DS436 Draft 2

Date:

IAEA SAFETY STANDARDS

for protecting people and the environment

Action: SPESS Step 7 - First review of the draft safety standard by the Safety Standards Committees.

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 is part of the set of publications developed within the framework of the IAEA Research Reactor Safety Programme, which covers all of the important areas of research reactor safety. It supplements and elaborates upon the safety requirements for design and operation of the Instrumentation and Control (I&C) system for research reactors that are established in Section 6 and 7 of the IAEA Safety requirements Publication NS-R-4 on the Safety of Research reactors [1].

1.2 Ageing and obsolesce of I&C systems is fast due to the extremely rapid development in the field of electronics. During the lifetime of a research reactor one or more refurbishment of I&C system can be predicted. There are different reasons demanding I&C modernization project such as improvement of maintainability and reliability, new utilization or experiments in research reactors, enhancement of safety, etc. The advances in technology will require special attention to the safety classification of I&C systems, to the development in the use of computer based I&C systems, to the significant structural changes of I&C systems caused by the intelligent devices, and to the software development including verification, validation and quality assurance.

OBJECTIVE

1.3 The objective of this Safety Guide is to provide guidance on the I&C systems important to safety in research reactors, including all I&C components, from the sensors allocated to the mechanical systems to the actuated equipment, operator interfaces and auxiliary equipment.

1.4 This Safety Guide deals mainly with requirements for those I&C systems that are important to safety. It expands on paragraphs 6.136-6.144 of Ref. [1] in the area of the design of I&C systems important to safety.

1.5 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 and other organizations involved in the research reactor project.

SCOPE

1.6 This Safety Guide provides general guidance on I&C systems important to safety which is broadly applicable to research reactors. The guidance presented is focused on the design principles for systems important to safety that warrant particular attention, and should be applied to both the design of new I&C systems and the modernization of existing systems. Guidance is provided on how design principles should be applied, on the basis of a method of classifying systems by their importance to safety.

STRUCTURE

1.7 Section 2 discusses the identification of I&C functions and systems, the method and the basis of safety classification into safety and safety related functions and systems. Section 3 describes how I&C systems are arranged into a hierarchy. Section 4 and 5

gives an overview of general and specific design requirements of I&C systems, while Section 7 expands on the guidance given in Section 4 in the area of human–system interfaces. The operation aspects of I&C 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 I&C systems configuration management. Section 10 presents the I&C systems modification and modernization aspects.

PERCEPTION OF NEEDS FOR I&C MODERNIZATION

1.8 A large fraction of the approximately 280 research reactors now in operation are operating for many years. During this period a fast development in electronics took place and many of these reactors are using classical I&C systems. Although failed instruments have been replaced during this period, in view of safety requirements most of the I&C systems are a mixture of instruments from various suppliers with a variety of technical standards.

1.9 It is obvious that at a certain stage a decision has to be made to modernize the overall I&C system. It has also to be considered that such a modernization may require a period of extended shut-down or unavailability of the facility. Such a decision has to be carefully planned in view of the future of the research reactor facility. In certain cases it could be that decommissioning the facility is the better option.

1.10 One major reason to decide for an I&C modernization at a given facility is obsolescence of the present I&C system, the unavailability of spare parts and an increased failure rate of the I&C system leading to frequent reactor shut downs, long repair periods and therefore resulting in high 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 evidently the technological progress in I&C systems leading to higher reliability of I&C systems, improvement of human-system interface and extensive and fast data collection and processing.

1.11 Besides such technically based decisions also other aspects may influence the final decision for modernization of the I&C system of a given facility as technical specification and/or regulatory requirements might have been changed in the past. As an additional benefit an I&C modernization process might also be accompanied with the decision of a facility power increase, and it is important to take into consideration in these assessments that the facility will be forced to continue to enhance safety, to increase reliability, to shorten outage time and to reduce staff.

Forecasting problems and limits in the nearest future

1.12 Before entering the modernization project, it is advisable to collect information on needs and limitations in the current I&C 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 I&C system the decision maker should assess and attempt to foresee possible future problems and limits of the current I&C system.

2. SAFETY CLASSIFICATION OF INSTRUMENTATION AND CONTROL SYSTEMS

GENERAL CONSIDERATIONS

2.1 For the purposes of this guide the following classification scheme is used to grade recommendations according to safety significance:

- All I&C functions, systems, and components fit into one of two safety categories: important to safety or not important to safety (see Fig.1);
- functions, systems, and components important to safety are further categorized as either safety or safety-related;
- The ***main safety functions*** for a research reactor are:

    i. *Control* of *reactivity;*

    ii. Cooling of *radioactive material; and*

    iii. *Confinement* of *radioactive material.*

- I&C systems important to safety are those systems used to accomplish functions important to safety.
- functions, systems, and components important to safety are those which significantly contribute to:

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

    ii. remove *residual heat* from the reactor core after shutdown, and during and after appropriate *operational states* and *accident conditions;*

    iii. reduce the potential for the release of *radioactive material* and to ensure that any releases are within *prescribed limits* during and after *operational states* and within *acceptable limits* during and after *design basis accidents.*

    iv. permit the safe operation of the reactor

2.2 Safety systems consist of the protection system, the safety actuation systems and the safety system support features. Components of safety systems may be provided solely to perform safety functions or may perform safety functions in some facility operational states and safety related functions and/or non-safety functions in other operational states with the premise that the design should consider to do not add any component or function that are not strictly required by the highest safety classification.

2.3 Safety related systems are systems important to safety and performing other safety functions not mentioned in par. 2.2.

2.4 Systems not important to safety are those systems that do not belong to systems important to safety.

2.5 For I&C systems having safety importance, graded approach to the requirements of NS-R-4 can be applied but the extent of grading should be clearly justified in the Safety Analysis Report (see paragraph 1.14 of Ref. [1]).

2.6 Additional guidance on the application of a graded approach can be found in the Safety Guide [3]: The Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors.

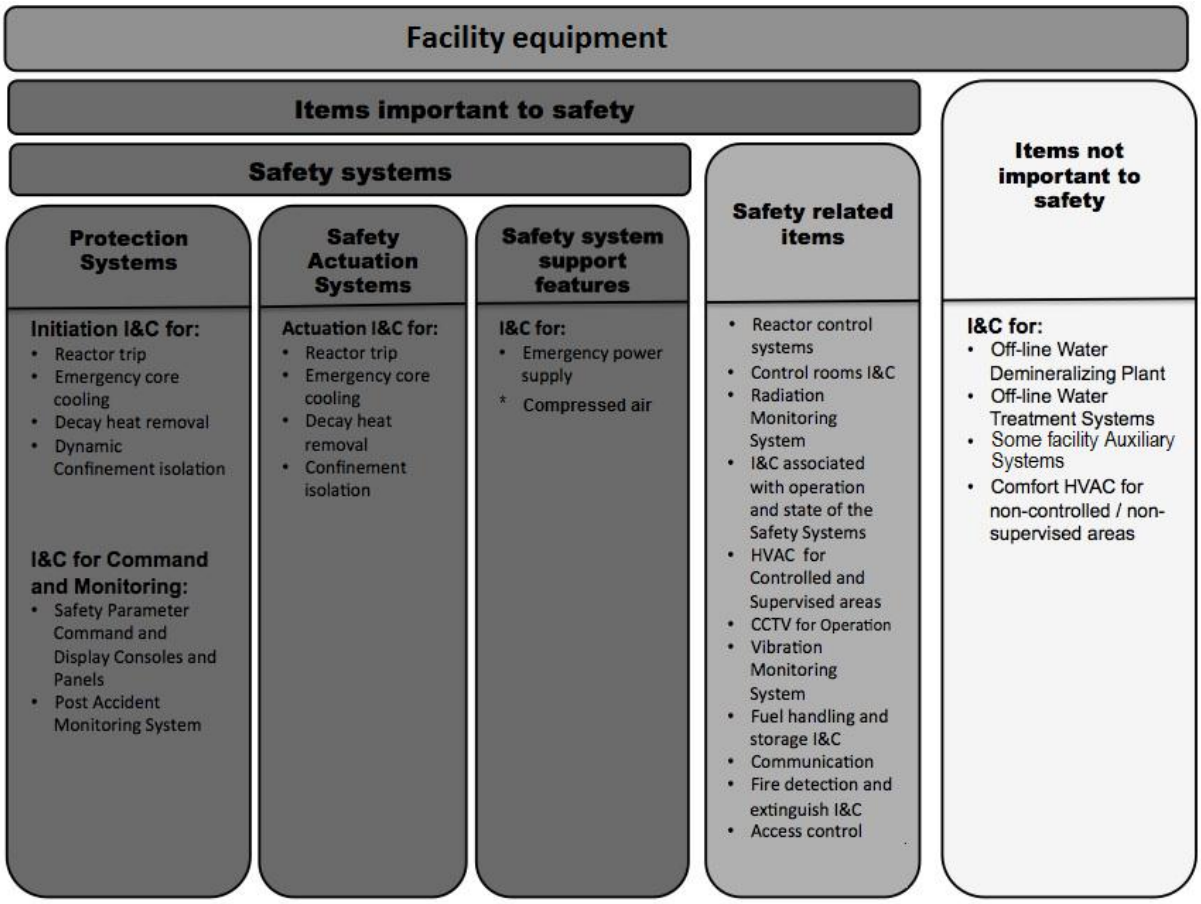

FIG. 1 Examples of I&C Systems classified in connection to their importance to safety.

