GUIDE NO. AERB/NPP-PHWR/SG/D-25

GUIDE NO. AERB/NPP-PHWR/SG/D-25

GOVERNMENT OF INDIA

AERB SAFETY GUIDE

COMPUTER BASED SYSTEMS
OF
PRESSURISED HEAVY WATER REACTORS

ATOMIC ENERGY REGULATORY BOARD

AERB SAFETY GUIDE NO. AERB/NPP-PHWR/SG/D-25

COMPUTER BASED SYSTEMS OF PRESSURISED HEAVY WATER REACTORS

Atomic Energy Regulatory Board
Mumbai-400 094
India

January 2010

Price

Order for this guide should be addressed to:

The Administrative Officer
Atomic Energy Regulatory Board
Niyamak Bhavan
Anushaktinagar
Mumbai-400 094
India

FOREWORD

Activities concerning establishment and utilisation of nuclear facilities and use of radioactive sources are to be carried out in India in accordance with the provisions of the Atomic Energy Act 1962. In pursuance of the objective of ensuring safety of members of the public and occupational workers as well as protection of the environment, the Atomic Energy Regulatory Board (AERB) has been entrusted with the responsibility of laying down safety standards and enforcing rules and regulations for such activities. The Board, therefore, has undertaken a programme of developing safety standards, codes and related guides and manuals for the purpose. While some of the documents cover aspects such as siting, design, construction, operation, quality assurance and decommissioning of nuclear and radiation facilities, other documents cover regulatory aspects of these facilities.

Safety codes and standards are formulated on the basis of nationally and internationally accepted safety criteria for design, construction and operation of specific equipment, structures, systems and components of nuclear and radiation facilities. Safety codes establish the objectives and set requirements that shall be fulfilled to provide adequate assurance for safety. Safety guides elaborate various requirements and furnish approaches for their implementation. Safety manuals deal with specific topics and contain detailed scientific, technical information on the subject. These documents are prepared by experts in the relevant fields and are extensively reviewed by advisory committees of the Board before they are published. The documents are revised when necessary, in the light of experience and feedback from users as well as new developments in the field.

The safety code on 'Design of Pressurised Heavy Water Reactor Based Nuclear Power Plants' [AERB/NPP-PHWR/SC/D (Rev. 1), 2009] spells out the requirements to be met during design for assuring safety. This safety guide is one of a series of guides, which have been issued or are under preparation, to describe and elaborate the specific parts of the code. This guide describes approach to design and review of computer-based systems when they are to be deployed for performing functions important to safety in the nuclear power plant. The elements presented herein are set of goals and good practices that form the basis of acceptance of the computer-based systems. In drafting this guide, current international practices as described in IAEA NUSS series and IEC standards have been utilised.

Consistent with the accepted practice, 'shall' and, 'should' are used in the guide to distinguish between a firm requirement and a desirable option, respectively. Appendices are an integral part of the document, whereas annexures, footnotes, references/ bibliography and lists of participants are included to provide information that might be helpful to the user. Approaches for implementation different to those set out in the guide may be acceptable, if they provide comparable assurance against undue risk to the health and safety of the occupational workers and the general public and protection of the environment.

This safety guide applies only for nuclear power plants built after the issue of the document. However during periodic safety review, a review for applicability of the current guide for existing power plants would be performed.

For aspects not covered in this guide, applicable national and international standards, codes and guides acceptable to AERB should be followed. Non-radiological aspects such as industrial safety and environmental protection are not explicitly considered in this guide. Industrial safety shall be ensured by compliance with the applicable provisions of the Factories Act, 1948 and the Atomic Energy (Factories) Rules, 1996.

The guide has been prepared by specialists in the field drawn from the Atomic Energy Regulatory Board, Bhabha Atomic Research Centre, Indira Gandhi Centre for Atomic Research, Nuclear Power Corporation of India Limited and other consultants. It has been reviewed by the relevant AERB Advisory Committee on codes and guides and Advisory Committee on nuclear safety.

AERB wishes to thank all individuals and organisations who have prepared and reviewed the draft and helped in its finalisation. The list of experts who have participated in this task, along with their affiliations, is included for information.

(S. K. Sharma)
Chairman, AERB

DEFINITIONS

Audit

A documented activity performed to determine by investigation, examination and evaluation of objective evidence, the adequacy of, and adherence to applicable codes, standards, specifications, established procedures, instructions, administrative or operational programmes and other applicable documents, and the effectiveness of their implementation.

Common Cause Failure

The failure of a number of devices or components to perform their functions, as a result of a single specific event or cause.

Diversity

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

Fail Safe Design

A concept in which, if a system or a component fails, then plant/component/system will pass into a safe state without the requirement to initiate any operator action.

Quality Assurance (QA)

Planned and systematic actions necessary to provide adequate confidence that an item or service will satisfy given requirements for quality.

Reliability

The probability that a structure, system, component or facility will perform its intended (specified) function satisfactorily for a specified period under specified conditions.

Responsible Organisation

An organisation having overall responsibility for siting, design, construction, commissioning, operation and decommissioning of a facility.

SPECIAL DEFINITIONS
(Specific for the Present Guide)

Configuration Item (CI)

Items treated as a unit for the purpose of configuration management, e.g. hardware, software, documents, tools.

Configuration Management (CM)

The process of identifying and defining the configuration items in a computer-based system, controlling the release and change of these items through out the system life cycle, recording and reporting the status of configuration items (CIs) and change requests, and verifying the completeness and correctness of configuration items (CIs)

Formal Verification

Process of verification of software or its part based on rigorous/mathematical techniques capable of providing proof that the software or its part satisfies a given property.

Integrity

Quality of completeness, dependability and freedom from defect

System Safety Analysis

Analysis, of design of computer based systems, consisting of confirmation of safety function implementation, failure analysis, CCF analysis.

Safety Case

Documented demonstration of the system safety and integrity of computer-based system as evidence for fulfillment of requirement of regulatory body.

Software Quality

The composite characteristics of software that determine the degree to which the software in use will meet the expectations of the user

Traceability

The degree to which a relationship can be established between two products of the development process, especially products having a predecessor-successor relationship to one another.

Validation

Test and evaluation of the integrated computer based system to ensure compliance with the system requirements.

Verification

The act of reviewing, inspecting, testing, checking, auditing, or otherwise determining and documenting whether items, processes, services or documents conform to specified requirements.

ACRONYMS

ASIC	-	Application Specific Integrated Circuit
CCF	-	Common Cause Failure
CMP	-	Configuration Management Plan
CMP-OM	-	Configuration Management Plan during O and M
CPLD	-	Complex Programmable Logical Devices
FPGA	-	Field Programmable Gate Arrays
IA	-	I and C Safety Class A
IB	-	I and C Safety Class B
IC	-	I and C Safety Class C
IV and V	-	Independent Verification and Validation
MTTR	-	Mean Time To Repair
PDS	-	Pre-developed System
PIE	-	Postulated Initiating Event
PLC	-	Programmable Logic Controller
PSAR	-	Preliminary Safety Analysis Report
QAP	-	Quality Assurance Plan
SAR	-	Safety Analysis Report
SCADA	-	Supervisory Control and Data Acquisition
SRRP	-	Standard Regulatory Review Process
V and V	-	Verification and Validation

CONTENTS

1. INTRODUCTION

1.1 General

Each instrumentation and control (I and C) system, performing protection, control or related tasks in a nuclear power plant, spans all elements from plant sensors to control actuators and includes provisions, which facilitate operation, in-service testing and maintenance tasks.

When I and C systems perform functions important to safety, these systems must be demonstrated to be safe and reliable with appropriate degree of confidence. I and C systems are classified, based on safety considerations, into three classes IA, IB and IC in AERB safety guide AERB/NPP-PHWR/SG/D-1 [1].

The basic requirements for the design of safety systems for nuclear power plants are provided in AERB/NPP-PHWR/SC/D, 2009 [6]. These requirements were interpreted and extended for design of protection systems (I and C class IA) in AERB safety guide AERB/NPP-PHWR/SG/D-10 [3] and for design of safety related I and C systems (class IB and IC) in AERB safety guide AERB/NPP-PHWR/SG/D-20 [4].

The practice of design and implementation of computer based systems has matured over last several years and with current state of technology, it is possible to develop computer based systems for carrying out functions important to safety in nuclear power plants and also to demonstrate their fitness-for-purpose. In nuclear power plants, both new and old, computer based instrumentation and control (I and C) systems are being used increasingly both in safety related applications, such as some functions of the process control and monitoring systems, as well as in safety critical applications, such as reactor protection or actuation of engineered safety systems.

The dependability of computer based systems important to safety is therefore of prime interest and should be ensured. However, as explained below, computer based systems have some characteristics that make them different from other electronic control (hardwired) systems and hence necessitate a different approach to demonstrate their safety and reliability.

Computer based systems are programmable and provide a number of advantages over non-programmable systems. However the features that give advantages also add complexity to software. Unlike in hardwired-based systems, faults in software, which does not wear-out, always result from improper requirements, design or implementation. Also, software implementations are discrete models of the real world and are less tolerant to “small” errors and are more difficult to test.

It is recognised that currently the computer based systems are not amenable to quantitative assessment of reliability, primarily due to software component of these systems. Therefore assessment of software in the computer based systems has to be based on evidence that the software is correct (with respect to specifications), safe and completely implements the requirements. In other words, the software in these systems must be demonstrated to be safe and to have high level of integrity.

In line with the current practice, demonstration of integrity and safety, has been emphasised in this guide as a necessary requirement and is considered as valid basis of acceptance of computer based systems. Integrity should be assured by developing system/software using systematic, technically appropriate, carefully controlled, fully documented and reviewable engineering process, which is suitably interfaced with V and V activities.

The safety case i.e. the arguments and evidence in support of system and, in particular, the software safety and integrity shall be based on designs created and based on design documents produced during the system development and the results of analysis of specifications, algorithms, designs and implementation. The reviews of designs/analysis are required to be performed by people other than those who designed and implemented the system/software (designers). Therefore precise, detailed and understandable documentation is required to be produced.

1.2 Objectives

The objective of this safety guide is to provide guidance on regulatory requirements of computer based systems to plant system designers, computer based system designers, configuration managers, V and V and quality assurance personnel, regulators, and plant O and M personnel.

This safety guide does not recommend any specific method, tool, computer languages etc.

1.3 Scope

The guidance for the overall design of I and C systems performing functions important to safety are covered in separate AERB safety guides AERB/NPP-PHWR/SG/D-10 [3] and AERB/NPP-PHWR/SG/D-20 [4]. The guidance contained in this guide specifically deals with that part of an I and C system which are realised (implemented) by means of a computer based system and are therefore applicable in such cases in addition to those contained in the safety guides AERB/NPP-PHWR/SG/D-10 and AERB/NPP-PHWR/SG/D-20. The recommendations in this guide relate to:

(i) Design and development of computer based systems

(ii) Quality assurance, verification and validation and system safety analysis

(iii) Management and control of changes to system during design and O and M phases

(iv) Regulatory requirements for computer based systems

(v) Regulatory review process.

The guidance for environmental and seismic design of computer based systems are same as those covered in AERB safety guides AERB/NPP-PHWR/SG/D-1 [1], AERB/NPP-PHWR/SG/D-20 [4], AERB/SG/D-3 [2], and AERB/NPP-PHWR/SG/D-23 [5].

This safety guide also applies to pre-developed software or system software (such as an operating system), software specifically developed for the system, or system developed using existing pre-developed equipment family of hardware or software modules. The issue of the use of pre-developed or commercial off-the-shelf system components for safety critical functions has been addressed in detail in this guide and recommendations have been provided for the same.

1.4 Structure

Section 2 describes computer based systems, associated safety issues, review issues, recommended life cycle, and the standard regulatory review process. Fig. 1 shows the recommended system development methodology. Fig. 2 shows V and V methodology as part of the standard review process.

Section 3 defines safety case and its contents, regulatory requirements for computer based I and C systems, general requirements for design and development of computer based systems; additional requirements for classes IA and IB system safety and reliability requirements.

Section 4 provides the regulatory review process for newly developed systems, pre-developed systems and generic design certification.

Appendix-1 provides detailed guidance on the system development planning process, configuration management during development and O and M, and system security planning.

Appendix-2 provides detailed guidance on quality assurance as well as verification and validation planning.

Appendix-3 provides detailed guidance on the generation of system requirements.

Appendix-4 provides detailed guidance on the system architectural design including generation of hardware requirement specifications and software requirement specifications.

Appendix-5 provides detailed guidance on the hardware design, development and testing.

Appendix-6 provides detailed guidance on the software design, implementation and testing.

Appendix-7 provides detailed guidance on the system integration and testing during development.

Appendix-8 provides detailed guidance on the system safety and reliability analysis.

