ansto

Replacement Research Reactor Project

SAR – CHAPTER 8
INSTRUMENTATION AND CONTROL

Prepared By

INVAP

For

Australian Nuclear Science and Technology Organisation

1 November 2004

ANSTO		Document N°: **RRRP-7225-EBEAN-002-Rev0-CHAPTER-08** Revision: 0		
Replacement Reactor Project		Document Title: SAR – Chapter 8, Instrumentation and Control		
REVISION SHEET		Ref No:		
		Print name, date and sign or initial		
Revision	Description of Revision	Prepared	Checked/ Reviewed	Approved
0	Original Issue for public release	CM	KWH	GW
Notes: 1. Revision must be verified in accordance with the Quality Plan for the job.				

TABLE OF CONTENTS

End of Table of Contents

8 INSTRUMENTATION AND CONTROL

8.1 INTRODUCTION

8.1.1 Objectives and General Description

This chapter presents the design and performance information for the instrumentation and control aspects of the Replacement Research Reactor Facility (the Reactor Facility) safety and safety-related systems. Safety instrumentation and control systems are designated either as Safety Category 1, or 2, depending on their importance to safety. Some portions of a system may have a safety function, while other portions of the same system may be classified as non-safety related, (Safety Category 3). A description of the system classification can be found in Chapter 2.

The interaction of the main instrumentation and control systems with the Reactor Facility's operational staff and reactor systems is shown diagrammatically in the instrumentation and control context diagram of Figure 8.1/1.

The objectives for this chapter are:

a) To identify the specific safety requirements and safety design bases applicable to the instrumentation and control systems.

b) To provide a summary description of the design and operation of the instrumentation and control systems.

c) To identify the safety features of the instrumentation and control systems that contribute to nuclear and personnel safety.

d) To evaluate the design and operation of the instrumentation and control systems so as to demonstrate that they meet the identified safety requirements and safety design bases.

e) To identify faults that are subject to detailed safety analysis in Chapter 16.

Safety and safety related instrumentation and control systems consist of:

a) Reactor Protection Systems

   The Reactor Protection Systems (RPS) includes all electrical and mechanical devices and circuits for the First and Second Reactor Protection Systems, which generate signals associated with protective functions that are carried out by the safety actuation systems. The First Reactor Protection System (FRPS) actuates the First Shutdown System (FSS), Reactor Containment System (RCS), start-up interlocks and other process interlocks. The Second Reactor Protection System (SRPS) actuates the Second Shutdown System (SSS) and a process interlock. Both the FRPS and SRPS are Engineered Safety Features and Safety Category 1 Systems.

b) Post Accident Monitoring System

   The Post Accident Monitoring (PAM) System includes all electrical components required to monitor conditions of the facility during and after an accident. The PAM system is an Engineered Safety Feature and a Safety Category 1 system.

c) Reactor Control and Monitoring System

The Reactor Control and Monitoring System (RCMS) include all the components required for reactor process control and monitoring during normal operation and plant incidents. It is the main interface for plant operations through the Main Console (MC) in the Main Control Room (MCR), and is a Safety Category 2 system

d) Process Instrumentation and Controls associated with Safety Category 2 Systems

The Reactor Facility's Safety Category 2 systems' instrumentation consist of all the field mounted instruments and controls required to carry out the monitoring, control and protection actions required for the safe operation of the facility. The instrumentation associated with a Safety Category 2 system is, at a minimum, classified as Safety Category 2. Where instrumentation on a Safety Category 2 system performs a safety function related to the RPS or PAM, the instrumentation is classified as Safety Category 1.

e) Main Control Room and Emergency Control Centre

The MCR is the area where reactor and associated systems are normally controlled. The Emergency Control Centre (ECC) is an alternative control room for the purpose of maintaining the reactor in a safe shutdown state if the MCR is uninhabitable.

All operator interfaces with plant control and monitoring equipment have been designed taking into account operator interfaces, human factors, and ergonomics.