SAFETY SYSTEMS

2.7 Functions of safety systems are to ensure timely detection of violations of limits and conditions for safe operation of research reactor and automatically initiate reactor shutdown, emergency core cooling and residual heat removal, and containment of radioactive materials and/or limitation of accidental releases.

2.8 Safety systems perform a number of functions to ensure the safe operation of a research reactor such as:

- Shut down the reactor as necessary to prevent anticipated operational occurrences from leading to design basis accident conditions;
- Maintain the reactor in a safe shutdown condition after all shutdown actions;
- Remove residual heat in appropriate operational states and design basis accident conditions;

- Confine radioactive materials and control of operational discharges, as well as limit accidental releases;
- Mitigate the consequences of beyond design basis accidents (BDBAs).

2.9 The safety system should automatically initiate the required protective actions for the full range of PIEs to terminate the event safely.

2.10 The examples of I&C safety systems are:

- Initiation I&C for:
  - Reactor trip, which consists in the Reactor Protection System that includes:
    - Sensors and instruments which monitor neutron flux, flow rates, temperatures, pressures, and other safety variables and by demand, experimental facilities and devices safety variables.
    - The system which processes these signals compares them against the safety system settings and initiates the reactor trip if any of these settings has been exceeded.
  - Emergency core cooling;
  - Decay heat removal;
  - Confinement isolation.

- I&C for Command and Monitoring:
  - Safety Parameter Command and Display Consoles and Panels; and
  - Post-Accident Monitoring System.

- Actuation I&C for:
  - Reactor trip;
  - Emergency core cooling;
  - Decay heat removal;
  - Confinement isolation.

- and I&C for:
  - Emergency Power Supply.

SAFETY RELATED SYSTEMS

2.11 Safety related systems perform a number of functions to ensure the safe operation of a research reactor such as:

- Provide for reactivity control within safe limits;

- Remove heat from the core;
- Maintain sufficient coolant for core cooling in normal operational states and following any PIE's;
- Maintain the integrity of the cladding for the fuel in the reactor core;
- Maintain the integrity of the reactor coolant boundary;
- Minimize the radiation exposure of personnel;
- Prevent degradation of reactor safety originating from experimental devices and facilities;
- Provide information to the operator regarding the state of the facility.

2.12 Control functions assure that the research reactor facility is controlled and kept within its operating limits and conditions (OLCs), thereby contributing to nuclear safety by minimizing the demand on safety system.

2.13 Monitoring and display functions provide the interface between the reactor facility, reactor operators and maintenance personnel. These functions are related to safety as they allow the facility personnel to intercept transients and maintain the reactor within the OLCs.

2.14 Some examples of safety related I&C systems are:

- Reactor control systems;
- Control rooms I&C;
- Radiation Monitoring System;
- I&C associated with operation and state of the Safety Systems;
- I&C for HVAC for Controlled and Supervised areas;
- I&C for CCTV for Operation;
- Vibration Monitoring System (VMS);
- Fuel handling and storage I&C;
- Communication;
- Fire detection and extinguish I&C; and
- I&C for access control

SYSTEMS NOT IMPORTANT TO SAFETY

2.15 Systems not important to safety support operation of the facility while having no impact on the reactor's safety.

2.16 Some examples of I&C systems not important to safety are I&C for:

- Off-line Water Demineralizing Facility
- Off-line Water Treatment Systems
- Some Facility Auxiliary Systems
- Comfort HVAC for non-controlled / non-supervised areas

METHOD OF CLASSIFICATION

2.17 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 Probabilistic Safety Assessment (PSA). The basis for such classification should consider:

- The safety function(s) to be performed by the I&C system;
- the consequences of the I&C system's failure (failure or faulty performance of the function(s));
- the probability that the I&C system will be called upon to perform a safety function; and
- following a PIE, the time at which or the period for which the I&C system will be called upon to operate.

2.18 In addition to considering the factors mentioned above, the following factors should also be taken into account in determining the class of the I&C system:

- the probability of PIEs and the potential severity of their consequences if the I&C system provided fails (e.g.: high, medium or low probability, with high, medium or low consequences (e.g. radiological consequences));
- the probability that the I&C system will be called upon to perform a safety function;
- the potential of the I&C system itself to cause a Postulated Initiating Event (PIE) (i.e. the I&C system's fail-safe modes), the provisions made in the safety systems or in other I&C systems covered by this Safety Guide for such a PIE (i.e. provisions for detection of I&C system failure), and the combination of the probability and consequences of such a PIE (i.e. frequency of failure and radiological consequences);
- the timeliness and reliability with which alternative actions can be taken (e.g.: immediate/low reliability, beyond 30 minutes/high reliability); and
- the timeliness (e.g.: up to 12 hours, beyond 12 hours) and reliability with which any failure in the I&C system can be detected and remedied.

2.19 The criteria, should be chosen so as to provide a quantitative and/or qualitative indication of the relative importance to safety of the I&C system being classified.

2.20 Once each of the factors has been considered and analysed for each I&C system a decision should be made on system's classification.

DESIGN, CONSTRUCTION AND MAINTENANCE OF I&C SYSTEMS

2.21 All I&C systems and equipment should be designed, constructed and maintained in such a way that their specification, verification and validation process, quality assurance, quality control and reliability are commensurate with their safety classification.

2.22 All I&C 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 will not propagate to a system classified in a higher class. Equipment providing the function to prevent the propagation of failure should be treated as being of the higher class.

2.23 It should be ensured that the classification of necessary service systems (electrical, pneumatic or hydraulic power supply, lubrication systems) is commensurate with the classification of the safety functions that they support.

3. OVERALL I&C SYSTEM ARCHITECTURE

GENERAL

3.1 The research reactor should be provided with sufficient Instrumentation and Control systems in the form of an architectural design for a safe operation of the research reactor during normal operation, shut down, refuelling, maintenance and, to automatically initiate reactor shutdown, emergency core cooling, residual heat removal, and the containment of radioactive materials and/or limitation of accidental releases during Anticipated Operational Occurrences (AOO) or during and after accident conditions.

3.2 I&C system architecture should fulfil the IAEA Safety Standard NS-R-4 [1], Safety Objectives, Concepts and Principles [para.2], and Design [para.6]. I&C system architecture should support all I&C functions needed to fulfil the design basis. The set of Research Reactor I&C systems may vary depending on the type of reactor and their operation modes and usually include those systems stated in section 2 as examples of I&C systems.

3.3 The overall I&C system architecture provides high level definition of the I&C systems, the assignment of I&C functions to these systems, and the communications between I&C systems (Interfaces) between them and with the facility.

3.4 Modern I&C systems are more highly integrated than were the last generations of I&C systems. The architecture of highly integrated systems should be carefully considered to ensure proper implementation of the defence in depth concept. A well designed architecture can reduce the complexity of I&C systems and can locate essential complexity in systems where it can be better managed or where it will pose less risk to the facility safety. For example, in existing designs the separation of I&C functions between safety and safety related systems allocates complex functions to safety related systems and limits the safety systems to the performance of simpler functions.

3.5 The identification of all the different and individual I&C Systems of a Research Reactor that can be included in a particular facility depends on the type of reactor, the purpose and its operation modes. They are shown and described in Annex I - Research Reactor`s I&C Systems.

DEFENCE IN DEPTH

3.6 As it is stated in the Safety Standard, Safety of Research Reactors, Safety Requirements, NS-R-4 [1], "*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".

3.7 The design should incorporate the defence in depth. The levels of defence should be independent as far as is practicable.

3.8 INSAG-10 [6] and INSAG-12 [7] further amplify the previous paragraphs.

3.9 The implementation of the defence-in-depth concept for I&C is mostly achieved at the level of the overall I&C architectural design as a mean to achieve independence between levels of defence in depth.

3.10 The overall I&C architecture should implement a defence in depth concept.

3.11 The overall I&C architecture should not compromise the Defence in Depth strategy of the facility design.

3.12 For I&C, Defence in depth should consist of implementing successive I&C functions designed to limit the consequences of a design basis event to an acceptable level despite the failure of I&C functions designed to respond first.

INDEPENDENCE

3.13 The Independence is intended to prevent the propagation of failures from the item affected by the failure to other redundancies, or from a system to other system independently to the safety class that they belong.

3.14 The overall I&C architecture should neither compromise the independence of the Structure, Systems and Component safety classes, nor the independence implemented at the different levels of defence in depth.

