anomalies should be maintained. These records should be reviewed to determine whether or not any lessons can 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 life cycle phases. The means by which the verifiers are recording the results of their reviews should be stated in the verification plan together with a justification of the chosen method. 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 so as to facilitate regression testing, by ensuring that tests are repeatable and require minimal human intervention.

8.63 Any anomalies in test performance 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.

~~8.63~~8.64 Each anomaly in 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. Additionally, a cross-reference record of software fixes and software builds should be maintained for configuration management of the installed software.

COMPUTER SYSTEM INTEGRATION

8.65 The software version integrated into the computer system should be the latest version that has been verified and validated.

~~8.64~~8.66 The computer system integration phase should encompass at least three sequenced activities: software tests, hardware test and integration and hardware-software integration.

8.658.67 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.

8.668.68 During the verification of the system evidence should be generated which will demonstrate that the system integration has been properly controlled.

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

Integrated computer system tests

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

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

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

- Coverage of all requirements (including robustness tests and security features);
- Coverage of full ranges of values for input signals;
- Exceptions handling (for example demonstration of acceptable behaviour when input failure occurs);
- Timing related requirements (such as response time, input signal scanning, synchronization);
- Accuracy;
- All interfaces (such as the hardware–software interface in system integration and external interfaces during validation);
- Stress and load testing;
- Security functionality requirements (i.e.: logging of user activities); and
- All modes of operation of the computer system, including transition between modes and recovery after power supply failure.

8.718.73 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

8.728.74 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.

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

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

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

OPERATION, MAINTENANCE AND MODIFICATION

8.768.78 During the operation, maintenance and modification phases the following main activities should be considered:

- Periodic tests, performed in order to verify that the system is not degrading;
- Regression testing due to modifications, implemented to enhance or change the functionality or to correct errors;
- Change of operating parameters;
- Diagnosis activities, e.g. the execution of special diagnostic programs;
- Hardware components replacement due to failures.;

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

8.778.80 The life cycle of the systems should include the processes for implementing modifications. This life cycle should contain the phases of the main 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 introduced.

8.788.81 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 such a need.

Computer security

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

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

8.818.84 If computer security features are implemented in the Human Machine Interface, they should not adversely affect the operator’s ability to maintain the safety of the facility.

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

8.838.86 Ref. [713] provides additional guidance on concerns, requirements, and strategies for implementing computer security programmes at nuclear facilities.

9. CONFIGURATION MANAGEMENT

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

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

- General information (e.g. system identification, serial number, manufacturer, supplier support, location, safety class);
- System summary (e.g. functionality, configuration, safety impacts caused by the system, current performance, loss of operational availability due to the unavailability of the system, interfaces, security, documentation);
- Physical characteristics (e.g. number of cabinets, detailed component inventory, limits);
- Boundaries (environment, power supply, grounding, margins in the cabinets and the rooms for power supply, amount of information exchanged between other systems);
- System constraints (e.g. licensing conditions, technical specifications, design constraints, operating characteristics);
- Obsolescence issues (e.g. maintenance costs, replacement parts, performance degradation);
- Measures for improvements (e.g. functionality, configuration, performance, maintenance); and
- References.

9.3 Operational and maintenance staff should collaborate in the improvement and the updating of instrumentation and control configuration control documentation. Information of the documentation and data base mentioned above (9.1 and 9.2) should be protected according requirements on security of information

10. MODIFICATION AND MODERNIZATION OF INSTRUMENTATION AND CONTROL SYSTEMS

10.1 One major reason to decide for an instrumentation and control modernization at a given facility is obsolescence of the present instrumentation and control system, the

unavailability of spare parts and an increased failure rate of the instrumentation and control system leading to frequent reactor shut downs, long repair periods and therefore resulting in increasing unavailability of the facility. Recommendations for ageing management for research reactor systems are given in Ref. [8]. Additional aspects supporting a positive decision for modernization is the technological progress in instrumentation and control systems leading to higher reliability of instrumentation and control systems, improvement of human-system interface and extensive and fast data collection and processing. Besides such technically based decisions also other aspects (such as new regulatory requirements) may influence the final decision for modernization of the instrumentation and control system.