8.1.2 Identification of Instrumented Safety Class 1 Systems

8.1.2.1 Reactor Protection Systems

The Reactor Protection Systems (RPS) consists of two functionally independent and diverse protection systems that initiate, among other actions, automatic reactor shutdown. The First Reactor Protection System (FRPS) initiates the fast insertion of Control Rods (CRs), called a Trip 1 action, via the First Shutdown System (FSS) whenever FRPS monitored parameters exceed pre-established limits. The Second Reactor Protection System (SRPS) initiates the partial draining of heavy water from the reflector vessel, called a Trip 2 action, via the Second Shutdown System (SSS), whenever SRPS monitored parameters exceed pre-established limits. These actions are aimed at avoiding reactor fuel damage and preventing the release of radioactive material from the reactor pool. The FRPS also initiates actions to isolate the Reactor Containment in case of release of radioactive material, and incorporates a number of interlocks that prevent reactor start-up when certain systems are unavailable. Additionally the FRPS includes a number of process interlocks and also triggers some safety control actions by the Containment Energy Removal System (CERS). The SRPS includes a single process interlock. The FRPS and the SRPS are triple redundant systems, each consisting of three trains. Each train receives as inputs, measurements from channels that monitor various system parameters. Whenever a channel determines that one of its monitored parameters exceeds the safety limit setting, the associated bistable trip is in the tripped state. Whenever two out of three channels are in a tripped state, for the same parameter, the reactor is shutdown, or a protective action initiated.

The FRPS and SRPS input information to the RCMS via Class 1E qualified isolation devices.

Each individual safety system uses three channels of safety process instrumentation for the initiation of safety actions, one channel per train.

8.1.2.2 Post Accident Monitoring System

The Post Accident Monitoring (PAM) system provides the operators with reliable information about the relevant safety parameters to determine whether the protection systems have performed their safety functions satisfactorily.

The Post Accident Monitoring system provides indication that the reactor is shutdown, that safety functions are being carried out, and provides indication of the effectiveness of all Engineered Safety Features (ESF). In addition, the Post Accident Monitoring system indicates if the barriers to fission product release have the potential for being breached or have been breached. The parameters provide sufficient information to alert operators to take actions on systems that are not automatic. The Post Accident Monitoring system is a hard-wired system with information available in the MCR, and in the ECC.

8.1.2.3 First Shutdown System

The FSS is a reactor shutdown system, which carries out the fast insertion of control plates (identified in this document as control rods or CRs). The CRs are made of a neutron absorbing material that once inserted into the core shuts down the reactor by making it highly sub-critical.

8.1.2.4 Second Shutdown System

The SSS is a reactor shutdown system that partially drains the heavy water in the reflector vessel, leaving the core in a sub-critical condition. The removal of heavy water in the reflector vessel reduces the number of neutrons reflected towards the core, resulting in a highly sub-critical core.

8.1.2.5 Reactor Containment Systems

The Reactor Containment Systems are systems that isolate the containment when very high activity is detected in the reactor building stack, and ensure the containment is unaffected by over or under pressure conditions. These latter systems include the Containment Energy Removal System, the Containment Pressure Relief and Filtered Venting System and the Containment Vacuum Relief System.

8.1.2.6 The Emergency Control Centre Ventilation and Pressurisation System

The ECC Ventilation and Pressurisation System is an Engineered Safety Feature that ensures the continued habitability of the ECC in case evacuation of the Main Control Room is required.

8.1.2.7 Standby Power System

The Standby Power System provides electric power supply to loads important to safety when the Normal Power System is not available. The Standby Power System comprises diesel generator, switchboard and Uninterruptible Power Supply (UPS) systems.

8.1.3 Identification of Instrumented Safety Class 2 Systems

Some Safety Category 2 process systems include Safety Category 1 equipment or have Safety Category 1 instrumentation associated with them. Details regarding these issues are addressed in Sections 8.7 to 8.12 of the chapter.

8.1.3.1 Reactor Control and Monitoring System

The Reactor Control and Monitoring System (RCMS) is a Safety Category 2, computer-based, high availability system which monitors all plant and reactor parameters, displays them in the MCR, ECC, and at local supervision centres. The RCMS functions include control of the reactor operation, process control, and overall information management.

The RCMS also manages information from the following systems in addition to the reactor process systems:

Radiation Monitoring System

Vibration Monitoring System

Facilities Control and Monitoring System

Nucleonic Instrumentation System

8.1.3.2 Primary Cooling System

The Primary Cooling System (PCS) removes the heat produced by the fission of the fuel during full power operation of the reactor by forced upward circulation of light water through the core. The core is cooled by natural circulation when the reactor is in the Physics Test state. The core can be cooled by natural or forced circulation when the reactor is in the Shutdown state. Natural circulation is possible by the automatic opening of flap valves in the PCS that allow natural convection water flow through the core. As the flap valves open on cessation of forced flow, there are no RPS actions required to actuate this change.