3.15 Safety systems should be independent from systems of lower safety classification as necessary to ensure that the safety systems can perform their safety functions during and following any design basis event that requires these functions without any interference or degradation from those systems of lower safety classification.

3.16 Safety items should be independent of the effects of the design basis accidents to which they must respond.

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

CONSIDERATION OF COMMON CAUSE FAILURE

3.18 A common cause failure (CCF) is defined as the concurrent failure of two or more structures, systems or components due to a single event or cause.

3.19 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.

3.20 Latent failures and common failure modes which potentially might result in a common failure of the redundancies should be identified, and justification should be provided

for any that need not be considered as credible sources of CCF between systems or individual components.

3.21 Justification that a CCF need not be considered may, for example, be based on the component dependability, technology, or feedback gained over its wide usage.

3.22 The consequences of a PIE in combination with a CCF that prevents necessary reactor protection system response to the PIE should be no greater than those accepted for design based conditions.

3.23 The accident sequences and consequences resulting from the combination of a PIE and CCF of the reactor protection system may be analysed using best estimate methods.

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

3.25 Often it is necessary to provide a Diverse Actuation System (DAS) to limit the consequences of the PIE in conjunction with CCF in one or more protection system functions.

3.26 A complete elimination of all vulnerabilities of I&C systems and architecture to CCF is not required, but justification should be provided for accepting identified vulnerabilities that have are not addressed.

OVERALL ARCHITECTURAL DESIGN OF THE I&C SYSTEM

3.27 The overall I&C architecture should:

- Provide all I&C functions needed to fulfil the design basis;
- provide systems necessary to support the defense in depth concept of the facility;
- provide a hierarchical system design where I&C safety systems keep the highest hierarchy and priority to perform the safety functions for which they have been designed.
- define the interfaces between the individual I&C systems, and
- divide the overall I&C system into individual systems as necessary to:

    a) Support 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 to the main control room and supplementary control rooms;

    f) Provide necessary operator controls in the main control room and supplementary control rooms; and

g) Provide automatic controls necessary to maintain and limit the process variables within the specified normal operational ranges.

3.28 The inputs to the overall I&C architecture design process should refer to the facility safety design basis documents, which should provide the following information:

a) The defense in-depth concepts of the facility;

b) The groups of functions to be provided to address Postulated Initiating Event (PIE) 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) Member State requirements for I&C licensing, e.g. security, software qualification; and

i) Member State requirements with respect to operational requirements (i.e., the I&C design as it affects the interface with facility operators) for systems important to safety.

3.29 The I&C systems should be architecturally designed in a top-down approach (see Figure 3.1) having different monitoring, processing, acquisition/actuation and sensors/actuator drivers levels. The monitoring functions should be allocated at the supervision level; the calculation, algorisms, 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 in the facility level.

3.30 The I&C system top-down approach requires the inclusion of three independent communication levels namely:

a) Supervision communication level;

b) Control communication level; and

c) Field communication level,

to be possible to establish a communication interface between the different top-down approach architectural levels and the reactor and facility systems.

3.31 The use of diversity, redundancy, physical separation, electrical and functional isolation, in the overall architectural design of the I&C system, should be based on the safety classification of each I&C system and the impact in the safe state of the reactor upon the presence of an I&C system's failure (failure or faulty performance of the function(s)) and the probability that a specific I&C system will be called upon to perform a safety function.

3.32 The use of the same design features, those mentioned in 3.31, where these features be reasonably and justifiably applicable to, should be enough to avoid that a failure in one level causes failures in another subsequent level(s).

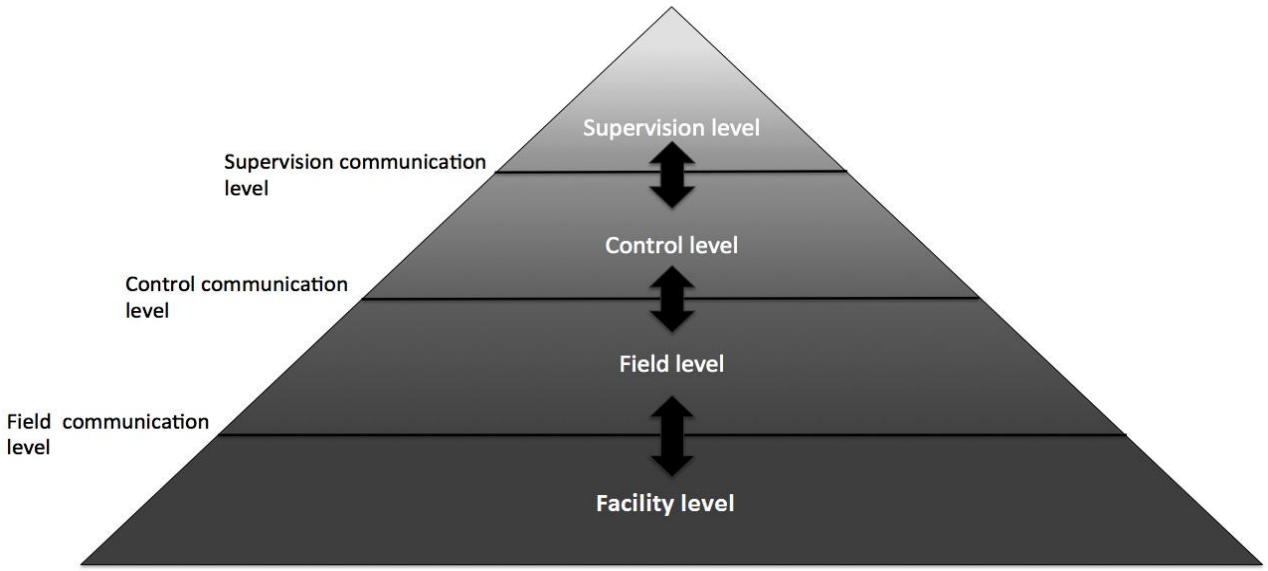

Figure 3.1: Top-down architectural approach design

4. DESIGN GUIDELINES

GENERAL

4.1 I&C systems should fully implement the requirements of their design bases.

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

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

4.4 The intent of avoiding complexity is to keep the I&C system as simple as possible but still fully implement its safety requirements. Examples of complexity to be avoided are the inclusion of functions not important to safety, architectures involving overly complex communication or system interactions, use of design and implementation features not amenable to sufficient analysis or verification, and use of implementation platforms that are too complex to facilitate an adequate safety demonstration. Careful documentation and review of the rational for each requirement is one effective means for avoiding inessential complexity.

DESIGN BASES

4.5 Each research reactor I&C system important to safety should have design bases that specify the following:

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

b) The various facility and experimental configurations that the I&C must accommodate.

c) Functionality requirements for each facility state and during extended shutdown.

d) PIEs to which the system must respond.

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

f) The ranges, rate of change, required accuracy of input and output signals of the system.

g) Constraints on values of process variables.

h) Requirements for periodic testing, self-diagnostics, and maintenance.

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

j) The acceptance criteria of the system.

k) Security and operational constraints.

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

m) The range of natural phenomena hazards under which the system is required to perform functions important to safety.

n) Conditions with the potential to functionally degrade the performance of systems important to safety and the provisions to be made to retain the capability.

4.6 In addition the design bases for protection and reactor shutdown systems the following should be specified as well:

a) The limiting values of actuation for safety systems.

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

c) The conditions 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

4.7 The level of system reliability should be commensurate with the safety importance of the system and could be achieved by means of a comprehensive strategy that uses various complementary means (including an effective regime of analysis and testing) at each phase of development of the system and a validation strategy to confirm that the design requirements for the system have been fulfilled. All I&C systems important to safety regardless of technology should be developed using a defined development process that includes verification and validation. In case of safety systems the verification and validation process should be independent.

Single failure

4.8 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.

4.9 I&C systems important to safety have a critical role in achieving the three basic safety functions — shutting down the reactor, providing cooling, in particular for the reactor core, and confining radioactive material. In the design of I&C safety systems the single failure criteria should be applied so that the system is capable of performing its task in the presence of any single failure.

4.10 The design of I&C systems important to safety should include provisions for detecting all identifiable failures in the system by means such as anomalous indication, alarm, or periodic testing.

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

a) Very rare PIEs

b) Very improbably consequences of PIEs

c) Withdrawal of certain components from service for limited period of time for the purposes of maintenance, repair, or periodic testing.

d) Components whose likelihood of failure can be shown to be sufficiently remote as to be discounted.

Redundancy

4.12 The principle of redundancy should be considered as provision of alternative (identical or diverse) SSCs, so that any of them can perform the required function regardless of the state of operation or failure of any other SSC.

4.13 The principle of redundancy is an important design principle for improving the reliability of systems important to safety. 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.

4.14 Multiple sets of equipment that cannot be tested individually should not be considered redundant.

4.15 The degree of redundancy should depend upon the potential for failures that could degrade reliability. For all I&C systems important to safety redundancy should be applied to the extent necessary to meet reliability and unavailability requirements of the design basis. For I&C 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.