10.2 Before entering the modernization project, it is advisable to collect information on needs and limitations in the current instrumentation and control system. Such information can be found from past failures and incidents as collected by event recording systems as used in the facility. Other weaknesses can be identified from regular self-assessment of operational performance, including analysis of even small deviations from normal operation. In addition to identifying current problems and limits with the current instrumentation and control system the decision maker should assess and attempt to foresee possible future problems and limits of the current instrumentation and control system.

10.3 Upgrade and modification of instrumentation and control systems should be performed in accordance with the guidance provided in Ref. [94] on planning, organizational aspects, safety assessment, implementation and post implementation, training, and documentation of facility modifications. Vigorous independent verification and validation should be done for every change associated with modification and modernization.

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

10.5 Modification to instrumentation and control equipment is expected during the life of the facility. Regardless of the reason, thought should be given to the functional intent of the equipment being modified, for example, when changing from one technology to another (e.g. analogue system to a digital system or obsolescence of the existing system preventing the access to spare parts).

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

10.7 Special assurance is needed to verify that every modification has been properly assessed, documented and reported in terms of potential effect on safety, and that the reactor is not restarted without formal approval after the completion of modifications of instrumentation and control systems.

10.8 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 current states of instrumentation and control systems in the facility should be available. A process of

verification and update of the existing documentation should be undertaken prior to commencing any modernization activities. Operational and maintenance staff should collaborate on the update of existing documentation to ensure all modernization activities are completely captured in the instrumentation and control configuration control documentation.

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

10.10 Verification and update 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.

10.11 There should be a designated designer that will be responsible for the design, integration, documentation and maintenance as well as training facility personnel in the use of the new equipment. Ref. [10~~5~~] provides details on the responsibilities that the responsible designer should assume.

10.12 Modifications to any instrumentation and control system should take into consideration the duties and the responsibilities of the operating personnel, (e.g. operators as well as the maintenance staff, experimenters and emergency response staff) in order to achieve an effective interface between the operating personnel and the research reactor systems.

10.13 The effect of the modification on the facility personnel interaction with the system should be considered. Particular requirements for the operating personnel should be taken into account from the early stages of the project. (refer to section 7 for details on human factors considerations).

10.14 The reliability of the new or modified equipment should be considered as well as the effect of the modification on the overall system reliability. The performance of a qualitative analysis (e.g. failure modes, effects and criticality analysis) may be helpful in determining which parts of the system may be affected by the modification and what the implication is on the ability of the system to perform its safety function.

10.15 When modifying an existing safety system, the effect on the current defence-in-depth implementation should be considered.

10.16 Safety systems are required to be independent, as far as reasonably practicable, of other reactor systems. When modifying any instrumentation and control system, development of design guidelines should be considered.

10.17 Generally, when modifying any system, the complexity of the modification 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/or the ability to expand the capabilities of the existing safety systems in the future.

10.18 The requirement for system environmental qualification should be considered. Environmental qualification should be based on the qualification programme of the modification.

10.19 Change control procedures should be in place, including appropriate procedures and organizational structures for the review and approval of the safety aspects of the modification.

10.20 The design of instrumentation and control upgrades and modification should consider:

- The limitations due to the physical characteristics of the installed facility, which effectively restrict the design options for instrumentation and control systems;
- The possible need to maintain consistency between the design of replacement equipment and existing instrumentation and control equipment (e.g. to reduce the complexity of the overall operator interface and maintenance tasks of the facility); and
- Practical considerations with respect to the equipment or technology commercially available when required by the project programme and the prospects for securing support of such equipment and technology by manufactures or third parties for the installed life of the equipment.

10.21 The benefits of changes should be weighed against potential negative safety consequences and this assessment documented as part of the justification for the changes. For instance, enhancements to the operator interface features might increase errors by operations and maintenance personnel for some time after the change. As required, sufficient and proper training programs should be developed and implemented to minimize or eliminate the potential for such errors, if changes are implemented.

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

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

10.24 Once complete, and before start-up of the reactor, the installation should be functionally tested following the recommendations of Ref. [94].

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

10.26 When an instrumentation and control system is replaced, the new instrumentation and control system may, when appropriate, be run in parallel with the old system for a probationary period, i.e. until sufficient confidence has been gained in the adequacy of the new system. In this configuration, only the old 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 have the possibility to assess and compare their response against the response of the old system.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Safety Standards Series No. NS-R-4, IAEA, Vienna (2005).

[2] 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).