2. LIFE CYCLE AND OVERVIEW OF REGULATORY REVIEW

2.1 Safety Issues with Computer based I and C Systems

Nuclear power plants use computer systems with widely varying size and capabilities of computer, for example, from tiny intelligent relays and single loop controllers to distributed systems, consisting of large number of nodes. Several programmable components like FPGAs and CPLDs are also used and these have resident programmes. Such programmes need to be reviewed in accordance with the safety classification of their functions.

It is important to arrive at applicable safety classification of every computer based I and C system performing functions important to safety. This is also to be used to allocate appropriate resources as well as efforts to ensure overall computer based system safety and integrity. The computer based systems form a part of the overall I and C for any defined function and belongs to safety class applicable to that function. The scheme of safety classification of systems is described in AERB safety guide AERB/NPP-PHWR/SG/D-1 [1] and for the sake of completeness; the three safety classes are described below briefly.

Class IA computer based systems: Class IA applies to those computer based systems, which play a principal role in achievement or maintenance of nuclear power plant safety. These systems prevent postulated initiating events (PIEs) from leading to a significant sequence of events, or mitigate the consequences of a PIE. This class also applies to those computer based systems, whose failure could directly cause a significant sequence of events.

Class IB computer based systems: Class IB applies to computer based systems that play a complementary role to the class IA systems in the achievement or maintenance of nuclear power plant safety. The operation of class IB computer based systems may avoid the need to initiate class IA systems. Class IB computer based systems may improve or complement the execution of class IA systems in mitigating the effects of a PIE. Class IB also applies to computer based system whose failure could initiate or worsen the severity of a PIE.

Class IC computer based system: Class IC applies to computer based systems that play auxiliary or indirect role in the achievement or maintenance of nuclear power plant safety. Class IC includes those computer based systems that have some safety significance but do not belong to class IA or IB. They can be part of total response to an incident but not be directly involved in mitigating the physical consequences of the incident.

This classification determines both approach to development and also reviews as detailed in sections 3 and 4.

In case of a distributed implementation of a computer based system, it may comprise of several sub-systems each of which may be further sub-divided in a similar manner. Each of the “sub-systems and components” of the distributed system shall be assigned one of the safety classes referred above based on the contribution of that node to the overall safety. Since an individual sub-system may be involved in implementation of several aspects of the requirements specification, the classification process may result in some sub-systems being assigned multiple classes, in which case the safety class of the sub-system shall be the highest assigned class.

2.2 Review Issues with Computer based I and C Systems

Computer based systems are reviewed so as to ensure the correctness of implementation and safety of operation. The process of review is determined by the development life cycle of the computer based system.

Computer based systems intended for use in applications important to safety are often designed for specific applications in NPPs. The hardware and software are built from scratch and it is possible to develop these as per recommendations of this guide. AERB will carry out the regulatory review of these computer based I and C systems as per standard regulatory review process (SRRP). However, in many situations, it is practical to obtain and embed pre-developed hardware and/or software components in such systems. Such embedded pre-developed hardware and/or software components may or may not have been certified earlier and, may or may not have been used in applications of similar safety significance in NPPs. The SRRP includes assessment procedures for such pre-developed components, that may have been used in implementation of computer based I and C system.

There may be systems which are pre-developed i.e. these have been reviewed by some regulatory authority and have been used in nuclear power plants in applications of similar safety significance. In such cases the life cycle used should be mapped to the recommended life cycle described in subsection 2.3. The regulatory review process for such pre-developed systems as given in subsection 4.2 takes care of this requirement.

2.3 Recommended Development Life Cycle of Computer based Systems

The development life cycle of computer based I and C systems consists of the entire stretch from defining the requirements through development to the installation and commissioning of the system as shown in Fig. 1. The recommended life cycle also permits use of pre-developed components as illustrated in Fig. 1. The use of pre-developed component is preceded by evaluation of its functional suitability and fulfillment of regulatory requirements.

The entry to the life cycle is made with the generation of system requirements (SR), which should provide the detailed requirements of the system from all relevant viewpoints. The SR (Appendix-3) should describe the complete requirements of the system at a ‘black box’ level including the role of the system, various modes of its operation and functional and performance requirements in each mode, its external interfaces, environmental constraints etc.

The development of a computer based system should be planned carefully at the beginning of the project to ensure its timely completion simultaneously meeting its objectives. During this planning process all plans viz. system development, configuration management, security, QA, verification and validation should be finalised taking into account recommendations of this guide (Appendix-1 and Appendix-2). The project management planning should ensure risk-free, timely, and orderly conduct of the development life cycle. The QA process should ensure that the products (including the documents produced at various stages) comply with the quality standards set out at the beginning of the project and all tasks are carried out as per plan. The objectives of the verification and validation activities should be to ensure consistency and correctness of the products of the development process. The configuration management process should ensure that the system configuration (consisting of various hardware and software items and documents) is kept consistent at all times during system development. System validation document should provide details of the test plan and procedures to be carried out to check conformance of the complete system to the requirements.

The actual development should be commenced, subsequent to completion of the planning phase. During this phase, the system architecture is developed and the system is progressively decomposed, as per needs, into various functionally independent sub-systems and components. The system integration and test procedures should be developed alongside. The architectural design has to be carried out to meet the requirements imposed by the safety classification of the complete system as well as of each of its constituents. The system architecture design document (Appendix-4) should describe the architecture of the system, role of each subsystem, if applicable, and also define the functions, which will be carried out in hardware (hardware requirement specifications) as well as the functions, which will be carried out in software (software requirement specifications).

The detailed development process for the hardware (Appendix-5) of each constituent sub-system should lead to generation of the hardware design, and hardware integration and test procedure for each sub-system. Reliability analysis of the hardware should be carried out to ensure conformance with the applicable requirements.

The detailed development process for the software (Appendix-6) of each constituent sub-system should lead to generation of the software design for each sub-system. A programming guideline document defining applicable design practices for software programs to meet the requirements of the applicable safety classification should be generated. The software should be developed using programming guidelines and subjected to unit and integration testing.

Consequent upon completion of the hardware and software development (and testing) process, the composite system should be integrated and tested (Appendix-7) and this should result in generation of a system integration and test report. The system is then ready for independent validation.

In parallel to the development when requisite inputs are available, system safety analysis, failure analysis and hardware reliability analysis should be carried out (Appendix-8). For all class IA systems, a common cause failure (CCF) analysis should be carried out (Appendix-8).

Any modifications in the system design on account of operational needs, or, operational incidents including detection of deviant behaviour of the system should require appropriate authorisation, and the implementation should entail a re-entry into the development life-cycle and should be governed by CMP for operation phase (CMP-OM). CMP-OM should identify the change authorisation agency and change implementation agency (Appendix-2).

2.4 Overview of Standard Regulatory Review Process (SRRP)

The SRRP is based on the recommended life cycle shown in Fig. 1 and the typical verifications and validation tasks shown in Fig. 2.

The designer is required to carry out verification and validation as indicated in Fig 2. Guidance for V and V is given in Appendix-2. The thoroughness of the verification plan shall be commensurate with the safety class of the system. Every verification step shall produce a report of the analysis performed, compliance of the outputs of the phase with the inputs requirements, resolution of anomalies and the conclusions reached.

The verification of the system integration reports with respect to the system integration plan should be carried out before the validation activity. Following integration of the system, the overall functional and performance requirements of the system shall be validated in all specified modes of plant operation.

The results of validation testing and analysis shall be documented and reviewed against the requirements expressed in the system validation plan to confirm that the functional performance of the system meets those requirements.

Designer shall carry out analyses of system safety and reliability analysis as per Appendix-8.

The SRRP is designed to confirm that the delivered system satisfies all aspects of its requirements and the safety analysis demonstrates safe behaviour of the system under all operational states. The SRRP consists of reviews and audits, which are briefly described below.

The review process mainly consists of the following:

(i) Review of plans

(ii) Review of system requirements & design outputs, validation

(iii) Review of system safety and reliability analysis

(iv) Audit of V and V reports and QA reports.

2.5 Generic Design Certification Review

Details of products (hardware, software or components involving both), planned for use in computer based systems of NPPs, may be submitted, in advance, to AERB for generic design certification. Such products are not complete I and C systems, but may be used in design of I and C systems. Various software development tools also can be assessed under generic design certification. The process of generic certification is described in subsection 4.3.

Generic design certification is valid for the version of design assessed and any changes will lead to fresh reviews. Also, additional reviews would be required to ensure that computer based I and C systems using design certified components, have employed them in correct and safe manner.

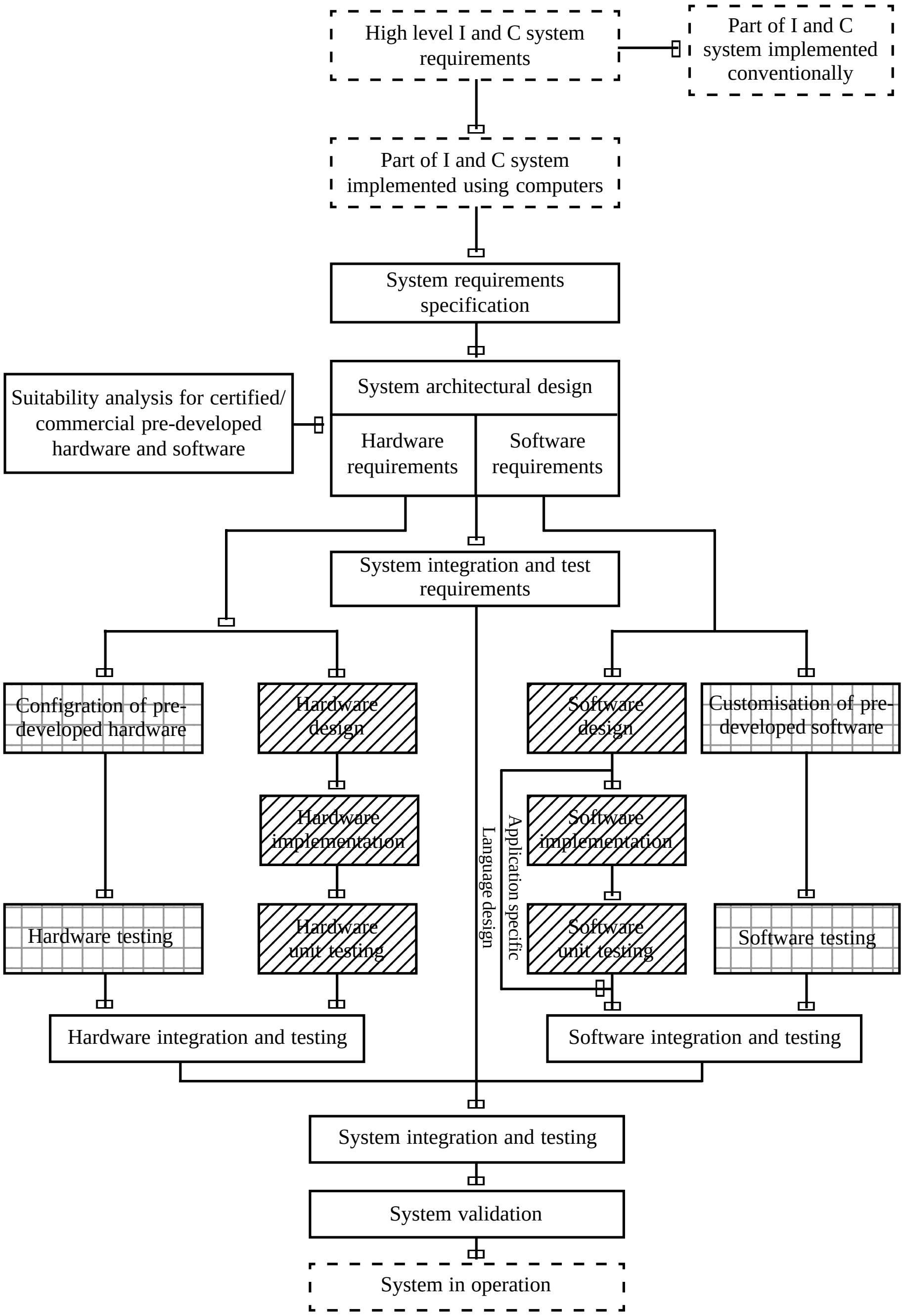
High level I and C system requirements
Part of I and C system implemented conventionally
Part of I and C system implemented using computers
System requirements specification
System architectural design
Suitability analysis for certified/ commercial pre-developed hardware and software
Hardware requirements
Software requirements
System integration and test requirements
Configration of pre-developed hardware
Hardware design
Software design
Customisation of pre-developed software
Hardware implementation
Software implementation
Language design
Application specific
Hardware testing
Hardware unit testing
Software unit testing
Software testing
Hardware integration and testing
Software integration and testing
System integration and testing
System validation
System in operation