4.16 When feasible, redundant safety systems should be physically separated from each other and from systems of lower safety classification. Moreover, the concept of independent equipment should be used.

Common cause failure

4.17 The design of I&C system important to safety should provide additional features to minimize the possibility of common cause failures by means of independence, physical separation and diversity of equipment.

Independence

4.18 The principle of independence (e.g. functional isolation, electrical isolation and physical separation by means of distance, barriers or a special layout for reactor components) should be considered and applied, as appropriate, to enhance the reliability of systems.

4.19 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 errors.

4.20 Design of certain areas of the facility such as containment penetrations, cable spreading rooms, equipment rooms, control rooms etc. should consider the extent to which independence might be lost after a PIE.

4.21 Different safety functions should be performed by different modules, components or systems to avoid the influences from the mode of operation or failure of one module, component or system on another.

4.22 Electrical and data connections between redundant systems and connections between safety systems and systems of a lower safety classification should be designed so that no credible failure in one system will prevent the other system(s) from meeting their performance and reliability requirements.

4.23 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 fiber), relays, cable or component shielding, separation, distance, or combinations thereof.

4.24 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.

4.25 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,

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

4.26 If data communication channels are used in safety systems they should satisfy the recommendations for independence (functional isolation, electrical isolation and physical separation).

Diversity

4.27 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*), and different sizes of equipment, different manufacturers, and types of equipment that use different physical methods (which provide *physical diversity*).

4.28 Diversity in I&C 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 significant event.

4.29 Diversity should provide defence against common cause failures, it is complementary to the principle of defence in depth and significantly increases the probability that safety actions will be performed when necessary.

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

4.31 Where independence is claimed between two systems (for example a RR's main reactor protection system and its second diverse reactor protection system) through multiplying their failure probabilities within the PSA, then the system platforms should be diverse and that diversity should also extend to the facility sensors and actuators.

4.32 Diversity applied to I&C systems should include:

- Functional diversity: could be achieved by systems providing different physical functions or means resulting in the same safety effects.
- Equipment diversity: achieved by sensors and systems using different technology, and
- Variable diversity: achieved by the use of more than one different type monitored parameters to identify an event that could require the initiation of a protective action.

4.33 The diversity should extend to the equipment's components to ensure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers' names are insufficient without consideration of this possibility.

4.34 It should be considered both the scope and the type of the diversity provided. The level of conservatism may be achieved by providing diversity to protect against the more frequent PIE, without extending full diversity to cover very unlikely PIEs or low consequence PIEs, since the risk of such events may be acceptable despite the possibility of common cause failure.

Failure modes

4.35 The failure modes of I&C systems important to safety should be known and properly documented using "Failure Mode and Effect Analysis" methods. As far as possible the more probably failure modes should neither place the system in an unsafe state nor cause spurious actuation of safety systems.

4.36 The failure modes of I&C components should be known and documented.

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

4.38 Any identified failures that are not detectable by periodic testing, alarm, or anomalous indication should be assumed to exist in conjunction with single failures when evaluating conformance with the single failure criterion.

Fail-safe

4.39 The principle of fail-safe design should be considered and adopted as appropriate in the design of I&C systems to pass into a safe state, with no necessity for any action to be initiated for any system failure..

DESIGN TO COPE WITH AGEING

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

4.41 Ageing mechanisms that could significantly affect I&C 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 (e.g., mechanical vibration, or chemical degradation) might be relevant to a specific component must be considered.

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

EQUIPMENT QUALIFICATION

4.43 I&C 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.

4.44 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).

c) Seismic qualification for components.

d) Electromagnetic compatibility qualification for systems and components.

4.45 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.

f) Ageing analysis as applicable.

4.46 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.

Suitability and correctness

4.47 The design of I&C systems and components should demonstrate to meet all functional, performance, and reliability requirements important to safety contained in the design bases and equipment specifications.

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

4.49 Examples of performance requirements should include, for example: accuracy and response time requirements.

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

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

Internal and external hazards

4.52 I&C systems and components should be protected against or designed and qualified to withstand internal and external hazards including seismic hazards.

Environmental qualification

4.53 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.

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

4.55 Components should be shown to meet all design basis requirements when subjected to the range of environmental conditions specified in the design basis. It is common practice to apply the most rigorous environmental qualification methods to safety systems and safety components.

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

Electromagnetic compatibility qualification

4.57 The undisturbed operation of electrical and electronic systems and components depends upon their electromagnetic compatibility (EMC) with components located nearby or with which they are connected.

4.58 Significant sources of electromagnetic interference should include, for example, fault current clearance by switchgear or circuit breaker or fuse operation, electric fields caused by radio transmitters, natural sources such as lightning strike, and other man-made sources internal or external to the facility.

4.59 Electromagnetic qualification of I&C systems and components depends upon a combination of system and component design to minimize the coupling of electromagnetic noise to electrical components, testing to demonstrate that components can withstand the expected levels and testing to demonstrate that electromagnetic emissions are within tolerable levels. I&C systems and components could be already qualified in which case; I&C systems and components should be accompanied with the corresponding qualification certificate.

4.60 Systems and equipment, including associated cables, should be designed and installed to withstand the electromagnetic environment in which they are located.

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

- Emission of and immunity to electromagnetic disturbances.
- Emission and conduction of electromagnetic disturbances via cables.
- Electrostatic discharge (ESD),

4.62 The emission characteristics of wireless systems and devices used at the facility as well as those of repair, maintenance and measuring devices should also be taken into consideration. Wireless systems and devices should include, for example, mobile phones, radio transceivers, and wireless data communication networks.

4.63 Any electrical or electronic equipment in the research reactor facility will contribute to the electromagnetic environment that must be withstood by I&C systems important to safety. Therefore, the need to apply limits to electromagnetic emissions should apply to all equipment, not just equipment important to safety.

4.64 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 reactor equipment.

TESTING AND TESTABILITY

4.65 The design of all I&C systems important to safety should include provisions that allow performance of the required testing during reactor shutdown that supports implementation of the guidance given in NS-G-4.4, Ref. [11] and NS-G-4.2, Ref. [12]. Most of the research reactors are operated on relatively short operating cycles therefore provisions for testing during operation generally are not necessary.

Test provisions

4.66 Provisions for testing I&C 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.

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.

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

g) Auxiliary test equipment should be appropriately calibrated.

4.67 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.

4.68 Self-checking features of I&C 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.

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

Preserving I&C functions during testing

4.70 Arrangements for testing include: procedures, test equipment interfaces, installed test equipment and built in test facilities. Arrangements for testing should neither compromise the independence of safety systems nor introduce the potential for common cause failures.

4.71 Test facilities that are permanently connected to safety systems should be considered as part of the safety systems.

Test considerations

4.72 Examples of considerations should include:

- location of sensors such that testing and calibration can be performed at their location;

- location of test devices and test equipment in areas convenient to the equipment to be tested;
- layout or administrative features;
- convenience of component status indication and test connections; and
- have communications facilities as needed to support the tests.

4.73 Where equipment to be tested is located in hazardous areas, the design should consider the provision of facilities to allow testing from outside the hazardous area.

4.74 Design of I&C 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 alarm.

Test programme

4.75 The design of I&C 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.

- A test programme should include:
- a description of programme objectives;
- identification of systems and channels to be tested;
- a master test schedule;
- the reasons and justification for the tests to be conducted and test intervals;
- a description of required documentation and reports;
- a requirement for periodic review of programme effectiveness; and
- specification of the individual test procedures that will be used during the conduct of tests.

4.76 The tests defined in the test programme should ensure that, during and after completion of the tests:

- the overall functional capabilities of the systems are not degraded; and
- the I&C safety systems continue to meet their design basis requirements of functionality and performance.

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

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

4.79 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.

4.80 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.

- 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 are met;
- test all inputs and output functions, such as alarms, indicators, control actions, and operation of actuation devices;
- ensure the safety of the facility during the actual testing; 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.

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

4.82 Temporary modification of computer code in systems and components is not allowed.

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

4.84 Test of a safety system channels should 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.

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

4.86 Test of a safety system should include as much of the function under test as practical (including sensors and actuators).

4.87 Wherever possible, test of a safety system should be accomplished under actual or simulated operating conditions, including sequence of operations.

4.88 Test should be capable of detecting faults in redundant equipment.

MAINTINABILITY

4.89 The design should consider provision of means for the maintenance of I&C systems. The design of I&C systems should include maintenance plans for all systems and components.

4.90 I&C systems and components should be designed so as to minimize risks to maintenance personnel and to facilitate necessary preventive maintenance, troubleshooting, and timely repair.

4.91 Design to facilitate maintenance, troubleshooting and repair includes:

- avoiding locating equipment in areas where conditions of extreme temperature or humidity, and risk of high radiation levels;
- considerations of human factors in performing the required maintenance activities; and
- leaving sufficient room around the equipment to ensure that the maintenance staff can perform their tasks.