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defense in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

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

~~[2]~~

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Research Reactors and Preparation and Content of the Safety Analysis Report, IAEA Safety Standards Series No. SSG-20, IAEA, Vienna (2012).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Research Reactors, IAEA Safety Standards Series No. NS-G-4.4, IAEA, Vienna (2008).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, Technical Guidance Reference Manual, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing management for research reactors, IAEA Safety Standards Series No. SSG-10, IAEA, Vienna (2010).

~~[3]~~

~~[4]~~[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety in the Utilization and Modification of Research Reactors, IAEA Safety Standards Series No. SSG-24, IAEA, Vienna (2012).

~~[5]~~[10] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, INSAG-19, IAEA, Vienna (2003).

~~[6] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defense in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).~~

~~[7] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, IAEA, Vienna (1999).~~

~~[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing management for research reactors, IAEA Safety Standards Series No. SSG-10, IAEA, Vienna (2010).~~

~~[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Glossary, IAEA, Vienna (2007).~~

Formatiert: Einzug: Hängend: 1,27 cm

Formatiert: Einzug: Links: -1,26 cm, Hängend: 2,51 cm

Formatiert: Einzug: Hängend: 1,27 cm

Formatiert: Englisch (USA)

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Research Reactors, IAEA Safety Standards Series No. NS-G-4.4, IAEA, Vienna (2008).

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

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/REVISION5), Recommendations, IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, Technical Guidance Reference Manual, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Specific Safety Requirements, IAEA Safety Standards Series No. SSR-2/1, IAEA Vienna (2012).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

ANNEX I - THE INSTRUMENTATION AND CONTROL SYSTEMS THAT CAN BE INCLUDED IN A RESEARCH REACTOR

GENERAL

1.1. The instrumentation and control (I&C) systems of a research reactor involve many systems that can be identified in a facility and they may vary depending on the type of reactor, the purpose and its operation modes. Usually it could include those systems identified in section 2 as examples of I&C systems. Typical set of I&C systems and their interrelations is shown on Fig. AI.1

1.2. This Annex identifies all I&C systems that can be included in a research reactor considering that some or several of these I&C systems could not be present in a particular facility as they are not required for that specific installation.

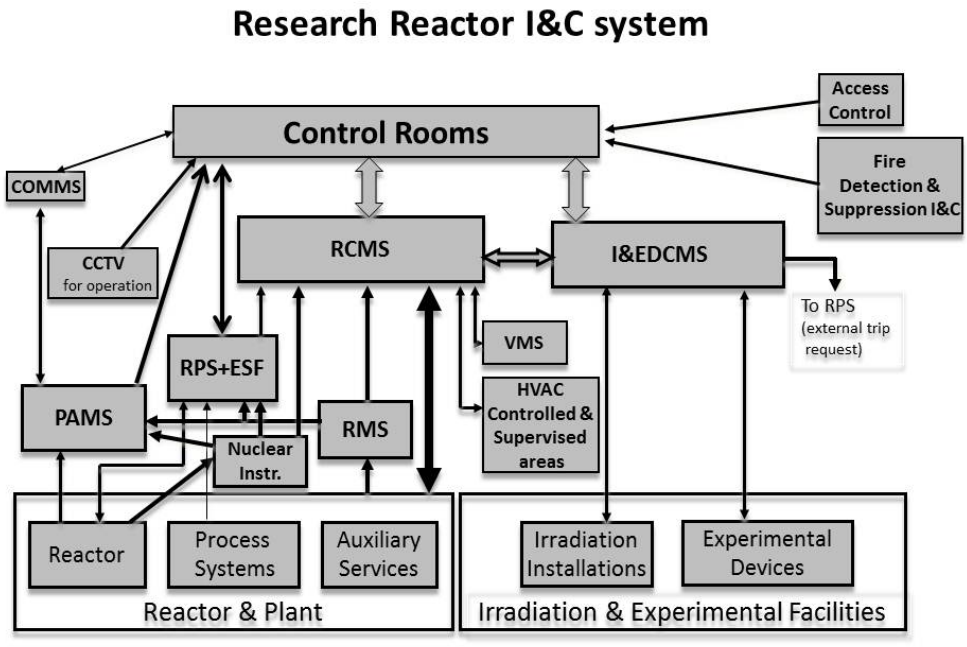

Fig AI.1 Research reactor I&C systems – Block diagram

Acronyms and abbreviations:

CCTV: Close Circuit Television;

COMMS: Communication System;

ESF: other Engineering Safety Features initiation I&C;

HVAC: Heating Ventilation and Air Conditioning for Controlled and Supervised areas;

I&EDCMS: Irradiation & Experimental Devices Control and Monitoring System;

Instr.: Instrumentation;

AMS: Accident monitoring system;

RCMS: Reactor Control and Monitoring System;

RMS: Radiation Monitoring System;

RPS: Reactor Protection System; and

VMS: Vibration Monitoring System.