8.1.3.3 Secondary Cooling System

The Secondary Cooling System (SCS) is responsible for the final transfer of the thermal energy produced in the reactor to the atmosphere, by means of the cooling towers. The SCS also supplies cooling water for the Cold Neutron Source (CNS) refrigeration and to the reactor building HVAC system.

8.1.3.4 Reflector Cooling and Purification System

The Reflector Cooling and Purification System (RC&PS) circulates the heavy water of the reflector vessel through a heat exchanger that transfers the heat to the de-mineralised water in the Intermediate Cooling System. The heat is then transferred to the SCS through a secondary heat exchanger.

8.1.3.5 Reactor and Service Pools Cooling System

The Reactor and Service Pools Cooling System (RSPCS) removes heat from the irradiation rigs during reactor power operation, and removes heat from the reactor pool during physics test operation, shutdown, and shutdown after abnormal conditions.

During power operation, the irradiation rigs are cooled by forced downward flow.

The RSPCS removes decay heat from rigs by means of natural circulation during normal reactor shutdown conditions and during shutdown after emergency conditions. This is possible by the passive opening of one or both flap valves in the RSPCS that allow natural convection water flow through the rigs. As the flap valves open on loss of forced flow, there are no RPS actions required to actuate this change.

The RSPCS also removes the decay heat from the spent fuel stored in the service pool.

8.1.3.6 Reactor Water Purification System

The function of the Reactor Coolant Purification System (RWPS) is to keep the reactor pool and service pool water within the specified water purity limits by eliminating corrosion products, fission products and impurities.

8.1.3.7 Hot Water Layer System

The Hot Water Layer System (HWLS) has been designed to provide protection to the operators from radiation emitted by active impurities in the reactor pool water. The system fulfils its function by maintaining a non-activated water layer on the reactor pool surface by means of purification and heating.

8.1.3.8 Emergency Make-up Water System

The Emergency Make-up Water System (EMWS) is capable of maintaining the core under water by injecting water into the two vertical legs of the PCS core inlet pipes inside the reactor pool. If, as a consequence of a beyond design basis accident, the reactor pool water level decreases to the level of the upper chimney edge, the system valves open and water will flow into the PCS pipes. The system is passive and does not require actuation from either the FRPS or SRPS. The instrumentation of this system monitors the availability of the system and the success of the protection function.

8.1.4 Identification of General Safety Criteria

The design bases and criteria for instrumentation and control equipment design are based on the need to have each system perform its intended function while meeting the requirements of applicable general design criteria, codes, standards, regulatory guides, and other requirements.

The design bases for safety systems define, in functional terms, the unique design requirements that establish the limits within which the safety objectives will be met. The general functional requirement section of the safety design bases presents those requirements which have been determined to be sufficient to ensure the adequacy and reliability of the system from a safety viewpoint.

8.1.4.1 Design Bases for Safety Systems

Safety systems provide the necessary actions to accomplish the following: ensure safe reactor shutdown, maintain cooling of the core in all postulated conditions, protect the integrity of radioactive material barriers, and prevent the uncontrolled release of activity and mitigate the consequences of accidents. These safety systems consist of components, groups of components, systems, or groups of systems.

8.1.4.2 Requirements from Standards

The following standards have been applied in total, or, where not totally applicable, in part (noting that some sections of some standards are not relevant to Research Reactors):

AS 1345, Identification of the contents of pipes, conduits and ducts.

AS 2220, Emergency warning and intercommunication systems in buildings.

AS 3000, SAA Wiring Rules (Australian Standard Criteria).

AS 3013, Classification of the Fire and Mechanical Performance of Wiring Systems.

AS 3666, Air handling and water systems of Buildings – Microbial Control.

IAEA Safety Series No. 35, Safety Requirements for Research Reactors (Draft, February 1999).

IEEE, Standards for Class 1E Power Systems for Nuclear Power Generating Stations, Generating Station Control Rooms and Other Peripheries.

NATO Military Specification.

Nuclear Safety Bureau 1998, draft working document RG-5, Criteria for the design of nuclear installations (December 1998).