4.92 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 to put back in operation again.

DESIGN ANALYSIS

4.93 Safety analysis in design is used to support the design of a new I&C system or modifications to the design of an existing one. Design analyses, including the following specific activities, should be performed to confirm that I&C systems fulfil their design basis requirements. [3]

a) Verification that safety systems comply with the single failure criterion.

b) Verification that the design of I&C systems includes adequate test provisions.

c) Failure Mode and Effects Analysis is often used to confirm compliance with the single failure criterion, and to confirm that all known failure modes are either self-revealing or detectable by planned testing.

d) Verification that the overall I&C system supports the facility defence-in-depth concept.

e) Verification that common cause failure vulnerabilities of I&C safety systems are known and have been adequately addressed.

f) Defence-in-Depth and Diversity Analysis is one means of investigating vulnerability of safety systems to common cause failure.

g) Common cause failure (CCF) vulnerabilities may be addressed by eliminating the vulnerability, providing diverse means of achieving the safety functions subject to the CCF, or justifying acceptance of the vulnerability.

h) Verification that design basis reliability requirements are met.

i) This demonstration may be based on a balance of application of deterministic criteria and quantitative reliability analysis that considers design features such as, for example, redundancy, testability, failure modes, and rigour of qualification.

j) For complicated systems a combination of qualitative analysis, quantitative analysis, and testing is usually needed to verify compliance with design basis reliability requirements.

k) Test facilities that are part of the safety system must be considered when determining system availability.

l) Confirmation that all system requirements have been implemented and validated.

m) Typically traceability analysis is used to confirm implementation and validation of requirements.

n) Confirmation of correct system behaviour following power interruptions and restart or reboot.

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

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

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

SAFETY SYSTEM SETTINGS

4.96 The requirements and operational limits and conditions established in the design for the research reactor facility should include limiting settings for safety systems. The limits and conditions for safe operation include safety system settings for I&C systems.

4.97 Determination of I&C 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.
- Allowable value - the limiting value that a safety system setting may have when tested periodically, 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 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.

4.98 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.

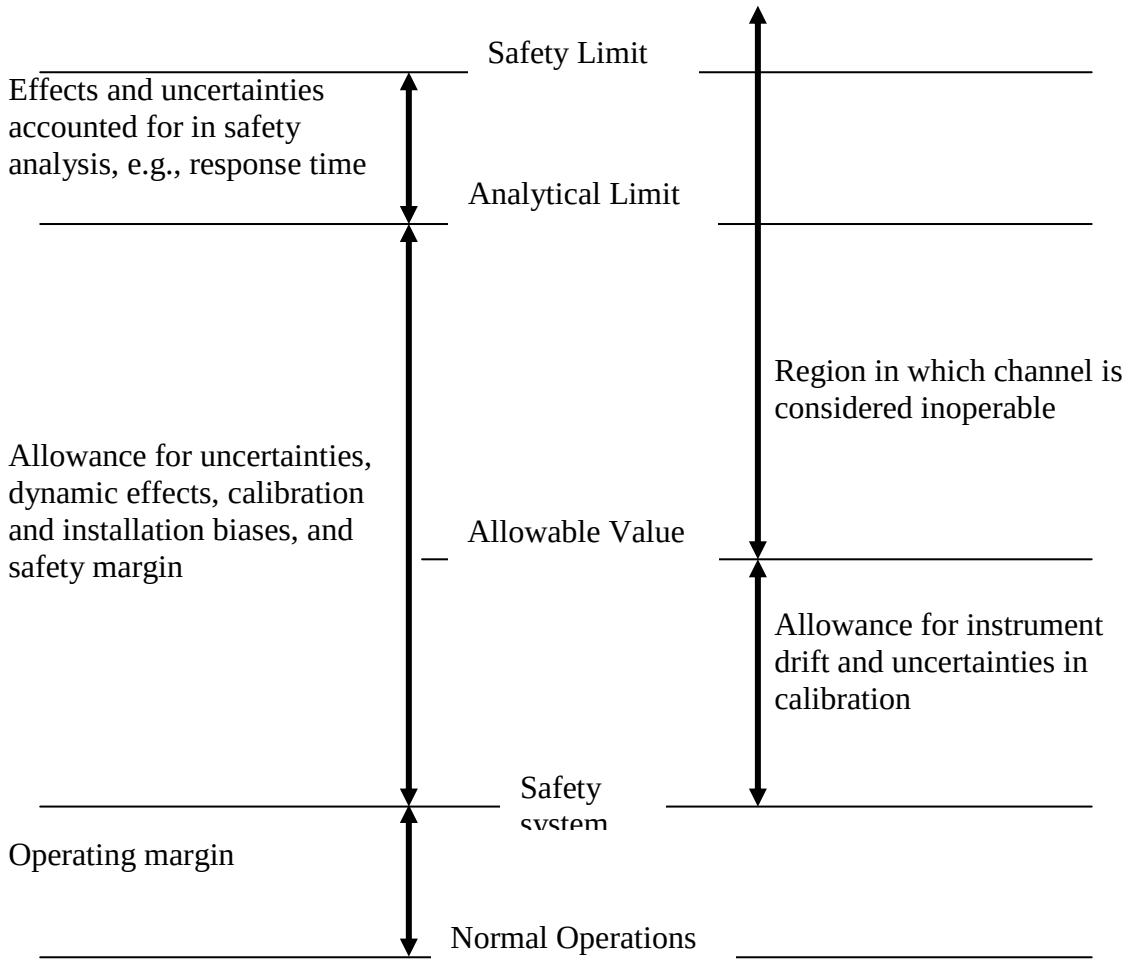

FIG. 4.1 Safety system setting terminology and errors to be considered in safety system setting determination

IDENTIFICATION OF ITEMS IMPORTANT TO SAFETY

4.99 A consistent and coherent method of naming and identifying all I&C components should be determined and followed throughout the design, installation and operation phases of the reactor facility. Clear identification of components is necessary to reduce the likelihood of inadvertently performing maintenance, tests, repair or calibration on an incorrect channel.

4.100 Coherent and easily understood naming and identification of systems and components is important for engineering, construction and maintenance staff as well as for use to label the controls, displays and indications. Components or modules mounted in equipment or assemblies that are clearly identified may not themselves need identification.

4.101 Systems important to safety and their components should be uniquely identified and marked to differentiate them from systems of lower safety category and to differentiate the different redundancy groups from each other.

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.

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.

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 should be identified by the design.

REACTOR PROTECTION SYSTEM

5.8 The protection system should comply with all of the general guidance for design of I&C systems given in the Chapter 4 where applicable.

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

5.10 The 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 maintain the reactor in a safe and stable condition acting in this case as extended ESF I&C system.

5.11 Where two independent reactor protection systems are provided, these two systems should be independent and diverse from each other.

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

5.13 The action initiated by the protection system should be latched so that once an action is started, it will continue even if the initiating state may have ceased 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 operator has sufficient and clearly presented information to make reasoned 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; and
- the operator is provided with sufficient means of reactor control to perform the required actions.

5.15 In addition to any automatic actions, means should be provided to manually initiate reactor trip and any other safety actions of the reactor protection system. 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 functions, including the means for activating and deactivating these inhibit 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 past the low power trip safety system setting. In this guide such reactor protection system inhibit functions are called operational interlocks and are classified as safety interlocks.

5.17 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.

5.18 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.

5.19 The general guidance for design of I&C systems gives recommendations on temporary connections used for maintenance and testing (see par. 4.80). That guidance should be strictly applied to reactor protection systems.

5.20 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 need to take in account the following:

- inaccuracy of instrumentation;
- uncertainty in calibration;
- instrument drift; and

- instrument and system response time.

5.21 If a computer based system is intended to be used in reactor protection system, it should prove to offer advantages of improved reliability, accuracy, functionality and maintainability in comparison with analogue systems.

5.22 Where the necessary integrity 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 (e.g. hard wired backup system) should be provided.

5.23 Diversity may be provided internal to the reactor protection system or by a separate and independent system, as long as the design bases are met.

5.24 Diverse systems may be hardwired or computer-based as long as the existence of diversity can be justified. Normally, it is easier to justify diversity between computer-based and hardware-based systems than between two computer-based systems.

5.25 Where a computer based system is intended to be used in a reactor protection system, the following requirements should be applied:

- hardware and software of high quality and best practices should be used;
- the whole development process, including control, testing and commissioning of the system should be systematically documented and reviewed; and
- independent verification and validation process should be applied.

5.26 "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." ([1], para. 6.104)

OTHER I&C SYSTEMS IMPORTANT TO SAFETY

5.27 The reactor should be provided with sufficient instrumentation for monitoring the operation and process systems of the reactor during normal operation, shut-down, refuelling and maintenance, and for recording all variables important for safety.