MAIN I&C SYSTEMS DESCRIPTION

Reactor Protection System (RPS)

1.3. The reactor protection system is a set of components designed to monitor reactor operation parameters (neutron power and period, coolant flow rate, inlet and outlet temperatures, pressure drop in reactor core, etc.), 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 should be measured by two or more independent channels. The automatic actions are initiated on the basis that the logic arrangement for the protective action initiations comply with the single failure criteria and, when three independent channels are available, the logic arrangement of two out of three should be used to prevent the initiation of protective actions by spurious signals. A reactor protection system also could be actuated manually by the operator, the experimenters or from irradiation & experimental devices control and monitoring system. A trip of the RPS results in shutdown of the reactor.

Other Engineering Safety Features Initiation I&C (ESF)

1.4. The engineering safety features initiation I&C is a set of components designed to, upon request, initiate the action of the emergency core cooling, decay heat removal, confinement isolation and confinement heat removal systems. Also, it could be actuated manually by the operator. A trip in the ESF results in the initiation of one or more of the actions mentioned before. The functions of the ESF could be included in the RPS.

Accident Monitoring System (AMS)

1.5. Accident monitoring system is becoming an important feature of nuclear facilities. Its purpose is to provide the operators and their backup teams with necessary accident management information and to ensure that the sources of this information are, and remain, trustworthy. Under accident conditions, the operators require information so that they can:

(a) Perform those preplanned manual control actions for which automatic control is not provided and which are necessary to prevent or mitigate the consequences of the accident. Such actions, specified in the safety analysis report, are compiled in the accident management procedures;

(b) Determine whether critical safety functions related to reactivity control, core cooling, reactor coolant system integrity, heat sink, containment integrity and radioactivity surveillance are challenged and are being accomplished by the RPS, the engineered safety features system and/or their essential support systems.

Nuclear instrumentation

1.6. The nuclear instrumentation follows the value and evolution of the neutron flux of the reactor in all its operational states as this parameter is of the highest relevance to assure a safe operation of the reactor. It also provides the means to establish a suitable control strategy to start up the reactor and to keep it in a stable operation at different power levels.

Reactor Control and Monitoring System (RCMS)

1.7. At the lowest level of the I&C systems resides the process instrumentation (detectors, sensors, switches) which measure process parameters and actual state (position) of actuators, and are connected to the reactor control & monitoring system.

1.8. Reactor control and monitoring system is intended for reliable monitoring of reactor performance and its safe operation. RCMS provides start-up, automatic adjustment of power, compensates fuel burn-up, and provides interlocks for safe operation. RCMS is built using fail-safe and redundant devices to receive and process signals from a large amount of sensors, actuate the corresponding control drivers as well as to present the reactor status information for the operator at the main console of the reactor (the main human machine interface).

Radiation Monitoring System (RMS)

1.9. The radiation monitoring system is designed for continuous radiation monitoring of nuclear facilities as well as surrounding areas to identify the possible release of radioactive materials or radiation due to a failure of the technological equipment, the integrity of protective barriers, the effectiveness of water purification systems, confinement isolation, filters, and ventilation systems among the most relevant systems or components.

Heating Ventilation and Air Conditioning System (HVAC)

1.10. Heating, ventilation and air conditioning systems are used for assuring and maintaining adequate environment conditions for both personnel and equipment by providing ventilation, air quality and temperature control. The ventilation system also helps in maintaining the radiological conditions by pressure gradients, use of appropriate filters, etc. Modern electronic equipment generates much less heat than older types but, nevertheless, excess temperature can degrade performance and air-conditioning, as a means of removal of excess heat from I&C safety systems, should meet the requirements specified for safety system support features. In regions with a tropical climate or high humidity, the proper design of ventilation systems (physical separation, redundancy and closed cycle) may be the only way to eliminate a source of potential common mode failure in I&C equipment. Nevertheless, in some facilities, the

reactor control and monitoring system has the capability to send remote commands to the heating, ventilation and air conditioning systems (i.e. remote trip of the emergency ventilation system).