FIG. 1 : SYSTEM DEVELOPMENT METHODOLOGY

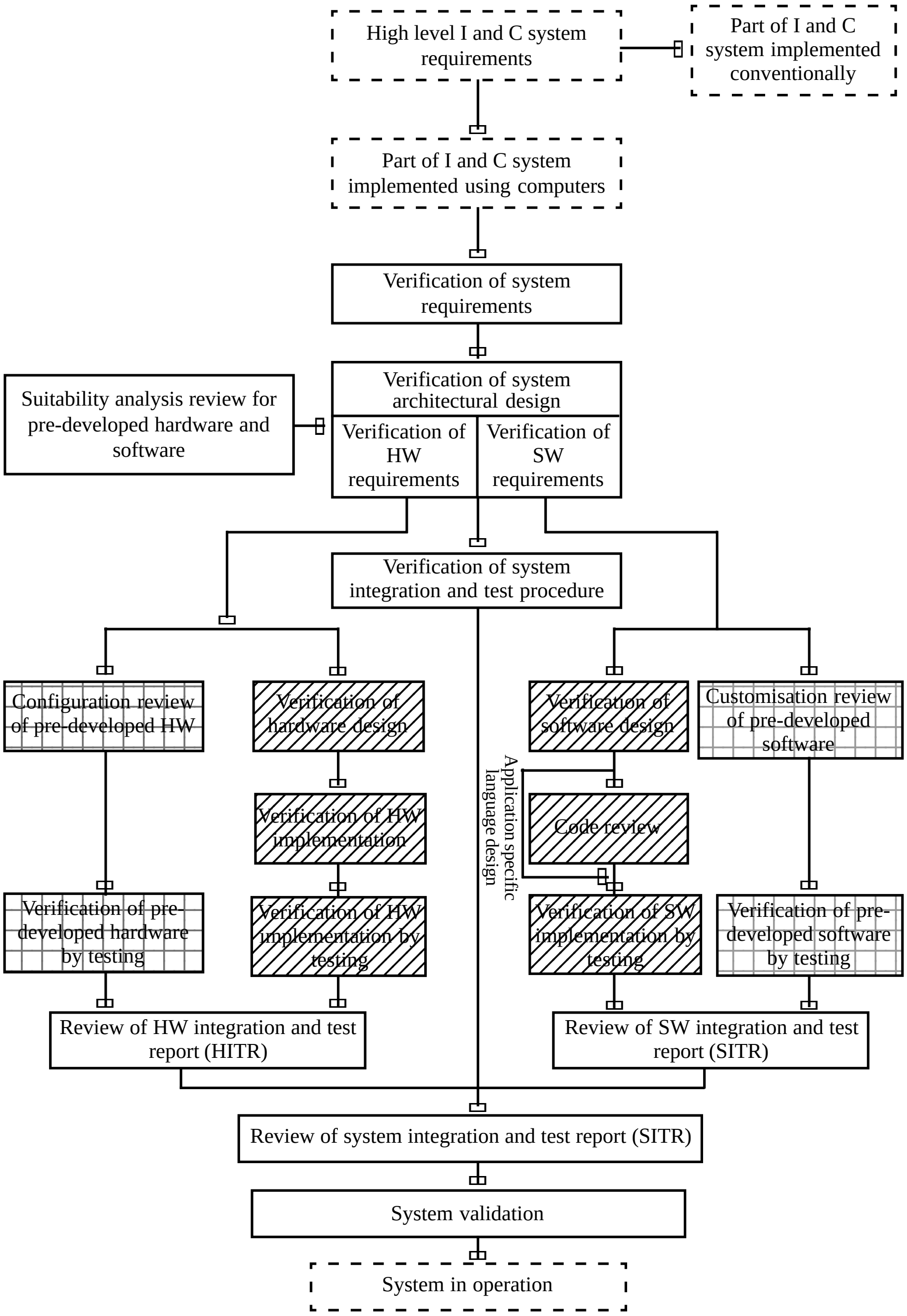
High level I and C system requirements
Part of I and C system implemented conventionally
Part of I and C system implemented using computers
Verification of system requirements
Verification of system architectural design
Verification of HW requirements
Verification of SW requirements
Suitability analysis review for pre-developed hardware and software
Verification of system integration and test procedure
Configuration review of pre-developed HW
Verification of hardware design
Verification of software design
Customisation review of pre-developed software
Application specific language design
Verification of HW implementation
Code review
Verification of pre-developed hardware by testing
Verification of HW implementation by testing
Verification of SW implementation by testing
Verification of pre-developed software by testing
Review of HW integration and test report (HITR)
Review of SW integration and test report (SITR)
Review of system integration and test report (SITR)
System validation
System in operation

FIG. 2 : SYSTEM V AND V METHODOLOGY

3. REGULATORY REQUIREMENTS

3.1 The Safety Case

The computer based systems, performing functions important to safety, shall be subjected to regulatory safety review prior to being deployed in nuclear power plant.

The subsection 3.2 states the regulatory requirements to be fulfilled with regard to computer based systems, performing functions important to safety. The fundamental importance of the quantitative estimate of reliability of computer based system, with necessary confidence margin, is well recognised. However, considering the problems associated with the quantitative estimation of software reliability, this guide places high level of importance on demonstration of qualitative attributes of software as reflected in its integrity level.

The computer based system should be demonstrated to be safe and of integrity level commensurate with the class of safety functions assigned to it.

3.1.1 Contents of Safety Case

The collective evidence of fulfillment of regulatory requirements shall constitute the safety case to be submitted to AERB and shall form the basis of AERB approval.

The safety case produced for computer based system, shall consist of documentary evidence, as applicable to safety class, to demonstrate that,

(i) System has been developed complying to regulatory requirements

(ii) System has been subjected to V and V as per recommendations of this guide

(iii) Pre-developed system components, if used in system, have been assessed as detailed under section 4 and have been found suitable

(iv) The system meets reliability and safety goals as demonstrated through safety and reliability analysis.

Collectively all computer based systems of class IA class shall meet criteria for protection against CCF.

Specific submissions for conducting regulatory reviews are provided in section 4.

3.1.2 Aspects not Covered in Safety Case

The computer based system submitted for review may in some cases form only a part of a I and C system. Hence aspects, which fall outside the scope of this guide, are:

(i) The correctness and completeness of the computer based system requirements (these requirements are the starting point of the development of computer based systems) with respect to the overall requirements of I and C system of which computer based system is a part

(ii) Compliance to all regulatory requirements by other parts of I and C system outside the computer based part (e.g. sensors, actuators, any hardwired equipment, interfaced to computer based systems etc.)

3.2 Regulatory Requirements for Computer based Systems

The overall regulatory requirements mainly relate to development process, system design, V and V and safety and reliability analysis of computer based systems of classes IA, IB and IC which are given in subsection 3.2.1 and subsection 3.2.2. Additional recommendations for class IA and IB systems are given in subsection 3.2.3. subsection 3.2.4 gives requirements for system safety and reliability analysis. subsection 3.2.5 describes requirements related to security.

The requirements given below are in addition to requirements of safety guides AERB/NPP-PHWR/SG/D-10 [3] and AERB/NPP-PHWR/SG/D-20 [4] wherever applicable.

The mechanical structures, sub-assemblies and components of computer based systems shall be designed as per applicable seismic categories specified in AERB safety guide AERB/NPP-PHWR/SG/D-1 [1].

3.2.1 General Requirements

For all systems of safety classes IA, IB and IC, following general requirements shall be met:

(a) System development plan shall be prepared to elaborate development life cycle (refer Appendix-1). Complete adherence shall be ensured to development life cycle described in system development plan and any deviation shall be justified during submission of safety case.

(b) Configuration management (CM) shall be integral part of the computer based system development process. The CM tasks and procedures to be followed in development of the computer based system shall be incorporated in the configuration management plan (development). The configuration control shall be applied to all plan documents, development tools, system requirements, all work products of software and hardware development process, input databases and project created databases, system software and pre-developed software which will be part of the final system. Complete list of configuration items

(CIs) shall be included in the configuration management plan (development) (refer Appendix-1).

(c) A system security plan shall be prepared for the computer based system to protect from unauthorised access during development and operation (refer Appendix-1).

(d) Quality assurance plans for hardware and software shall be developed prior to commencement of system development. The QA activities shall be performed by persons other than those involved in system design, manufacture and testing of computer based system. Performance of QA tasks as recorded in QA reports shall be audited during regulatory review of computer based systems. (refer Appendix-2).

(e) Verification plans and system validation plan shall be developed (refer Appendix-2). These plans shall be prepared prior to commencement of system development. These plans should address requirements of section 3 and section 4 as applicable.

(f) The computer based system achieves its defined purpose through interaction with external environment. Therefore the overall computer based system specifications shall be developed to clearly describe its functionalities, all external interfaces and system boundaries (refer Appendix-3). If the computer based system is forming part of a larger C and I system, then the computer based system requirements shall be described in relation to the larger C and I system.

(g) The development and V and V teams shall have necessary technical skills and be fully aware of requirements of this guide and other applicable regulatory guides.

(h) The system architectural design shall identify the role of hardware and software in the computer based system by mapping system requirements to hardware and software within the system. The hardware and software functions shall be defined completely and unambiguously (refer Appendix-4).

(i) The tools selected for the software specification and design should be suitable for the type of application (e.g. real-time). The use of computer aided software engineering tools is recommended as they help produce well documented specifications and designs, which improves the reviewability. The tools shall be suitably qualified for the safety class.

(j) For software development languages e.g. general purpose or application specific programming languages, development tools e.g.

compilers, code generators, testing tools, system software e.g. operating systems, the specific recommendations given in Appendix-6 for class IA and IB systems shall be complied with.

(k) The design and testing of hardware and software shall be carried out following the general design guidance (refer subsection 3.2.2 and Appendix-5 and Appendix-6).

(l) System integration and testing activities shall be carried out as per system integration plan (refer Appendix-7).

(m) Prior to commissioning of the computer based system at site, a configuration management plan for the system during the O and M phase shall be prepared (refer Appendix-1).

3.2.2. General Design Requirements

(a) Systems/sub-systems of higher safety class shall not depend on outputs from systems/sub-systems of lower safety class for performing their safety functions.

(b) Computer based system shall meet single failure criteria as per AERB/NPP-PHWR/SG/D-10 [3] and AERB/NPP-PHWR/SG/D-20 [4] respectively

(c) Communication channels between systems/sub-systems of different safety class shall be designed to ensure that faults in system/ sub-system of lower safety class do not affect safety functions of system/ sub-system of higher safety class.

(d) Stability, accuracy and timeliness of the performance of system functions shall not be adversely affected by operational conditions, length of the time system has been in operation, process avalanche conditions and in-service system testing demands.

(e) The system design shall ensure that software (i.e. run-time program code including safety parameters settings) is adequately secured against unauthorised access for modification at all times and unauthorised attempts are brought to the notice of operators.

(f) The system design shall ensure protection of the run-time program code including safety critical parameters settings, from virus attacks from any source. A computer based system shall not be part of any general-purpose network.

(g) The system design shall support role-based access to system by plant personnel (plant operators, supervisors, maintenance personnel etc.) If operator access is required to change data to operate the I and C functions then the human-machine-interface devices shall restrict access to the necessary extent.

(h) The overall I and C design shall ensure logging and archiving of operator actions through computer based systems, important safety parameters and operational data required for investigation of safety significant events during the operation of plant. Safety significant events shall be identified to define the logging and archiving requirements. The logged and archived data shall be time stamped to accuracy sufficient to carry out proper investigation of safety significant events. The logs shall be tamperproof.

(i) Pre-developed software used in the system should be analysed for security vulnerabilities and configured so as to minimise the vulnerabilities. Any remaining vulnerabilities shall be mitigated through additional means.

(j) The CPLDs/FPGAs/ASICs or similar programmable components used in designs of computer based systems shall be developed using software lifecycle approach. Requirements shall be traced to both design and verification tests.

3.2.3 Additional Requirements for Class IA and Class IB Systems

(a) Class IA computer based systems should only contain program code which is necessary to implement the intended operational functions and exceptions to this shall be justified. In case of IB systems any extra code shall be shown to be having no effect on system operation.

(b) For class IA systems additional verification and validation (V and V) shall be carried out by third party accepted by AERB. The identification/constitution of independent V and V team shall be performed at the beginning of the system development. The V and V team members shall have prior experience of carrying out V and V of at least IB class systems. For IB systems the verification and validation (V and V) shall be carried out by people who are independent of the system designers and accepted by AERB. The identification/ constitution of independent V and V team shall be performed at the beginning of the system development. The specific recommendations for V and V and reviews for class IA systems given in section 4 shall be complied with.

(c) Formal verification of specifications, algorithms, designs and code for demonstration of absence of errors in code are recommended.

(d) Computer based safety system (IA) or computer-based sub-system of a safety system shall meet online testability requirements as per AERB/NPP-PHWR/SG/D-10 [3].