5.28 The reactor should be provided with sufficient indicating and recording instrumentation to monitor important reactor parameters during and following anticipated operational occurrences and accident conditions.

5.29 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.

5.30 Audible and visible alarm systems should provide an early indication of changes in the operating conditions of the reactor if these conditions could lead to a reduction in safety.

5.31 The safe normal 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 I&C systems as necessary for safe operation of the facility. These requirements should cover:

- the information necessary to establish the 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; and
- clearly defined operating configurations, including operational restrictions in the event of safety system outages.

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

Control rooms

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

5.33 Normal working environments to be considered include: lighting, temperature and humidity. Hazards to be considered include radiation, fire smoke or toxic substances in the atmosphere. The design of the main control room and supplementary control room should take into account environmental and/or seismic conditions expected during both normal and abnormal conditions.

Main control room

5.34 The principal location for 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 such a state after the onset of anticipated operational occurrences and design basis accidents. In addition, measures can be taken from the control room to mitigate the consequences of BDBAs.

5.35 The design should consider the layout of instrumentation and the mode of presenting information providing to operating personnel with an adequate overall picture of the status and performance of the facility. Ergonomic factors should be taken into account in the control room design.

5.36 The functional design of a control room should provide the operating personnel with accurate, complete and timely information on the status of facility equipment and systems for all operational states and design basis accident conditions, and to optimize the activities of the operator in monitoring and controlling the facility.

5.37 The information displayed should allow operators to:

- take specific manually-controlled actions for which no automatic control is provided and that are needed to respond to AOOs or accident conditions;
- confirm facility critical safety functions availability;
- 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 the release of radioactive materials and ~~to~~ continually assess such releases.

Supplementary control room

5.38 A remote reactor shutdown capability should be provided if the safety analysis identifies events that could inhibit the operators' ability to shutdown the reactor from the main control room. A supplementary control room or emergency control console should be provided if operators are required to perform any actions beyond reactor trip after operations from the main control room are inhibited.

5.39 Events that could inhibit the operator's ability to shutdown 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.

5.40 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.

5.41 Sufficient I&C equipment should be available, preferably at a single location that is physically and electrically separate from the main control room, so that the reactor can be placed and maintained in a 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.

5.42 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 AOOs 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 a beyond design basis accident (BDBA).

5.43 The design of supplementary control rooms should include suitable provisions for preventing unauthorized access and use.

Irradiation and experiment facility control systems

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

5.45 The operator of experimental facilities should have communication links with reactor operator to share information on reactor status and in special situations to require shut-down of the reactor. The reactor may be shut-down on the decision of reactor operator despite of running an experiment in order to mitigate any dangerous situation caused by running an experiment.

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

5.47 Important alarms of the facilities related to the reactor operation should be included in the reactor alarm system. Other alarms of experimental facilities should be presented with a functional separation from reactor's alarms.

5.48 Some actions in the facilities could affect the safety of the facility and they should be included in the safety system functions.

Voice communication system

5.49 Communications systems should be provided for staff to securely interface between the main control room, supplementary control room, other locations internally within the facility, the operators of experimental facilities, associated facilities, the emergency control system, and to external emergency organizations without having to leave the control room.

5.50 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 AOO or accident conditions;
- off-site emergency services; and
- associated facilities.

5.51 The diverse communications links should be routed such that they will not both be affected by common mode failures, fires, or PIE, and should be capable of operating independently of both the facility power systems and offsite power systems.

Provisions for fire detection and extinguishing

5.52 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.

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

5.54 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.

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

5.56 Fire detectors should be sited so that the flow of air due to ventilation or pressure differences necessitated 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.

5.57 If the environment does not allow detectors to be placed in the immediate 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 from the protected area for analysis by remote detectors with automatic operation.

5.58 When items such as fire pumps, water spray systems, ventilation equipment and fire dampers are controlled 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 in series. The design should allow the operation of the system to be stopped if the actuation is found to be spurious. There should be annunciation prior to the actuation of any automatic extinguishing system.

5.59 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.

POWER SUPPLIES OF I&C SYSTEMS

5.60 The power supply for I&C 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 I&C systems they serve.

5.61 I&C systems that are required to be available for use at all times in operational states or design basis accident conditions should be connected to uninterruptible AC power supplies (UPS) that provide the systems with power within the tolerances specified by the I&C design bases.

5.62 Modern I&C systems can be powered directly from DC power sources. This is advantageous for systems that need non-interruptible power because it eliminates the need for inverters, motor-generators, or power transfer devices in the electrical power system.

5.63 Power supplies can provide a transmission path for Electromagnetic Interference (EMI) which might originate outside the I&C systems or might arise from other I&C systems that are connected directly or indirectly to the same power supply. Such interference sources include electrical fault clearance associated with other equipment on the same supply. These interferences should be analysed and avoided in the extent possible.

6. OPERATION

OPERATIONAL LIMITS AND CONDITIONS

General

6.1 The Safety Standard [1] defines:

- "*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…*";

- "*The OLCs shall be used to provide the framework for the safe operation of the research reactor…*"

6.2 The design of the I&C systems of the reactor should assure that, during the operational states of the reactor, the I&C systems contribute to keep the set and values of the original selected OLCs.

Safety limits

6.3 The I&C systems should include those safety functions and safety related functions that prevent the exceeding of safety limits during the operational states of the reactor and accident conditions.

Safety System Settings

6.4 For each parameter for which a safety limit is required and for other important safety related parameters, there should be an I&C system that monitors the parameter and provides a signal that can be utilized in an automatic mode to prevent that parameter from exceeding the set limit. The required I&C systems to provide those functions should include the capability of storing of 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 I&C systems to assure a safe operation of the reactor.

CONTROL OF ACCESS TO SYSTEMS IMPORTANT TO SAFETY

6.1 All reasonable precautions shall be taken to prevent persons from deliberately carrying out unauthorized actions that could jeopardize safety.

6.2 I&C 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.

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

6.4 On the basis of the security policy that has been defined for the computer based system environment, appropriate security procedures - for instance password management - should be implemented (for example to guard against unauthorized access and viruses).

6.5 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.

6.6 Electronic access to software and data of computer based systems via external network connections should also be strictly avoided.

6.7 A hierarchical access method should be implemented in order to restrict authorised users only access to data and commands for which they are enabled.

6.8 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 hacking attacks.

MAINTENANCE, TESTING, SURVEILLANCE AND INSPECTION OF I&C SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY

6.9 Inspection, periodic testing, surveillance and maintenance of the I&C systems should be conducted to ensure that all their components are able to function in accordance with the design intent and with the requirements, in compliance with the OLCs and in accordance with the long term safety of the reactor.

6.10 The I&C systems should include, when reasonably applicable, on-line testing functions and capabilities to facilitate and reduce the time of periodic testing preserving the availability of the reactor.

PROVISIONS FOR REMOVAL FROM SERVICE FOR TESTING OR MAINTENANCE

6.11 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.

6.12 If use of equipment for testing or maintenance can impair an I&C function, the interfaces should be subject to hardware interlocking to ensure that interaction with the test or maintenance system is not possible without deliberate manual intervention.

6.13 The design should ensure that the system cannot unknowingly be left in a test or maintenance configuration.

6.14 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.

6.15 Where a safety system, or part of a safety system, has to be taken out of service for testing, adequate provisions should be made for the clear indication in the control room. For items that are frequently bypassed or frequently rendered inoperable, these indications should be automatic.

EXTENDED SHUTDOWN

6.16 A research reactor facility may have a period of extended shutdown pending decisions on its future.

6.17 The operating organisation should assess and define the minimal I&C systems that shall keep in operation mode during that extended shutdown.

7. HUMAN FACTORS ENGINEERING AND HUMAN-MACHINE INTERFACE

GENERAL CONSIDERATIONS

7.1 Human factors and Human-Machine Interfaces (HMI) should be given systematic consideration throughout the entire design process.

7.2 Effective HMI should be considered and applied for systems which should provide the operator with accurate, complete and timely information on the research reactor status and should enable proper operation of the I&C systems.

7.3 In the design of I&C systems the human factors should be taken into account. During the design of the HMI special attention should be paid to the duties and 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. Particular requirements of the operation organization should be taken into account from the early stages of the design.

7.4 All HMI should be designed according to ergonomic principles. The operational philosophy should determine which information is convenient to be displayed using conventional displays (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 management should be taken into account.

7.5 The requirements specification for HMI design should include 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.

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

7.7 Careful attention should be paid during the design of the HMI to ensure that all the necessary information is available to the operator when and wherever it necessary. At the same time, 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.

7.8 Operator interfaces to the reactor are primarily located in the main control room and supplementary control room where applicable for specified research reactor type. These facilities usually contain safety and safety related displays, safety and safety related controls, accident monitoring systems, alarm annunciators and historical data recording systems.

PRINCIPLES FOR HUMAN FACTORS ENGINEERING AND HMI DESIGN

7.9 The HMI design should retain useful features and avoid Human Factors Engineering (HFE) problems and issues experienced in previous designs.