Vibration Monitoring System (VMS)

1.11. Vibration monitoring system provides a means of monitoring and detecting abnormal vibration conditions on reactor main rotary equipment. The reactor control and monitoring system is used to pass the information of the vibration monitoring system to the control room.

Control Rooms

1.12. Sufficient controls, indications, alarms and displays are provided in main control room (MCR) 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 maintained.

1.13. The minimum set-up of the MCR includes the human system interfaces that operator needs to:

- safely operate the reactor in all its operational states
- monitor the safe operation of the reactor;
- monitor the appearance of alarms;
- perform and confirm a controlled shutdown;
- actuate safety-related systems;
- perform and confirm a reactor trip;
- perform and confirm the actuation of the ESFs
- monitor the status of fission product barriers;
- keep the reactor in a safe shutdown; and
- implement emergency operating procedures.

1.14. The alarm annunciators show status of systems. Safety systems have audible and visible alarms on operator's console or control panel to provide warning on violation of limits and conditions of safe operation. Operators can access all signals through the main console of the reactor control and monitoring System. Also consoles and displays for the experimental and irradiation facilities are usually located in the main control room.

1.15. Supplementary control room, if it is applicable, provides remote reactor shutdown possibility if it cannot be done from the main control room. Sufficient controls, indications, alarms and displays should be provided in the supplementary control room to initiate, supervise and monitor a reactor shutdown to a safe state and to provide assurance that a safe state has been reached and maintained.

Irradiation & Experimental Devices Control and Monitoring System (I&EDCMS)

1.16. The primary use of a research reactor is the production of neutrons for research and for neutron irradiation of materials. Irradiation installations include equipment that is used to place, move, and organize samples. A dedicated and tailored I&C system is designed to control and monitor these operations. Experimental and irradiation installations may have an impact on the reactor safe operation, so the parameters of the experimental devices that affect the safety of the reactor should be displayed in the main control room. Also trip signals from I&EDCMS to RPS could be provided as demanded by safety analysis.

Communication System (COMMS)

1.17. Communication systems is the link for the operators of the main and supplementary control rooms, reactor hall, process areas, staff of the irradiation and experimental devices, other internal locations within the facility and for external emergency organizations, A voice announcement system is used for making announcements that can be heard by all personnel on site and in the facility or to report an emergency or unforeseen circumstances requiring immediate response.

Close Circuit Television (CCTV)

1.18. Close circuit television is a useful aid, which allows the operator to monitor and supervise relevant operational or maintenance tasks or activities that are executed by the operating personnel of the reactor.

Fire detection and suppression I&C

1.19. This independent system has the capability to identify the presence of fire in the facility and, upon this event, initiate automatic fire suppression in the affected areas. Fire detection panels should be located in the control rooms to provide information to the reactor operators.

Access control

1.20. Physical access control system belongs to the physical security system and has the capability to supervise and manage the movement of the personnel in the facility. Access control panels may be located in the control rooms to provide the reactor operators with relevant information.

CONTRIBUTORS TO DRAFTING AND REVIEW

Abou Yehia H.	International Atomic Energy Agency
Boeck H.	Atominstitut der Österreichischen Universitäten, Austria
Boogaard J.	International Atomic Energy Agency
Busto A.	International Atomic Energy Agency
Diakov O.	International Atomic Energy Agency
Drexler J.	INVAP, Argentina
Hargitai T.	International Atomic Energy Agency
Johnson G.	International Atomic Energy Agency
Kim Hyung K.	KAERI, Republic of South Korea
Lokantsev A.	SNIIP, Russian Federation
Muhlheim Michael D.	Nuclear Science and Technology Division, Oak Ridge National Laboratory, United States of America
Rodriguez L.	AREVA, France
Shirley A.	Thermo Fisher Scientific, United States of America
Shokr A.M.	International Atomic Energy Agency
Waard J.	Nuclear Research and Consultancy Group (NRG), Netherland
Winfield D.	International Atomic Energy Agency