(e) Computer based systems are susceptible to CCF due to wide use of standard hardware and because of software design errors which can also occur in all redundant channels of a system. Therefore if a CCF could disable a safety function (IA), a diverse means, which is unlikely to be subject to the same CCF, should be provided to perform either the affected safety function or a different function that provides adequate protection.

(f) Access control of class IA system shall be based on two factor authentication of personnel. Access control of class IB and IC system shall include reliable identification of personnel. Use of biometric as one of the factors is recommended.

3.2.4 System Safety and Reliability Analysis Requirements

System safety and reliability analysis requirements for IA and IB systems consist of the following :

(a) Confirmation of safety function implementation

(b) Failure analysis

(c) Common cause failure (CCF) analysis for IA systems

(d) Hardware reliability analysis.

The detailed recommendation on these analyses is contained in Appendix-8.

3.2.5 Security Requirements

Computer based systems important to safety shall be protected from unauthorised access and modification, and disruption of its functions (denial of service). A security plan that specifies the procedural and technical measures shall be prepared for each system important to safety to ensure that the system is designed, developed, delivered and operated with adequate security measures. (refer Appendix-1.)

3.3 Admissibility of V and V Carried Out by Agencies Without Prior Approval by AERB

Regulatory review process requires submission of design documents, V and V reports and various analysis reports as indicated in section 4. While the design documents and analysis reports are produced by the system designer, V and V is conducted by independent group. In case of pre-developed systems V and V would have been already conducted. If in such case, the V and V is carried out by agencies other than those approved/appointed by AERB, the following requirements shall be met:

(a) All necessary reviews shall have been conducted as recommended by this guide

(b) The reviews shall have established that all applicable requirements of this guide have been complied with

(c) The requirement of independence of V and V group as per 3.2.3.(b) shall have been complied with

(d) Pre-developed systems shall have approval of a national nuclear regulatory body, or, V and V reports should have been vetted by a national nuclear regulatory body

(e) In case of pre-developed components the V and V group shall have approval of any national regulatory body or it should be an established agency having experience of carrying out V and V of software/ computer based systems designs of comparable complexity.

(f) The V and V reports shall be accessible to AERB for review/audit as required

(g) Necessary additional submissions should be included in safety case in support of above requirements.

4. REGULATORY REVIEW PROCESS

This section deals with regulatory review processes for computer based I and C systems. The standard regulatory review process (SRRP) deals with newly developed systems and is explained in subsection 4.1. The review process for pre-developed systems is described in subsection 4.2. Generic design certification is described in subsection 4.3.

4.1 Standard Regulatory Review Process

This subsection deals with the standard review process for computer based I and C systems. These computer based I and C systems are specifically designed for use in NPPs. The software and hardware shall meet the requirements of this guide.

The SRRP is based on the recommended life cycle shown in Fig. 1 and the typical verifications and validation tasks shown in Fig.2. The submissions are made as indicated by tables 4.1-A and 4.1-B. Documents are to be generated as per the deliverables listed in each of the appendices. However merging of documents or of standard plans can be done as long as the information coverage is complete.

It is recognised that computer based I and C systems reviewed under SRRP may have used some pre-developed components. The review methodology for such pre-developed components is explained in subsection 4.1.2

4.1.1 Review Methodology for Newly Developed Systems

The objective of review of computer based system is to establish that the software and hardware have been designed to the recommendations of this guide. The review process is designed to confirm that the delivered system satisfies all aspects of its requirements and the safety analysis demonstrates safe behaviour of the system under all operational states. The review process consists of the following stages: (a) reviews of system requirements, plans, design outputs, safety and reliability analysis, and validation; (b) audit of V and V reports and QA reports.

4.1.1.1 System Requirements Review

SR is reviewed to confirm the following:

(i) SR complies with the recommended contents given in this guide (Appendix-3).

(ii) SR clearly indicates safety class of each function and overall system safety class.

(iii) SR is traceable to preliminary safety analysis report (PSAR).

4.1.1.2 Review of Plans

All the plans listed in table 4.1(A) are reviewed to ensure conformance to the regulatory requirements in section 3 and recommendations given in Appendix-1 and Appendix-2 of this guide.

4.1.1.3 Review of Design Outputs

Design outputs listed in table 4.1(A) are reviewed to ensure compliance to requirements of subsections 3.2.2 and 3.2.3 and various standards prescribed. The depth of the review shall depend on the safety class of the system.

IB class system should confirm that system failures cannot have adverse effect on safety functions and will not make frequent demands on class IA functions.

4.1.1.4 Review of Analysis Reports

Review the analysis reports listed in table 4.1(A) to:

(i) Confirm that traceability and correct implementation of safety requirements of the system in all development phases

(ii) Confirm compliance to single failure criteria as per AERB/NPP-PHWR/SG/D-10 and AERB/NPP-PHWR/SG/D-20.

(iii) Confirm protection against CCF in class IA systems

(iv) Hardware reliability analysis report shall be reviewed to confirm reliability goals specified in system requirements (SR).

4.1.1.5 Review of System Validation

Review system validation report to confirm:

(i) System validation is carried out as per the system validation plan

(ii) All systems requirements as per SR are covered in validation. For IA systems, all IA functions and associated logic have been completely checked.

4.1.1.6 Audit of Verification Reports and QA Reports

Verification reports listed in table 4.1(B) are audited to ensure that all verification tasks as per this guide are performed and all anomalies have been resolved. Hardware QA report is audited to confirm that all QA tasks have been performed. For software, process implementation compliance report is audited to confirm that the development, V and V and configuration management have been carried out as per respective plan.

TABLE 4.1 (A) : SRRP REVIEWS

Submittal	IA	IB	IC
1. Requirements			
1.1 System requirements (SR)	√	√	√
2. Plans			
2.1 System development plan	√	√	√
2.2 Configuration management plan - development	√	√	√
2.3 System security plan	√	√	√
2.4 QA plan - hardware	√	√	√
2.5 QA plan - software	√	√	√
2.6 Verification plan - hardware	√	√	√
2.7 Verification plan - software	√	√	√
2.8 System validation plan	√	√	√
3. Design Outputs			
3.1 System architectural design	√	√*	-
3.2 Hardware requirements specification	√	√*	-
3.3 Hardware design	√	√*	-
3.4 Software requirements specification	√	√*	-
3.5 Software design	√	√*	-
3.6 Software programmes (source code)	√	√*	-
3.7 Programming guidelines	√	-	-
4. Analysis Reports			
4.1 Confirmation of safety function implementation	√	√	√
4.2 Failure analysis report (for single failure criterion)	√	√	-
4.3 CCF analysis	√	-	-
4.4 Hardware reliability analysis	√	√	-
5. System Validation			
5.1 System validation report	√	√	√

* Intensity of review of IB class system can be less than that for IA and should confirm that system failures cannot have adverse effect on safety functions and will not make frequent demands on class IA functions.

TABLE 4.1 (B) : SRRP Audits

Submittal	IA	IB	IC
1. Verification Reports of:			
1.1 System architectural design	√	√	√
1.2 Hardware requirements specification	√	√	√
1.3 Software requirements specification	√	√	√
1.4 Hardware design	√	√	√
1.5 Software design	√	√	√
1.6 Software programmers (source code)	√	√	-
1.7 Software unit test	√	-	-
1.8 System integration and test	√	√	-
2. QA Reports			
2.1 Hardware QA report	√	√	√
2.2 Software QA report (process implementation compliance)	√	√	√

4.1.2 Review Methodology for Pre-developed System Components

Each pre-developed system component used in computer based system shall be evaluated for its suitability and quality for use in NPP systems important to safety. The degree of evaluation should be commensurate with the safety class of the system.

4.1.2.1 Review of Suitability Evaluation of Pre-developed System Components

Review pre-developed system component suitability evaluation to confirm the following:

(i) The functional, performance and constraint characteristics of pre-developed system component appropriate for system function.

(ii) Pre-developed system component does not contain any functions that are not required by the system. If it is not possible to eliminate such functions, it has been ensured and demonstrated that these extra functions will not affect the performance of safety functions of the system.

(iii) If the pre-developed system component was modified to satisfy the requirements given in (i) and (ii) above, the modification shall have been performed in manner specified in the configuration management plan.

4.1.2.2 Review of Quality Evaluation of Pre-developed System Component

Review of pre-developed system component shall be carried out to confirm the following:

(i) The pre-developed system component has been developed as per requirements given in this guide (development process compliance).

(ii) If complementary tests and/or documentation has been done to compensate for deficiencies in (i) above, review the test results and/or documentation to confirm that deficiencies are adequately compensated.

(iii) In case of any short fall in (ii) above, operating experience and product certification, if any, of the pre-developed system component may be used to substantiate quality evidence.

4.1.3 Review of Tools

The tools used in design, development and testing shall comply to tools validation requirements of IEC 60880 [9] in case of class IA systems and IEC 62138 [10] in case of class IB systems respectively.

4.1.4 Regulatory Review Report

Regulatory review report shall comprise of review reports and audit reports.

Acceptance criterion:

(i) For class IA systems : Satisfactory review, audit and validation

(ii) For class IB, class IC systems : Satisfactory review, audit and validation. Any deficiency shall be justified

4.2 Review Process for Pre-developed Systems (PDS)

4.2.1 Purpose

The review process for pre-developed systems is a variation of the SRRP as explained below.

Pre-developed systems can be grouped into two major categories:

(i) Certified pre-developed systems : Systems that have been qualified as per standards for computer based safety critical systems including standards applicable to NPP.

(ii) Commercial pre-developed systems : Pre-developed systems or HW-SW platforms that have proved to be reliable due to the way they have been designed and manufactured and also based on their use elsewhere and hence considered potential candidates for deployment in NPPs. However they were not formally qualified as per recommendations of any standards for computer based safety critical systems or of this guide.

In case of pre-developed systems, the development process, V and V and certification/regulatory reviews would have happened in the past. The design outputs and the reports of V and V and certification/regulatory reviews shall be scrutinised (through audit) to determine if the complete process as implemented can be treated as equivalent to the recommendations of this guide. The balance of reviews for PDS is to be carried out as per SRRP. If PDS was qualified to standards applicable to NPPs it is then easier to establish equivalence to the requirement of this guide. Additionally pre-developed systems may have operational experience which can be assessed and given appropriate consideration in the regulatory review. These differences have been factored into recommendations in following subsections.

4.2.2. System Requirements Review

SR is reviewed to confirm the following:

(i) SR complies with the recommended contents given in this guide (Appendix-3)

(ii) SR clearly indicates safety class of each function and overall system safety class.

(iii) SR is traceable to preliminary safety analysis report (PSAR).

4.2.3 Review and Assessment of Plans

(i) Quality assurance plan (QAP) of the design organisation shall be reviewed to establish that following processes are governed by the QAP:

- Design and implementation of software
- Design, manufacturing of hardware
- Testing and integration of system
- Documentation generation
- Procurement tasks
- Tasks carried out by subcontractors.

(ii) Quality assurance plans (hardware and software) that were applied during development of PDS shall be reviewed for conformance with recommendations of Appendix-2.

(iii) The software verification plan that was applied during development of PDS and system validation plan used by developer for validation shall be reviewed. The reviews shall be conducted to check conformance to requirements of this guide.

4.2.4 Review of Design Outputs

Design outputs listed in Table 4.2(A) are reviewed to ensure compliance to requirements of subsections 3.2.2 and 3.2.3 and various standards prescribed. The depth of review shall depend on the safety class of the system.

IB class system should confirm that system failures cannot have adverse effect on safety functions and will not make frequent demands on class IA functions.

4.2.5 Audit

Design, V and V documents and certification or regulatory approval reports listed in table 4.2(B) shall be audited.

4.2.6 Customisation/Configuration Review

(i) The PDS systems may be configured/customised for deployment in the NPP. This configuration/customisation process shall not involve hardware and software modifications but may involve configuration of databases, system parameters etc.

(ii) Configuration and customisation shall be reviewed to ensure compliance to SR.

4.2.7 Review of Analysis Reports

Review the analysis reports listed in table 4.2(A) to:

(i) Failure analysis - confirm compliance to single failure criteria.

(ii) Confirm protection against CCF in class IA systems

(iii) Hardware reliability analysis report shall be reviewed to confirm reliability goals specified in SR.

4.2.8 Review of Operating Experience

(i) The operating experience of PDS shall be reviewed to ascertain that the observed reliability is commensurate with overall reliability goals stated in SR.

(ii) The operating experience shall relate to the PDS version (hardware/ software) to be deployed in NPP.

4.2.9 Review of System Validation

Review system validation report to confirm:

(i) System validation is carried out as per the system validation plan

(ii) All systems requirements as per SR are covered in validation and for IA system all IA functions and associated logic has been completely checked.