7.10 I&C functions necessary to achieve facility safety objectives should be identified and allocated to human and system resources according to a defined methodology.

7.11 The HMI characteristics need to support tasks assigned to operators should be identified and documented according to a defined methodology. All aspects of the HMI (formats, terminology, sequencing, grouping, and operator's decision-support aids) should be designed in accordance with the task requirements.

7.12 The I&C system should provide operators with the information necessary to detect changes in system status, diagnose the situation, and verify manual or automatic actions.

7.13 The I&C system design should ensure that operator tasks can be performed within the time required.

7.14 The I&C system should be designed to detect operator errors, offer simple, comprehensible notification of the error, and simple, and effective methods for recovery.

7.15 Information displays should indicate the safety classification of the displayed variables.

7.16 Allocation of functions between manual and automatic actions should be made early in the design process.

7.17 Where a function is carried out automatically, the I&C 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.

7.18 The I&C system should alert the operator of the failure of an automatic control system.

7.19 The I&C system characteristics should be identified as necessary by a Task Analysis.

7.20 The relationship of each display, control, and data-processing aid to the associated tasks and functions should be clear.

7.21 The HMI should provide an effective overview of the facility status.

7.22 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.

7.23 The operation and appearance of the HMI should be consistent across information and control locations, reflect a high degree of standardization, and be fully consistent with procedures and training.

7.24 The HMI 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.

7.25 The I&C systems should provide sufficient instrumentation for monitoring its operation and process systems in normal operation and for recording all variables important to safety.

7.26 The I&C systems should provide sufficient indicators and recording instrumentation to monitor important reactor parameters during and following anticipated operational occurrences and DBAs. This instrumentation should be adequate for the purposes of emergency response (BDBAs).

7.27 Audio and visual alarm systems should be provided for the early indication of changes in the operating conditions of the reactor that could affect its safety.

Control Rooms

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

7.29 In control room design HFE 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 following design basis accident conditions.

8. COMPUTER BASED SYSTEMS AND SOFTWARE

GENERAL CONSIDERATIONS

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

8.2 The current technology allows developing computer based instrumentation and control systems for systems important to safety that has the potential for improving the level of safety and reliability with sufficient reliability. The reliability could be predicted and demonstrated with a systematic, fully documented and reviewed engineering process. This process should include the evaluation of operating experience with pre-existing software.

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

8.4 Organizational, regulatory and licensing aspects should be carefully taken into consideration at a very early stage of the project in order to ensure its success.

8.5 Depending on the complexity of experimental facilities in the research reactor, it should be considered to functionally split the development of Computer Based System in reactor system and experimental facilities system. In that way, both systems could be treated with its own set of requirements and objectives.

COMPUTER BASED SYSTEMS AND SOFTWARE DESIGN CONSIDERATIONS

8.6 In safety systems implementation it should be considered that all unnecessary complexity has been avoided both in the functionality of the system and in its implementation, and showing evidence of compliance to 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 separated 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 the problems of 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 for the system and its associated software should be used to facilitate the assessment of design objectives. The computer system should meet the criteria for the highest safety class of the functions it is implementing.

8.10 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 errors, 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.

8.11 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 a demonstrable global increase in safety.

8.12 It should be demonstrated that measures have been taken to protect the computer based system throughout its entire lifetime against physical attack, intentional and non-intentional intrusion, fraud, viruses and so on. Safety systems should not be connected to external networks.

8.13 The computer based system should be designed for maintainability to facilitate the detection, location and diagnosis of failures so that the system can be repaired or replaced efficiently. Software that has a modular structure will be easier to repair and will also be easier to review and analyse, since the design can be easier to understand and easier to modify without introducing new errors. Software maintainability also includes the concept of making changes to the functionality. The design of a computer based system should ensure that changes are confined to a small part of the software

8.14 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.

8.15 Computer systems that perform safety functions should have deterministic (real-time) behaviour with regard to functions and timing.

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

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

8.18 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.

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

8.20 Appropriate consideration should be given to the use of redundancy in the data communication.

8.21 The data communication network topology and network interface should be designed and implemented to avoid CCF of independent systems or subsystems.

8.22 Data flow from lower to higher classified safety systems should be prevented.

8.23 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.

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

8.25 Software tools could be used to support all aspects of the I&C life cycle where benefits result through their use and where 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.

8.26 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.

PROJECT PLANNING

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

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

8.29 All phases of the development process should be identified. Each phase consists of specification, design and implementation and the design activity of one phase sets the requirements for the next phase. Verification should be performed across each phase of the development and before starting the next phase

8.30 The methods to be used in the development should be identified as well. This selection should be related to the quality assurance programme description, in which standards and procedures are established.

8.31 A quality assurance programme should be prepared and implemented and should be available for regulatory review before the project begins. A software quality assurance plan should be produced at the start of the project.

Verification and validation plan

8.32 Verification and Validation (V&V) 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.

8.33 V&V management planning should include the listing and collection of applicable standards, procedures and conventions that guide the verification process.

8.34 It is recommended that the teams performing verification and validation will be independent of the development team. Independence is usually ensured by having different line management for the V&V and development teams

8.35 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 the change control process.

Configuration management plan

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

8.37 A procedure for change control should be defined. The change control procedure should maintain records of the problems that were identified during the development process, 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 solve the problems.

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

Installation and commissioning plan

8.39 The installation and commissioning plan should cover the following:

- The sequence of steps for proper integration of the system into the facility and the corresponding facility states needed for safe introduction of the new or changed system.
- The required interactions with the regulatory body, including any 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.
- A description of the records and reports that will be generated to describe the results of commissioning.

COMPUTER BASED SYSTEM REQUIREMENTS

8.40 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.

8.41 Safety analyses, for example accident analyses, transient analyses or facility safety analyses (based on postulated initiating events and safety criteria), should be an

essential part of this design. 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 availability.

8.42 An accurate and clear description of these requirements should be written before starting the next stage of the project. This description should be understandable to regulatory body and experts involved.

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

8.44 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 should be derived from the security policy that has been defined for the computer based system environment and should take into account the security procedures that should be implemented.
- Whether and where physical separation is needed (for example between safety and control functions).

Software requirements

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

Software design

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

8.47 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.

8.48 The design should contain no contradictions and no ambiguities. The description of the interfaces between modules should be complete.

8.49 The design and its description should be such that it is possible to demonstrate that each software requirement has been met and to verify that the implementation is correct with respect to the detailed design.

8.50 The documentation on software design should provide technical information on the overall architecture of the software and on the detailed design of all software modules. Relevant implementation constraints should also be specified.

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

8.52 Diagrams and flow charts could be used 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 graphical methods.

Software implementation

8.53 The production of software code should be verifiable against the software specifications. If verification is made by human inspection, the code should be readable, adequately commented and understandable. Validated software tools could be used to facilitate the code verification process.

8.54 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.

8.55 The code of each programme of a module should be kept simple and easy to understand, both in its general structure and in its details.

8.56 Data structures and their naming conventions should be used uniformly throughout the whole system.

VERIFICATION AND ANALYSIS

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

8.58 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.

8.59 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 to record the results of their reviews should be stated in the verification plan together with a justification of the chosen method.

8.60 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.

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

8.62 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.

COMPUTER SYSTEM INTEGRATION

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

8.64 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.

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

8.66 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

8.67 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 (FAT) to form a single test activity.

8.68 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 (including out-of-range 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.
- All modes of operation of the computer system, including transition between modes and recovery after power supply failure.

8.69 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

8.70 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.

8.71 The validation and commissioning tests should be usually combined with the Site Acceptance Test (SAT), which includes verification of the operation and maintenance of the equipment.

8.72 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.

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

OPERATION, MAINTENANCE AND MODIFICATION

8.74 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.
- Perform regression testing due to modifications, implemented to enhance or change the functionality or to correct errors.
- Change of parameters.
- Diagnosis activities, e.g. the execution of special diagnostic programs.
- Hardware components replacement due to random failures.

8.75 The life cycle of the systems should include the processes for implementing of modifications. This life cycle should contain the phases of the main development, including V&V. 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.

8.76 After failure of a hardware component, corrective actions should be limited to one-for-one replacements of hardware and to the reloading of the existing software modules. These actions should not include any modification.

Computer security

8.77 IAEA Nuclear Security Series No. 17, Ref. [9], provides guidance on concerns, requirements, and strategies for implementing computer security programs at nuclear facilities.

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

8.79 The failure modes of computer security features and the effects of these failure modes I&C functions should be known, documented, and considered in system hazard analyses.

8.80 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.

8.81 Where practical, security measures that do not also provide a safety benefit, should be implemented in devices that are separate from I&C systems.

9. CONFIGURATION MANAGEMENT

9.1 A full set of documentation reflecting the configuration and status of I&C systems in the facility should be available prior to the commissioning of the facility.

9.2 A baseline database of systems/components of the I&C systems should include the following information:

- general information (e.g. system ID, 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 with the improvement and the updating of I&C configuration control documentation.

9.4 A process of verification and update of the existing documentation should be undertaken prior to commencing any modernization activities.

10. MODIFICATION AND MODERNIZATION OF I&C SYSTEMS

10.1 Upgrade and modification of I&C systems should be performed in accordance with the guidance of [4], Ref. [4] provides guidance on planning, organizational aspects, safety assessment, implementation and post implementation, training, and documentation of facility modifications.

10.2 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 I&C systems are discussed in chapter 4.

10.3 Modification to I&C 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).

10.4 When the decision is made to follow through with a modification to existing I&C equipment, careful consideration of the possible effects on reactor safety should be considered and assessed.

10.5 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 competition of modifications of I&C systems.

10.6 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 I&C 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.

10.7 A baseline database of systems/components of the existing I&C systems should be updated or created following the recommendations at 9.2.

10.8 Verification and update of existing documentation should start at a high-level functional description of the I&C system architecture, preferably in the form of a diagrammatic representation with an accompanying list of all I&C systems. If such a representation exists, it should be verified for accuracy.

10.9 There should be a designated Design Authority that will be responsible for the design, integration, documentation and maintenance of the facility as well as training facility personnel in the use of the new equipment. Refer to [5] for details on the responsibilities that the Design Authority should assume.

10.10 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.

10.11 The affect the modification will have on how the facility personnel interact with the system should be considered. Particular requirements of the end-user should be taken into account from the early stages of the project. (Refer to section 7 for details on Human Factors considerations).

10.12 The reliability of the new or modified equipment should be considered as well as the effect the modification will have on overall system reliability. The performance of a qualitative analysis (e.g. Failure Modes, Effects and Criticality Analysis (FMECA)) 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.

10.13 When modifying an existing safety system, the effect on the current defence-in-depth implementation should be considered. (Refer to chapter 4 and [1]).

10.14 When modifying any I&C system, consideration on Design Guidelines should be considered. (Refer to chapter 4).

10.15 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.

10.16 Safety Systems are required to be independent of other reactor systems. The designated Design Authority/safety review committee should determine the need for, as well as the effect on, independence during the initial design phase of the modification.

10.17 The effect on system Environmental Qualification (EQ) should be considered. EQ should be based in recommendation of Equipment Qualification. (Refer to chapter 4, EQUIPMENT QUALIFICATION).

10.18 When an I&C 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.

10.19 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 I&C upgrades and modification should consider:

- the limitations due to the physical characteristics of the installed facility, which effectively restrict the design options for I&C systems;
- the possible need to maintain consistency between the design of replacement equipment and existing I&C equipment to, for example, reduce the complexity of the overall operator interface and maintenance tasks of the 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 personal for some time after the change.

10.22 When an I&C system is replaced the new I&C system should, 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.

10.23 The consequences of a 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).

10.24 Installation of the equipment should be performed by qualified personnel under the supervision of the Design Authority or other qualified Authority.

10.25 Once complete, and before start-up of the reactor, the installation should be functionally tested following the recommendations of Ref. [4].

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, The Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series, IAEA, Vienna (approved for publication). [(DS 351)]

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Research Reactors and Preparation and Content of the Safety Analysis Report, IAEA Safety Standards Series, IAEA, Vienna (approved for publication). [(DS 396)].

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

[5] 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, IAEA, Vienna (2010).

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

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

[11] 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).

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

ANNEX I

GENERAL

1.1. The I&C Systems of a Research Reactor involve many systems that can be identified in a particular 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 the 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 application.

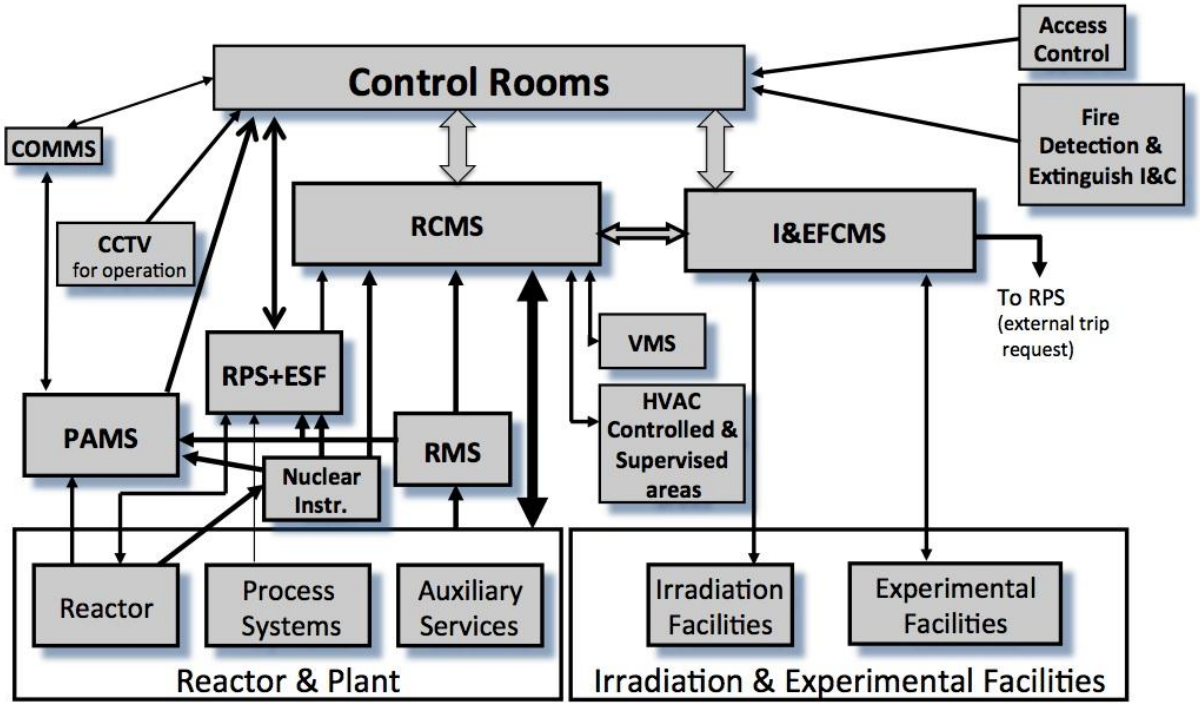

Fig AI.1 Research Reactor I&C systems – Block Diagram

Acronyms and abbreviations:

CCTV: Close Circuit Television;

COMMS: Communication System;

ESF: other Engineering Safety Features initiation I&C;

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

I&EFCMS: Irradiation & Experimental Facilities Control and Monitoring System;

Instr.: Instrumentation;

PAMS: Post 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 allowable values and automatically initiate actions 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 Facilities 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.

Post-Accident Monitoring System (PAMS)

1.5. Post-accident monitoring instrumentation 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 post-accident operating 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 if of the highest relevance to assure a safe operation of the reactor. Also bring 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 root 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 following-up of the 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 in the Main Console of the reactor (the main human machine interface).

Radiation Monitoring System (RMS)

1.9. 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.

Humidity Ventilation and Air Conditioning (HVAC)

1.10. Heating, ventilation and air conditioning systems are used for assuring and maintaining consistent operable environments 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 major source of CMFs in I&C equipment.

Vibration Monitoring System (VMS)

1.11. Vibration monitoring system provides a means of monitoring and detecting abnormal vibration conditions on reactor main rotary equipment.

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;
- bring the reactor to a safe shutdown; and
- implement Emergency Operating Procedures (EOPs).

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 isotope production facilities are 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 Facilities Control and Monitoring System (I&EFCMS)

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

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 experimental and associated facilities, 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 operator and security staff to monitor and supervise relevant controlled or supervised area tasks and other outer approaches (i.e. control room entrance, reactor hall and restricted areas where radioactive sources are stored).

Fire detection and extinguish I&C

1.19. This independent system has the capability to identify the presence of fire in the facility and, upon this event, initiate an automatic fire extinguish 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. 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 should be located in the control rooms to provide the reactor operators with relevant information.

CONTRIBUTORS TO DRAFTING AND REVIEW

Abou Yehia H.	IAEA	
Boeck H.	University of Technology/Atominstitute Reactor	Austria
Boogaard J.	IAEA	
Busto A.	IAEA	
Diakov O.	IAEA	
Drexler J.	INVAP	Argentina
Hargitai T.	IAEA	
Johnson G.	IAEA	
Kim Hyung K.	Korea Atomic Energy Research Institute	Korea, Republic of
Lokantsev A.	SNIIP	Russian Federation
Muhlheim Michael D.	Nuclear Science and Technology Division Oak Ridge National Laboratory	Unites States of America
Rodriguez L.	AREVA	France
Shirley A.	Thermo Fisher Scientific	Unites States of America
Shokr A.M.A.	IAEA	
Waard J.	Nuclear Research and Consultancy Group (NRG)	Netherlands
Winfield D.	IAEA	