TABLE 4.2 (A) : PDS REVIEWS

Submittal	IA	IB	IC
1. Requirements			
1.1 System requirements (SR)	√	√	√
2. Plans			
2.1 Quality assurance plan of the design organisation	√	√	√
2.2 Configuration management plan - development	√	√	√
2.3 Verification plan - software	√	√	√
2.4 System validation plan	√	√	√
3 Design Outputs			
3.1 System architectural design	√	√	√
3.2 Hardware design	√	√	√
3.3 Customisation/Configuration description	√	√	√
3.4 System build	√	√	√
4. Analysis Reports			
4.1 Analysis of failures within PDS on its outputs	√	√	-
4.2 CCF Analysis	√	-	-
4.3 Hardware reliability analysis	√	√	-
5. Operating Experience			
5.1 Operating experience data	√	√	√

TABLE 4.2 (B) : PDS AUDIT

Documents	IA	IB	IC
1. Plans			
1.1 QA Plan - hardware	√	√	√
1.2 QA Plan - software	√	√	√
2. Design Outputs			
2.1 Software requirements specification	√	√	√
2.2 Software design	√	√	-
2.3 Programming guidelines	√	√	-
2.4 System integration and test plan	√	√	-
2.5 System integration and test report	√	√	-
2.6 System validation report	√	√	√
3. Verification Reports			
Verification report of software requirements specification/application programming requirements	√	√	√
Verification report of software design	√	√	-
Verification report of code/programs in application programming languages	√	√	-
4. Certification Reports			
4.1 Certification/regulatory approval reports (report of compliance to general design criteria, safety criteria and quality policy)	√	√	√

4.2.10 Availability and Accessibility of Documents

The documents and reports required for carrying out reviews and audits above shall be available and accessible to the review teams and to AERB as and when needed.

4.2.11 Regulatory Review Report

(i) All reviews and audits shall be performed to assess compliance to sec. 3.2 of this guide

(ii) Regulatory review report shall comprise of review reports and audit reports [tables 4.2(A) and (B)].

(iii) Acceptance criterion

(a) For class IA systems: Satisfactory review, audit and validation

(b) For class IB and class IC Systems: Satisfactory review, audit and validation. Any deficiency shall be justified

4.3 Review Process for Generic Design Certification

4.3.1 Purpose

Products involving software or hardware or both which have been designed for specific purpose and can be used as ready to use building blocks in design and implementation of computer based I and C systems can be offered to AERB for evaluation under generic design certification. Examples of such products are PLCs, SCADA software, real-time data base software, software design tools, real-time operating systems etc.

During generic design certification review the offered product designs will be evaluated to check if they comply with the requirements of this guide. The evaluation will be carried out based on the safety class to which the product is to be certified. Once certified the product can be incorporated in I and C system to perform functions of the safety class to which it has been certified.

4.3.2 Review Process during Design Certification

Based on the nature of product offered for generic certification, the applicable subsections of 4.1 or 4.2 will be invoked to carry out the evaluation.

The evaluation will be valid for the version of the product submitted. Generic design certification report will be generated based on the review process invoked.

4.3.3 Review Process at the Time of Deployment

Additional reviews will be conducted at the time of review of computer based I and C system in which a design certified product is incorporated. The reviews will focus on

(i) Confirming that the design certified component has been used in the system without modification.

(ii) Confirming that interface requirements of the design certified component have been met, where applicable.

(iii) Confirming that the design certified component has been properly customised/configured to meet system requirements.

APPENDIX-1

PROJECT MANAGEMENT PLANNING

A1.1 Introduction

The development of a computer based system should be carefully planned at the beginning of the project and these plans must be strictly followed throughout the project. The plans should guard against risks which are inherent in the development of a new computer based system, keeping in consideration the capabilities of current technologies to meet the functional and performance requirements of the system.

The planning process includes system development planning, configuration management planning and system security planning.

A1.2 System Development Plan

It is recommended that the model of development life cycle as recommended in this guide should be followed for system design, development of both hardware and software and system integration. Engineering Procedures should be defined which describe the work methods to be followed and work products including documents, to be generated during the development life cycle to ensure such compliance. Any deviation in the model should be justified in accordance with the applicable safety class of the system.

The development organisation should define detailed design guidelines for system design, coding etc. to ensure that the entire design activity is carried out in conformance with the requirements of this guide. If it is proposed to utilise any pre-developed and/or any readily available hardware/software omponents, these should be assessed to ascertain their suitability for use in the applicable class of systems.

The organisational structure of system development agency should be identified clearly assigning responsibilities. The methods and resources to be used for each phase of development should be identified in conformity with the quality assurance plan. The deliverables for each phase of the life cycle should be identified and acceptance criteria for these should be defined in conformance with the requirements of this guide.

It is also recommended that an internal mechanism is established to carry out a preliminary review for the product of each stage of the development activity to ascertain conformance to engineering procedures, and assure product quality and correctness.

A1.3 Configuration Management Plan

A1.3.1 The configuration management (CM) activity shall control and coordinate the identification, storage and any changes in the hardware and software components of the computer based systems including all associated documents and tools. Each such component/collection of components should be treated as a configuration item (CI) for the purpose of CM. The whole system/sub-system should be treated as a CI which is composed of lower level CIs derived from the design process. The CIs should have sufficient granularity so as to ensure precise control and should be easy to manage as discrete physical entities.

A1.3.2 The configuration management plan (CMP) should be defined to conduct and document major CM activities which must include configuration identification, configuration change control, configuration status tracking/reporting and CI release. It should ensure that all components can be identified, and system/ sub-systems are built from a consistent set of such components. Every change to the component should be approved and documented along with authorship and reasons for change and all versions of each component should be available. The plan should also address roles and responsibilities and guidelines and procedures for the following activities.

(a) Configuration identification

It is required to systematically identify CIs such that each CI must have a unique name and version number. A derived CI, obtained from source CIs and the procedure for generating the same (including tools involved) should also be identified.

(b) Configuration change control

Configuration change control should be exercised to ensure proper evaluation of the proposed changes and coordinate the implementation of approved changes and release of new versions of CIs after subjecting them to review/testing. The process involves generation of a formal change request, generation of impact analysis report, approval of the change by CI control authority, and change implementation and test, review and release. The impact analysis should analyse the proposed change for effort involved, other CIs affected by the change, requirement for additional testing and V and V etc. The configuration change control procedures should identify responsibilities and methods for carrying out various tasks listed above.

(c) Configuration status tracking/reporting

The purpose of this activity is to keep information about all CIs that have been created and their versions, status of all change requests and CIs releases.

(d) CI release

The CIs are in the custody of CM authority and the purpose of this CM activity is to make release of CIs as and when required for any purpose.

Based on the above guidance (items (a) through (d)), CMP should be prepared for the development phase (CMP-development) as well as for the O and M phase (CMP-OM). The inputs to CMP for development phase are system development plan, which identifies all documents to be produced and the system architectural design, hardware design and software design, which define all the components. This input is used to define the hierarchy of CIs and results in the list of configuration items. The configuration items for CMP-OM should include system build as deployed, parameter settings, all documentation at site which can be affected by any changes in hardware and software.

A1.4 System Security Plan

The system security plan shall specify the procedural and technical measures to be taken to protect the computer based I and C systems important to safety. An analysis of the potential security threats regarding the system and software shall be performed by taking into account the relevant phases of the system and software life cycles. It shall identify the counter measures including recovery procedures in case of loss of system due to any security related incident. It shall include:

(i) Procedures related to the interface between administrative and technical security, access to systems, security aspects of data handling and storage, security aspects of modification and maintenance, security auditing and reporting, and security training

(ii) The security plan shall also address security procedures to be applied during operation such as for periodic audits, resolution of anomalies discovered during operation, assessment of safety system changes and their impact on safety system security so as to ensure that modifications do not introduce any security vulnerabilities.

A1.5 Deliverables

The following are the deliverables from this phase

(i) System development plan

(ii) Configuration management plan - development

(iii) Configuration management plan - O and M

(iv) System security plan.

APPENDIX-2

QUALITY ASSURANCE AND VERIFICATION AND VALIDATION

A2.1 Quality Assurance (QA)

The responsible organisation (RO) shall have organisational level QA plan compliant to the requirements of AERB/NPP/SC/QA (Rev. 1) [7]. Separate quality assurance plans shall be developed for hardware, software and system for computer based system at the beginning of the system development. These plans shall be prepared within the framework of organisational level QA plan.

(a) The QA plans for hardware, software and system aspects shall cover all processes required to implement system development plan and configuration management plan described in Appendix-1 and V and V and safety analysis.

(b) The QA plans shall identify all the governing standards and procedures (for products and processes) to be used during the project.

(c) The QA plans shall specify mechanism for the reporting and disposition of non-conformance to standards and procedures.

(d) The QA plan for hardware, software and system shall have specific tasks which have impact on safety as described in AERB/NPP/SC/QA (Rev. 1) [7].

A2.2 Verification and Validation (V and V)

A2.2.1 V and V Planning

At the beginning of system development, plans and procedures shall be produced which shall cover hardware verification, software verification and system validation (refer Fig. 2).

(a) The verification plans and procedures shall contain

(i) Description of all required verification tasks

(ii) Tools, techniques and procedures that will be used to perform verification

(iii) List of verification goals for each stage (e.g. missing requirement, implementation error, violation of quality attribute etc.)

(iv) The teams performing verification activities.

(b) The system validation plan and procedures shall contain

(i) Description of system under validation

(ii) Test and measuring equipment details

(iii) Simulator details if applicable

(iv) Test cases, test procedures and acceptance criteria

(v) Traceability to system requirements.

A2.2.2 Verification Requirements

(a) Verification shall be carried out for each of the following:

(i) System architectural design

(ii) Hardware requirements specification

(iii) Software requirements specification

(iv) Hardware design

(v) Software design

(vi) Hardware implementation and testing

(vii) Software implementation and testing.

The process of verification at each stage shall include confirmation that

- refinement of the design carried out at this stage is traceable to the requirements of previous stage (forward traceability),
- no design object in this stage exists which can not be traced to requirements of previous stage (backward traceability),
- requirements of previous stage are correctly interpreted/ implemented,
- design guidelines and applicable standards have been complied with, and disposition of non-conformances has been carried out as per agreed procedure, and
- functional and performance requirements have been met at various stages.

(b) Verification of programmable hardware components

Design process of hardware programmable components like CPLDs, FPGAs, ASICs, used in implementation of class IA and IB systems, shall include generation of functional requirements and design documents. The verification will involve tracing design to the requirements (both forward and backward traceability) and testing with complete traceability to requirements.

(c) Software code verification

In case of safety class IA and IB systems, for the software developed using general purpose languages, the code verification should include the following :

(i) Traceability of code to software design

(ii) Verification of call graph

(iii) Verification of control flow

(iv) Review of interrupt handling

(v) Review of exceptions handling

(vi) Review of implementation of communication protocols

(vii) Review of buffer usage

(viii) Verification of functional and performance requirements (unit and integration testing)

(ix) Compliance to programming guidelines

(x) Compliance to design and implementation guidelines of IEC 60880 (for class IA only) [9]

(xi) Review for absence of malicious programmes.

Use of static and dynamic analysis tools is recommended.

In case of software developed using application oriented languages, the verification tasks shall include

(i) Traceability of application programmes to their specifications

(ii) Functional testing of application programmes.

(d) Confirmation of safety function implementation

During verification, it shall be ensured that system level safety requirements have been properly carried and correctly interpreted and implemented during following design phases:

- System architectural design
- Hardware requirements specification
- Software requirements specification
- Hardware design and implementation
- Software design and implementation.

(e) Verification reports

The results of all verifications carried out shall be issued as stage wise verification reports. Verification reports shall be maintained to provide evidence that all planned verifications have been performed, results recorded and anomalies investigated and corrected using change control procedures (see Appendix A1) and re-verified.

A2.2.3 System Validation Requirements

The completely integrated system shall be subjected to system validation testing to demonstrate that the system achieves its overall functional and performance requirements. System validation testing is planned based on the system requirements (SR). Testing with simulators is recommended.

(a) The validation tests should aim at

(i) Testing of system in all modes of operation and transfers from one mode to other mode of operation

(ii) Functional testing to exhaustively test the implementation of all the specified functionalities of the system

(iii) Performance testing to test the performance requirements of the system. The testing should be done to establish that nominal and worst-case performance targets are met

(iv) Testing of human computer interface. Testing of user commands and system responses, error and diagnostic messages, response times etc. should be covered

(v) Stress testing to test behaviour of the system beyond the rated load. The objective of stress tests is to verify that contingency measures in the system when overload conditions occur, such as maintenance of all priority services while guaranteeing performance requirements etc. work as required. Other design features like management of buffers, use of system resources etc. are also tested during stress testing

(vi) Stability testing to demonstrate output stability with continuous system operation under all operating environments

(vii) Failure mode testing shall demonstrate the behaviour of the system in the case of hardware and software failures. In case of fault tolerant systems the system should recover from all specified faults and continue to provide service. The faults should be simulated and recovery period for various types of faults should be checked against the specified limits

(viii) Safety tests should be carried out to ensure all safety functions are correctly implemented

(ix) Interface testing is designed to validate system for external interface (interfaces with sensors, actuators, other systems, external environment etc.) requirements

(x) Security testing is aimed at checking that basic security mechanisms provided in the system are able to protect the integrity and availability of the system in all modes of operation.

(b) The results of the validation testing shall be documented in detail and shall contain the following information:

(i) Verification of system build including hardware and software and their versions

(ii) All events that occur during the testing process which require further investigation (test incidences)

(iii) Summary of the results of the designated testing activities and the conclusions based on these results.

Chronological record of relevant details about the execution of tests (test log).

A2.2.4 Verification of User Manual

User manual verification should include verification of system operating procedures in different operating modes, commands, options, error and diagnostic messages, help facilities, operation of utilities provided to the operating staff etc.

A2.3 Deliverables

The following are the deliverables from this phase

(i) QA plans - hardware and software

(ii) QA reports - hardware

(iii) QA reports - software (process implementation compliance)

(iv) Verification plans and procedures (hardware and software)

(v) System validation plan and procedure

(vi) Verification reports (hardware and software)

(vii) System validation report

(viii) Verification report of user manuals.

APPENDIX-3

SYSTEM REQUIREMENTS

A3.1 Introduction

The system requirements specifications describe the computer based system as a black box and are implementation independent. The system requirements should be specified at the beginning of the project, and must be complete, comprehensive, consistent, verifiable and unambiguous. The specifications should describe an overview of the system with the help of a context diagram so as to bring out its role in the nuclear power plant, and also state its safety class. Its relation, if any, to the other safety/engineered safety systems of the nuclear power plant should be specifically brought out.

A3.2 Functional Requirements

A list of functional requirements should be given followed by detailed description of each. The functional requirements should be described in narrative form using simple and unambiguous sentences. If the function involves decisions to be taken based on relatively complex logic, then formal notations such as flow chart, Boolean expressions, or state transition diagram could be used to describe the function. Information on the aim of the function, criticality, priority and safety class applicable for this function and inputs taken and outputs produced should be specified for each function.

The functional requirements under various modes of system operation, wherever applicable, should also be described. These include, for example, system start-up, normal operation, shut-down, fault recovery states, degraded operation under various types of sub-system, component and sensor failures, and operational modes and mode changeovers.

Requirement for data archival and retrieval could arise due to need for long term trend monitoring of parameters, incidence analysis, need for analysing operator actions, need to analyse system performance, and to meet regulatory requirements,. The requirements should specify data (including operational records) to be archived, frequency and period for archiving, and retrieval requirements.

Safety-related functional requirements: To ensure plant safety, specifications should clearly bring out the requirements regarding the state of all relevant physical outputs of systems under partial or total system failures so as to ensure fail-safe state in case of irrecoverable internal failures.

A3.3 Security Requirements

The security requirements in terms of access to computer system to persons at different levels with different requirements through secure means such as hardware key interlocks and/or passwords directly, or through network, should be specified. These should also address need, if any, for annunciation, on-line logging of accesses or recording identity of the user etc.

A3.4 Performance Requirements

The information on performance requirements shall be specified in terms of accuracy, resolution and response time required for various outputs associated with each functional requirement in each of the modes of operation as stated in the previous paragraph. In addition, the performance under conditions of maximum load (i.e. system throughput) should also be stated.

A3.5 Interface Requirements

A3.5.1 Interface with field I/O

The specifications should include description of

(i) Inputs from plant processes and operator panels, static and dynamic characteristics of sensors, signal conditioning requirements, signal validation requirements etc.

(ii) Outputs to plant processes and operator panels, static and dynamic characteristics of actuators, state under various failure conditions, validation checks to be done etc.

A3.5.2 Interfaces with other computer based systems

The interface of the system with other computer based systems as applicable should be described. The interface requirements should describe specifics of the information to be exchanged between the systems, and its periodicity. These should also describe the protocol to be followed including physical characteristics (galvanic isolation, cable length etc.) error checking and recovery, timing and speed characteristics, etc. In case of redundancy built using channelised implementation, requirements of physical isolation shall also be specified.

A3.5.3 Interface with station master clock

In order to ensure proper post incidence analysis it is necessary that all data logged is properly time stamped. All systems therefore should be time synchronised with the help of station master clock and the interface must be clearly stated.

A3.5.4 Human computer interface (HCI)

The HCI requirements should include nature (physical, soft) and detail of interfaces, and, operator functions required at each interface taking into account the user profile, as well as the sequence of dialogue between human and computer for each applicable operator function. The ergonomic requirements of controls and displays e.g. use of symbols, colours, alerting signals, etc. should be stated, but these must follow a uniform scheme plant wide and across all systems. Any special requirements, e.g. operator actions for rapid handling of emergencies, system response times to operator requests, refresh rates of displays, need for appropriate messages in response to operator errors etc. should also be specified explicitly.

A3.6 Environmental Requirements

The various environmental conditions to which the computer based system will be subjected during transport and storage at site and during its operation should be specified. These could include climatic conditions, vibration and shock, seismic qualification, classification of the system and qualification requirements, EMI/RFI, radiation levels etc.

The specifications of all power supply requirements shall also be included.

A3.7 Testing, Diagnostics and Self-supervision Requirements

Requirement for diagnostic programs/hardware should be specified to detect various hardware/software faults and to take appropriate actions. This should include identification of system resources to be checked, diagnostics on system start-up and during run-time, and requirements for audio-visual annunciation on detection of faults.

A3.8 Reliability Requirements

The reliability requirements should be commensurate with the criticality of the functions performed by the system. Quantitative reliability target or on demand failure probability, as appropriate shall be specified.

A3.9 QA Requirements

QA requirements should be specified in accordance with Appendix-2.

A3.10 V and V Plan Requirements

V and V requirements should be specified in accordance with Appendix-2.

A3.11 Documentation Requirements

Requirements for hardware and software documentation to be produced during development of computer based system should be stated. These should take into account regulatory documentation requirements as applicable to different classes of systems.

A3.12 Deliverables

The following is the deliverable from this phase

(i) System requirements (SR).

APPENDIX-4

SYSTEM ARCHITECTURAL DESIGN

A4.0 Introduction

The system architectural design phase is the ‘solution’ phase of the computer based system development life cycle and follows the system requirement specification phase. The main input to this phase is the system requirements document (Appendix-3).

The purpose of this phase is to decompose the system (subsection 2.2, Fig. 1) into a hierarchy of coherently partitioned subsystems which will serve as units for encapsulating functionality. This decomposition will be influenced by operational, safety, maintainability and layout considerations. Each subsystem shall be sufficiently independent to allow its specification and design to be carried out in parallel. The allocation of functions to hardware and software within each subsystem should be done alongside and interfaces between the sub-systems as well as with the external world shall be defined formally. Thus the development of each subsystem including development of its hardware and software can follow independent life cycle activities.

A4.1 Architectural Design

The design and development should be carried out based on general design principles relevant to assuring safety as enunciated in AERB safety guides AERB/NPP-PHWR/SG/D-1 [1], AERB/NPP-PHWR/SG/D-10 [3] and AERB/NPP-PHWR/SG/D-20 [4]. Depending upon the safety levels required to be met, these principles include simplicity, defence in depth, separation of safety functions from non-safety functions, diversity, single failure criterion etc. The design of security features should ensure prevention of unauthorised access to the hardware and software especially for alteration of crucial parameters.

The computer system architectural design is a fully documented physical model of the computer based system and shall define the major sub-systems and their interfaces and should include the description of overall architecture and decomposition description of the system as well as definition of sub-systems. It should also state in adequate level of detail, which functional requirements are to be met by each sub-system and also describe how the overall performance requirements are met. The design documentation should unambiguously define external and internal interfaces for each sub-system and should also provide a description of fault diagnosis and fail-safe design features.

The design should also describe how requirements other than functional and performance, are met for each sub-system.

The system integration and test procedure should be defined to carry out the reverse process, i.e. integrating the system from the decomposed constituents.

During detailing of the architectural design, the functionalities for each sub-system are further allocated to hardware and software to achieve proper balance between performance and constraints. This process of allocation of functionalities should be faithfully carried over to the definition of hardware requirements and software requirements as described in the following sections.

A4.2 Hardware Requirements

The hardware requirements should be evolved for each of the sub-systems forming part of the total computer based system using the inputs from system requirements document. The hardware requirements for each sub-system shall define all infrastructure requirements to ensure that the software resident on the same can meet all functionalities and performance allocated to the corresponding sub-system, highlighting safety-related requirements (Appendix-3).

The hardware requirements for each sub-system should provide a precise definition of the interfaces with field inputs and outputs, with other systems/ sub-systems, with master clock and with the operator. These should also cover non-functional aspects of the computer system requirements such as component and equipment qualification, electromagnetic interference, power supply requirement etc. The requirements should state the hardware support required for the software to carry out all relevant diagnostics, provide error indications etc.

It should include a description of types of hardware failures, which have to be tolerated without loss of function or with defined limited loss of function. Requirements for watchdog and switchover logic in case fault tolerant architectures are selected should be included. It should include definition of hardware/software interfaces and associated exception handling.

In addition, the requirements documentation should also state whether physical separation and electrical isolation between various hardware subsystems are required. ‘Fall-back’ requirements should specify how the computer based system must react to the potential failures at the interface with the plant. Security constraints, if any, such as prevention of unauthorised access, prevention of virus codes, etc. should be specified.

A4.3 Software Requirements

The software requirements should be evolved for each of the sub-systems forming part of the total computer based system using the inputs from system requirements document. Since software requirements are the input for the software design and coding phases, these should be written such that they bridge the developers' view and the designers' view. The software requirements for each sub-system shall include all functionalities and performance allocated to the corresponding sub-system, highlighting safety related requirements. In general the requirements should be specified to be met by the software of each sub-system, such that all sub-systems functioning in harmony lead to the collective system meeting the requirements stated in SR document (Appendix-3).

The software requirements should be neatly documented such that these are clear, unambiguous, consistent and verifiable. The textual descriptions should be augmented using logical and behavioural models of software, developed using standard methodologies.

In addition, the software requirements should address requirements applicable to the specific sub-system in terms of human computer interaction as applicable, interfacing with other systems/sub-systems, coping with hardware failures, self-diagnostics and corresponding error messages, modes of computer system operation, software maintainability, etc.

The application of formal methods of specifying requirements to aid in removing ambiguities and ensuring consistency are desirable for class IA systems.

A4.4 Verification of System Architectural Design

The architectural design documentation should provide a complete matrix of traceability of all requirements stated in system requirements document to the requirements listed against each sub-system hardware and/or software.

A4.5 Deliverables

The following are the deliverables from this phase

(i) System architectural design

(ii) Hardware requirements specification

(iii) Software requirements specification

(iv) System integration and test plan and procedure.

APPENDIX-5

HARDWARE DESIGN, DEVELOPMENT AND TESTING

A5.1 Introduction

The combination of hardware and software, which make up the computer system, must together achieve the required accuracy and response times to satisfy the overall system performance requirements. The hardware design and development phase of the system development life cycle proceeds simultaneously with the software design phase; the purpose is to design the hardware decomposing it into the required mechanical, electrical and electronic modules and their inter-relationships.

The design and development should be carried out based on general design principles relevant to assuring safety as enunciated in AERB safety guides AERB/NPP-PHWR/SG/D-1 [1], AERB/NPP-PHWR/SG/D-10 [3] and AERB/NPP-PHWR/SG/D-20 [4]. Depending upon the safety levels required to be met, these principles include simplicity, defence-in-depth, separation of safety functions from non-safety functions, diversity, meeting single failure criterion etc.

A5.2 Hardware Design

The selection of computer sub-system hardware should address the performance and reliability requirements contained in the system requirements document (Appendix-3). The use of tools for design and for simulation testing should be considered to detect problems early in the design life cycle.

The design and development of any sub-systems and modules shall conform to hardware requirements identified in the system architecture design (Appendix-4). In case off-the-shelf available equipment, module, or component (e.g. hardware with built-in programs) is proposed to be utilised, evidence shall be provided that such hardware is qualified to meet the design requirements.

The hardware design should include features for on-line diagnostics and should allow to be taken off-line for periodical testing and calibration. It should provide facilities to ease maintenance. Design measures should be used to achieve required reliability level commensurate with the safety class of the system. The design of security features should ensure prevention of unauthorised access to the system. The specific recommendations for design of hardware as given in IEC 60987 [11] should be followed.

A5.3 Hardware Design Document

The hardware design document should describe the hardware architecture as well as the structure of the proposed implementation. It should provide details of the function of each constituent, its design description and the numbers required. It should further provide the scheme for interconnection of these constituents with each other and with external hardware including field/panel elements as well as other systems/sub-systems.

The document should show how fail-safe behaviour is achieved. Anything affecting the compliance of the design with the specified functional and performance requirements, and, environmental conditions etc. should be brought out. Maintenance activities needed to meet the performance and reliability requirements like operational tests, calibration, repair, replacement periodicity and procedures should be included in the document. The document should include any special manufacturing instruction to meet the hardware requirements. Any specific installation and commissioning, maintenance and operation instructions should also be included.

A5.4 Verification of Hardware Design

The hardware design documentation should provide traceability of the hardware design to all the requirements listed against the corresponding sub-system hardware in the system architectural design.

A5.5 Hardware Integration and Testing

Test procedures should be defined for each hardware constituent to check the functional, performance and environmental requirements to be met by it. Each hardware module should be tested independently to confirm it meets the design intent.

Test procedures should also be defined (hardware integration and test procedure) for assembled hardware of each sub-system constituent to check the integrity of the assembled hardware. Each assembled sub-system should be integrated with appropriate test software and checked using these procedures to confirm its integrity and a hardware integration and test report should be generated.

A5.6 Deliverables

The following are the deliverables from this phase

(i) Hardware design

(ii) Hardware integration and test procedure

(iii) Hardware integration and test report.

APPENDIX-6

SOFTWARE DESIGN, IMPLEMENTATION AND TESTING

This appendix deals with all software development phases and applicable requirements. The software development as addressed in the following sections deals with

(i) Development of software design

(ii) Development of code

(iii) Software testing.

The main inputs to these phases from the previous phases are:

(i) System requirements

(ii) System architectural design

(iii) Software requirements specifications.

A6.1 Software Design

(a) Software design using general purpose languages

Software design is a process of designing software components, which can be collectively executed to achieve the required functionality and performance. The design is usually carried out in two stages - design of software architecture and software detailed design.

Software architectural design

The software architecture represents highest level decomposition of software into major interacting components, which are identified and defined in this phase. Decomposition should follow techniques of partitioning/layering. The architectural design results in construction of physical model of the software that defines

(i) Components that compose the software

(ii) Hierarchy of control

(iii) Global data structures/data bases

(iv) External interfaces

(v) Data flow between components (component interfaces)

(vi) Interrupt and exception handling.

The physical model uses implementation terminology (processes, tasks, files, databases etc.) and provides framework for software development that allows independent work on design of low level components in the detailed design phase. The response time and other timing related specifications can have great influence on this design and hence the design of the components should be analysed to ensure their fulfilment. The requirements that do not influence the software architecture may be deferred to detailed design phase for implementation.

Software detailed design

Detailed design follows from the software architectural design. The process of decomposition is carried out further till all lower level components are defined. The detailed component design shall include specification of its internal implementation of components and their interface with other components. The software design should be carried out to meet design guidelines. The design guidelines should specify rules for following:

(i) Naming conventions for components and variables

(ii) Method of documenting the module specifications

(iii) Criteria for sizing and controlling complexity of modules

(iv) Procedures for handling for all types of exceptions/error conditions.

Software implementation

Software implementation follows software design and results in generation of source code. The development of source code should follow the programming guidelines (see A6.4).

(b) Software design using application specific languages

Application specific languages allow software detailed design to be carried out using graphical notations, textual language or mix of both. The code is generated automatically using code generator. The generated code can be in the form of general purpose programming language (e.g. C) or in some proprietary format and is interpretively executed at run time. Thus in this case there is no software implementation phase.

For class IA systems conformance to IEC 60880 [9] recommendations applicable for use of application programming language shall be ensured.

(c) Software design and code generation tools

The software design and code generation tools, compilers, linkers shall comply to tools validation requirements of IEC 60880 in case of IA systems and IEC 62138 [10] in case of IB systems respectively.

(d) Documentation of software design

The software design shall be documented using techniques that will help in tracing design to software requirements and therefore will ease the process of review. The important aspects of design that need to be clearly brought out in the software design are the flow of control between software components, inter component and external interfaces, the internal structure of components at different levels of hierarchy, global data / shared data bases and interrupt and exception handling.

A6.2 Design of Diagnostics

The implementation of systems using computers enables designers to build in diagnostics to detect faults in the hardware, data or code corruption and take appropriate actions. Therefore software should include supervision of data and its control flow. In failure situations where ability of the software to ensure safe outputs is questionable, external independent means shall be utilised to ensure safe system behaviour.

A6.3 Test and Integration of Software

At the end of software design activity a plan should be prepared detailing all software integration and testing activities. The plan shall define

(i) Unit test procedures and test coverage criteria

(ii) Software integration stages

(iii) Testing tools to be used

(iv) Detailed test cases.

The test results and observation shall be recorded in a document for review/ audit during V and V.

For class IA systems the requirements of IEC 60880 [9] applicable to software test and integration shall be complied with.

A6.4 Programming Guidelines

Programming guidelines for software implementation should be developed prior to the beginning of software implementation. The programming guidelines shall contain guidelines for

(i) Naming conventions for variables, program units

(ii) In line documentation, module headers

(iii) Programming dos and don'ts

(iv) Acceptable ranges for quality metrics (e.g. nesting depth, complexity etc)

(v) Use of programming language sub-set

(vi) Use of dynamic memory and recursion

(vii) Run time checks on variable values

(viii) Use of standard libraries.

For class IA systems, software programming guidelines shall conform to the recommendations of IEC 60880 [9].

A6.5 Deliverables

The following are the deliverables from this phase

(i) Software design

(ii) Software programmes (source code or runtime code emitted by code generators)

(iii) Programming guidelines.

(iv) Software test and integration plan

(v) Software test and integration results.

APPENDIX-7

SYSTEM INTEGRATION

A7.0 Introduction

The system integration phase is the final phase of the development life cycle. The inputs to this phase are the set of assembled and tested hardware subsystems and the independently developed and tested software programmes corresponding to each sub-system. This process includes progressive integration of software components with hardware components, defined in the system architectural design, to progressively build a complete system and to conduct tests at every stage of integration to ensure that hardware and software function properly together.

The main inputs to this phase are system architecture design and system integration and test procedure.

A7.1 System Integration

The configuration management process (Appendix-1) should result in the preparation of a system build which will provide detailed information about each hardware and software component i.e. CI and this should be used as an input to the system integration process.

Likewise, the user manual should be compiled using the information available from previous design activities. The user manual will contain complete information to help the system users to efficiently train and safely use and maintain the system.

Each hardware sub-system built by integrating constituent hardware and tested vide Appendix-5 should be integrated with corresponding sub-system software and tested to confirm that it works properly and meets all functional and performance requirements assigned to it.

After all sub-systems have been independently integrated and tested these should be progressively integrated with each other and tested to assure that the complete system meets functional and performance requirements. This includes testing the system in all modes of operation, verification of user manual, verification of error responses, etc. The integrated system testing should be carried out using an environment as close as possible to the field environment in which the system would be deployed. The results of such testing should indicate with adequate confidence that the system meets the specifications.

The result of the complete system integration activity should be documented to generate the system integration and test report.

A7.2 Deliverables

The following are the deliverables from this phase

(i) System build

(ii) User manual

(iii) System integration and test report.

APPENDIX-8

SYSTEM SAFETY AND RELIABILITY ANALYSIS

A8.1 System Safety Analysis

System safety analysis includes the following:

A8.1.1 Confirmation of safety function implementation

The safety of computer based system hardware and software design shall be ensured through all development phases by ensuring traceability and correct implementation of safety requirements of the system. This shall be checked during V and V process as described Appendix-2.

A8.1.2 Failure analysis

(a) Analysis is required to establish that class IA and IB systems meet single failure requirements as per AERB/NPP-PHWR/SG/D-10 and AERB/NPP-PHWR/SG/D-20 respectively. Hence analysis shall be carried out of all single failures within computer based system to determine the effect of failures on system's immediate outputs with respect to class IA and class IB functions.

(b) If computer based system is part of the larger I and C system then the results of above failure analysis shall be used in failure analysis of overall I and C system to demonstrate fulfillment of single failure criteria as per AERB/NPP-PHWR/SG/D-10 and AERB/NPP-PHWR/SG/D-20 as applicable.

A8.1.3 Analysis for common cause failures (CCF)

Analysis of the potential for CCF shall be performed and documented at the level of the total C and I architecture including class IA and IB systems to demonstrate compliance to the criteria given in 3.2.3 (i). This should include:

(a) Identification of all potential CCF sources due to components (software or others) used within the C and I architecture

(b) Analysis of the possible effects of these CCFs with respect to each PIE.

(c) Confirmation that adequate diversity is provided to eliminate possibilities of CCFs or the requirement given in subsection 3.2.3 (e) has been complied with.

A8.2 Hardware Reliability Analysis

For class IA and class IB systems hardware reliability analysis shall be carried out to substantiate class IA and class IB functional reliability goals and MTTR values stated in system requirements (SR). This shall be documented in hardware reliability analysis report. The analysis report shall include details about component reliability data with its sources, reliability block diagrams/fault trees for class IA and class IB functions and method of reliability calculations.

A8.3 Deliverables

The following are the deliverables from this phase

(i) System safety analysis consisting of confirmation of safety function implementation, failure analysis, CCF analysis

(ii) Hardware reliability analysis.

REFERENCES

1. ATOMIC ENERGY REGULATORY BOARD: Safety Classification and Seismic Categorisation of Structures, Systems and Components of Pressurised Heavy Water Reactors, AERB Safety Guide No.AERB/NPP-PHWR/SG/D-1, Mumbai, India (2002).

2. ATOMIC ENERGY REGULATORY BOARD: Protection against Internally Generated Missiles and Associated Environmental Conditions in Pressurised Heavy Water Reactors, Draft AERB Safety Guide No.AERB/SG/D-3, Mumbai, India (2008).

3. ATOMIC ENERGY REGULATORY BOARD: Safety Critical Systems of Pressurised Heavy Water Reactors, AERB Safety Guide No.AERB/NPP-PHWR/SG/D-10, Mumbai, India (2002).

4. ATOMIC ENERGY REGULATORY BOARD: Safety Related Instrumentation and Control for Pressurised Heavy Water Reactors, AERB Safety Guide No.AERB/NPP-PHWR/SG/D-20, Mumbai, India (2002).

5. ATOMIC ENERGY REGULATORY BOARD: Seismic Qualification of Structures, Systems and Components of Pressurised Heavy Water Reactors, Draft AERB Safety Guide No.AERB/NPP-PHWR/SG/D-23, Mumbai, India (2008).

6. ATOMIC ENERGY REGULATORY BOARD: Design of Pressurised Heavy Water Reactors; AERB Safety Code No. AERB/NPP-PHWR/SC/D (Rev. 1), Mumbai, India (2009).

7. ATOMIC ENERGY REGULATORY BOARD: Quality Assurance in Nuclear Power Plants; AERB Safety Code No. AERB/NPP/SC/QA, Rev.-1, Mumbai, India (2009).

8. ATOMIC ENERGY REGULATORY BOARD: Consenting Process for Nuclear Power Plants and Research Reactors, Draft AERB Safety Guide No. AERB/SG/G-1, Mumbai, India (2001).

9. IEC: Nuclear power plants - Instrumentation and Control Systems Important to Safety - Software Aspects for Computer based Systems Performing Category A function, IEC 60880 (2006).

10. IEC: Nuclear power plants - Instrumentation and Control Systems Important to Safety - Software Aspects for Computer based Systems Performing Category B or C functions, IEC 62138 (2004).

11. IEC: Programmed Digital Computers Important to Safety of Nuclear Power Stations, IEC60987 (1989).

BIBLIOGRAPHY

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

2. INTERNATIONAL ATOMIC ENERGY AGENCY: Safety Assessment and Verification for Nuclear Power Plants IAEA Safety Standards Series No. NS-G-1.2, IAEA Vienna (2001).

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

4. ATOMIC ENERGY CONTROL BOARD CANADA: Four Party Regulatory Consensus Report on Safety Case for Computer-based Systems in Nuclear Power Plants, AECB-Canada, DSIN/IPSN-France, NII-UK, USNRC-USA, November (1997).

5. Licensing of Safety Critical Software for Nuclear Reactors Common Position of Seven European Nuclear Regulators and Authorised Technical Support Organisations. AVN Belgium, BfS Germany, CSN Spain, ISTec Germany, NII United Kingdom, SKI Sweden, STUK Sweden. Rev. (2007).

6. UNITED STATES NUCLEAR REGULATORY COMMISSION: Standard Review Plan, NUREG0800, USA (2007).

7. UNITED STATES NUCLEAR REGULATORY COMMISSION: Criteria for Digital Computers in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.152, Revision 2, USA, January (2006).

8. UNITED STATES NUCLEAR REGULATORY COMMISSION: Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.168, Revision 1, USA (2004).

9. UNITED STATES NUCLEAR REGULATORY COMMISSION: Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.169, USA (1997).

10. UNITED STATES NUCLEAR REGULATORY COMMISSION: Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.170, USA (1997).

11. UNITED STATES NUCLEAR REGULATORY COMMISSION: Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.171, USA (1997).

12. UNITED STATES NUCLEAR REGULATORY COMMISSION: Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.172, USA (1997).

13. UNITED STATES NUCLEAR REGULATORY COMMISSION: Developing Software Lice Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.173, USA (1997).

14. INTERNATIONAL ELECTROTECHNICAL COMMISSION: Nuclear Power Plants - Instrumentation and Control Important to Safety - Classification of Instrumentation and Control Functions, IEC 61226, Geneva, Switzerland (2009).

15. INTERNATIONAL ELECTROTECHNICAL COMMISSION: Nuclear Power Plants - Instrumentation and Control for Systems Important to Safety - General Requirements for Systems, IEC 61513-2001, Geneva, Switzerland (2001).

16. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, IEEE Std 379, USA (2000).

17. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603, USA (1998).

18. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std. 7-4.3.2, USA (2003).

19. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software Quality Assurance Plans, IEEE Std 730, USA (2002).

20. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software Configuration Management Plans, IEEE Std 828, USA (1998).

21. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software Test Documentation, IEEE Std 829, USA (1998).

22. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Recommended Practice for Software Requirements Specifications, IEEE Std 830, USA (1998).

23. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard Dictionary of Measures to Produce Reliable Software, IEEE Std 982.1, USA (1998).

24. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software Unit Testing, IEEE Std 1008-1987(R1993), USA (1993).

25. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software Verification and Validation, IEEE Std 1012, USA (1998).

26. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Recommended Practice for Software Design Descriptions, IEEE Std 1016, USA (1998).

27. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software Reviews, IEEE Std 1028, USA (1997).

28. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Guide to Software Configuration Management, IEEE Std 1042, USA (1987).

29. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard Classification for Software Anomalies, IEEE Std 1044, USA (1993).

30. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software Project Management Plans, IEEE Std 1058, USA (1998).

31. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for a Software Quality Metrics Methodology, IEEE Std 1061, USA (1998).

32. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: Edition IEEE Recommended Practice for Software Acquisition, IEEE Std 1062, USA (1998).

33. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software User Documentation, IEEE Std 1063, USA (2001).

34. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERSIEEE Standard for Developing Software Life Cycle Processes: IEEE Std 1074, USA (1997).

35. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software Maintenance, IEEE Std 1219, USA (1998).

36. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Software Safety Plans, IEEE Std 1228, USA (1994).

37. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: Edition IEEE Guide for Developing System Requirements Specifications, IEEE Std 1233, USA (1998).

38. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Recommended Practice for Architectural Description of Software Intensive Systems, IEEE Std 1471, USA (2000).

39. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Information Technology-Software Life Cycle Processes-Reuse Processes, IEEE Std 1517, USA (1999).

40. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS IEEE Standard for Software Life Cycle Processes-Risk Management: IEEE Std 1540, USA (2001).

41. INTERNATIONAL ATOMIC ENERGY AGENCY: Software Important to Safety in Nuclear Power Plant, IAEA TRS-367, IAEA Vienna (1994).

42. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: Guide to the Software Engineering Body of Knowledge (SWEBOK) 2004 Version, A project of the IEEE Computer Society Professional Practices Committee, USA (2004).

LIST OF PARTICIPANTS

WORKING GROUP

Dates of meeting:

April 30, 1996
August 12 & 13, 1996
November 19, 1996
April 28 & 29, 1997
February 10 & 11, 1998
May 4, 1998
February 28, 2001
March 1, 2001
July 26, 2001
November 17, 2003
August 08, 2006
September 04, 2006
October 06, 2006
December 17, 2007
January 09 & 10, 2008
January 21, 2008
February 06, 2008
February 21, 2008
March 10, 2008
April 02, 2008
April 24, 2008
May 28, 2008
August 21, 2008
January 28, 2009
September 11, 2009
September 24, 2009
October 01, 2009
October 06, 2009
October 08, 2009
October 12, 2009
October 15, 2009
October 20, 2009
October 22, 2009
October 27, 2009
November 05, 2009
November 11, 2009
November 16, 2009
November 20, 2009
November 25, 2009
December 09, 2009
December 15 to 17, 2009
December 22, 23, 2009
January 04, 2010

Members and Invitees of the Re-constituted Working Group: [Since July 11, 2006]

Shri Umesh Chandra (Chairman)	:	NPCIL
Shri R.K. Patil (Co-Chairman)	:	BARC
Shri S.D. Dhodapkar	:	BARC
Shri. P. Swaminathan	:	IGCAR
Shri Rajiv Bhargava	:	NPCIL
Shri A.K. Chandra	:	NPCIL
Shri C.K. Pithawa	:	BARC
Shri R.M. Suresh Babu	:	BARC
Shri S.A. Khan (Member-Secretary)	:	AERB
Shri N.G. Asokan Pillai (Permanent-Invitee)	:	AERB
Shri S.K. Pradhan (Permanent-Invitee)	:	AERB
Shri G. Bharadwaj (Invitee)	:	BARC
Shri B.B. Biswas (Invitee)	:	BARC

LIST OF PARTICIPANTS (CONTD.)

WORKING GROUP

Shri M.P. Diwakar (Invitee)	:	BARC
Shri L.R. Jangra (Invitee)	:	BARC
Dr. Kallol Roy (Invitee)	:	BARC
Shri T. Narsing Rao (Invitee)	:	ECIL
Shri N. Murali (Invitee)	:	IGCAR
Shri K.K. Chandra (Invitee)	:	NPCIL
Shri S.P. Dharne (Invitee)	:	NPCIL
Smt. Agilandaeswari Karunakaran (Invitee)	:	NPCIL
Shri Ravi Prakash (Invitee)	:	NPCIL
Smt. Ajita Srivastava (Invitee)	:	NPCIL

Members of the Working Group: [Upto July 10, 2006]

Shri G. Govindarajan (Chairman)	:	BARC
Prof. R.K. Shyamasundar	:	TIFR
Dr. K. Karunakar	:	ADA
Shri D. Ranga Rao	:	ECIL
Shri P.C. Dixit	:	NPCIL
Shri Umesh Chandra	:	BARC
Shri S.D. Dhodapkar	:	BARC
Shri P. Swaminathan	:	IGCAR
Late Dr. R.N. Kulkarni (Member-Secretary)	:	AERB (Upto March 2001)
Shri S.A. Khan (Member-Secretary)	:	AERB
Shri E.R. Titto (Permanent Invitee)	:	AERB
Shri C.K. Pithwa (Invitee)	:	BARC
Shri Y.S. Mayya (Invitee)	:	BARC

ADVISORY COMMITTEE ON CODES, GUIDES AND ASSOCIATED MANUALS FOR SAFETY IN DESIGN OF NUCLEAR POWER PLANTS (ACCGD)

Dates of meeting	:	October 4, 1996 February 3, 1999 April 28, 1999 August 5, 2002 February 15, 2004 December 24, 2009

Members of ACCGD:

Shri S.B. Bhoje (Chairman)	:	IGCAR (upto December 2003)
Shri V.K. Mehra (Chairman)	:	BARC
Shri S. Damodaran	:	NPCIL (Formerly) (upto 07.12.2004)
Shri Umesh Chandra	:	NPCIL (upto 07.12.2004)
Shri S.A. Bhardwaj	:	NPCIL
Shri S.C. Chetal	:	IGCAR
Dr. S.K. Gupta	:	AERB
Shri K.K. Vaze	:	BARC
Prof. R.P. Vedula	:	IIT, Bombay (upto 07.12.2004)
Shri S.G. Ghadge	:	NPCIL
Shri B.B. Biswas	:	BARC
Shri P. Hajra	:	AERB (Formerly) (from Feb 2004 to 07.12.2004)
Shri S.A. Khan	:	AERB
Shri S.K. Dubey (Secretary)	:	AERB

ADVISORY COMMITTEE ON NUCLEAR SAFETY (ACNS)

Dates of meeting	:	June 12, 2006 December 29, 2009

Members of ACNS:

Shri G.R. Srinivasan (Chairman)	:	AERB (Former)
Shri S.C. Hiremath	:	HWB (Former)
Shri S.S. Bajaj	:	NPCIL (Former)
Shri D.S.C. Purushottam	:	BARC (Former)
Shri A.K. Anand	:	BARC (Former)
Shri H.S. Kushwaha	:	BARC
Shri R.K. Sinha	:	BARC
Prof. J.B. Doshi	:	IIT, Bombay
Shri S. Krishnamony	:	BARC (Former)
Dr. S.K. Gupta	:	AERB
Shri K. Srivasista (Member-Secretary)	:	AERB

PROVISIONAL LIST OF SAFETY CODES, GUIDES AND MANUALS ON DESIGN OF PRESSURISED HEAVY WATER REACTOR BASED NUCLEAR POWER PLANTS

S. No.	Safety Series No.	Titles
1.	AERB/SC/D	Code of Practice on Design for Safety in Pressurised Heavy Water Based Nuclear Power Plants
2.	AERB/NPP-PHWR/ SC/D (Rev.1)	Design of Pressurised Heavy Water Reactor Based Nuclear Power Plants
3	AERB/NPP-PHWR/ SG/D-1	Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors
4	AERB/SG/D-2	Structural Design of Irradiated Components of Pressurised Heavy Water Reactors
5	AERB/SG/D-3	Protection Against Internally Generated Missiles and Associated Environmental Conditions in Pressurised Heavy Water Reactors
6	AERB/SG/D-4	Fire Protection in Pressurised Heavy Water Reactor Based Nuclear Power Plants
7	AERB/SG/D-5	Design Basis Events for Pressurised Heavy Water Reactors
8	AERB/NPP-PHWR/ SG/D-6	Fuel Design for Pressurised Heavy Water Reactors
9	AERB/SG/D-7	Core Reactivity Control in Pressurised Heavy Water Reactors
10	AERB/NPP-PHWR/ SG/D-8	Primary Heat Transport System for Pressurised Heavy Water Reactors
11	AER/SG/D-9	Process Design
12	AERB/NPP-PHWR/ SG/D-10	Safety Systems for Pressurised Heavy Water Reactors
13	AERB/SG/D-11	Emergency Electric Power Supply Systems for Pressurised Heavy Water Reactors
14	AERB/NPP-PHWR/ SG/D-12	Radiation Protection Aspects in Design for Pressurised Heavy Water Reactor Based Nuclear Power Plants
15	AERB/SG/D-13	Liquid and Solid Radioactive Waste Management in Pressurised Heavy Water Reactor Based Nuclear Power Plants

PROVISIONAL LIST OF SAFETY CODES, GUIDES AND MANUALS ON DESIGN OF PRESSURISED HEAVY WATER REACTOR BASED NUCLEAR POWER PLANTS (CONTD.)

S. No.	Safety Series No.	Titles
16	AERB/SG/D-14	Control of Airborne Radioactive Materials in Pressurised Heavy Water Reactors
17	AERB/SG/D-15	Ultimate Heat Sink and Associated Systems in Pressurised Heavy Water Reactors
18	AERB/SG/D-16	Material Selection and Properties for Pressurised Heavy Water Reactors
19	AERB/SG/D-17	Design for In-Service Inspection of Pressurised Heavy Water Reactors
20	AERB/SG/D-18	Loss of Coolant Accident Analysis for Pressurised Heavy Water Reactors
21	AERB/SG/D-19	Deterministic Safety Analysis of Pressurised Heavy Water Reactor Based Nuclear Power Plants
22	AERB/NPP-PHWR/ SG/D-20	Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants
23	AERB/NPP-PHWR/ SG/D-21	Containment System Design for Pressurised Heavy Water Reactors
24	AERB/SG/D-22	Vapour Suppression System (Pool Type) for Pressurised Heavy Water Reactors
25	AERB/NPP-PHWR/ SG/D-23	Seismic Qualification of Structures, Systems and Components of Pressurised Heavy Water Reactors
26	AERB/SG/D-24	Design of Fuel Handling and Storage Systems for Pressurised Heavy Water Reactors
27	AERB/NPP-PHWR/ SG/D-25	Computer Based Safety Systems of Pressurised Heavy Water Reactors
28	AERB/NPP-PHWR/ SM/D-2	Hydrogen Release and Mitigation Measures under Accident Conditions in Pressurised Heavy Water Reactors
29	AERB/NPP-PHWR/ TD/D-1	Decay Heat Load Calculations in Pressurised Heavy Water Reactors

NOTES

AERB SAFETY GUIDE NO. AERB/NPP-PHWR/SG/D-25

Published by **:** Atomic Energy Regulatory Board
Niyamak Bhavan, Anushaktinagar
Mumbai - 400 094
INDIA.