Note: The ISO 8802 series are standards that are equivalent to (or supersede) the IEEE 802 series and where equivalent the numbering scheme is simply prefixed with the number “8”.

8.1.4.3 Technical Design Bases

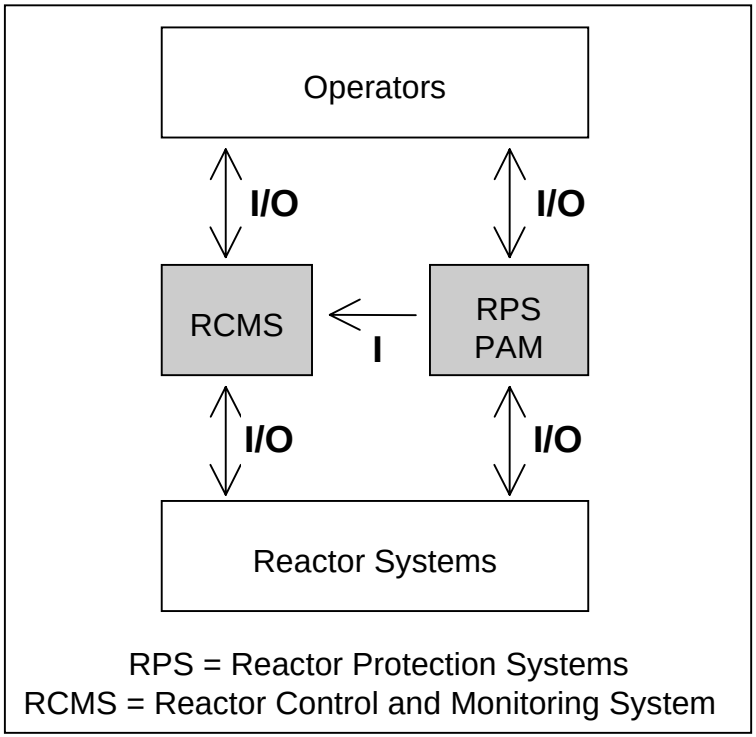
The technical design bases are included in each section.

8.1.4.4 Safety Category 1 Systems Testability

All instrumentation and control components are designed, arranged and located so that they can be adequately inspected, tested and serviced before commissioning and at suitable and regular intervals thereafter. During the conduct of periodic tests, the RPS, the PAM system, and other ESF will be able to accomplish their safety function. The test methods will optimise the time interval during which equipment is removed from service. The test program and the test frequency will not cause deterioration of any reactor component beyond that provided for in the design.

End of Section

Figure 8.1/1 Instrumentation and Control Context Diagram



End of Figures

8.2 REACTOR PROTECTION SYSTEMS

8.2.1 Introduction

The Reactor Protection Systems (RPS) comprise the instrumentation systems that initiate the actions that safely shutdown the reactor, and isolate the containment when radioactive discharges in the stack are above safety settings. The RPS also incorporates interlocks that prevent reactor start-up unless certain conditions are met, and other process interlocks. The RPS is separated into two different systems: the First Reactor Protection System (FRPS) and the Second Reactor Protection System (SRPS). These systems are classified as Safety Category 1.

8.2.2 Design Requirements

8.2.2.1 General Requirements

The RPS meets the following functional requirements:

1. To start protective actions in order to shutdown the reactor.
2. Initiate protective actions reliably to prevent or limit reactor fuel damage following abnormal operational transients.
3. To limit the uncontrolled release of radioactive materials by reliably initiating protective actions on detection of the release of fission products from the PCS.
4. Detect conditions that threaten the reactor, from process parameters that are direct measures of operational conditions.
5. Respond correctly to process parameters over the expected range and to the rates of change of those process parameters.
6. Reliably monitor essential parameters that have spatial dependence.

The following requirements assure the RPS reliability by means of redundancy, separation, diversity and equipment qualification:

7. Redundancy is provided, based on the potential for undetected failures that could degrade reliability.
8. Multiple sets of equipment that cannot be tested individually are not considered redundant.
9. Physical separation by distance, barriers or layout of reactor components are provided as appropriate, to enhance the reliability of systems, particularly with respect to common cause failures.
10. All use of diversity of equipment in redundant systems are identified and justified in the design documentation.
11. If a single random failure can cause an RCMS action that generates a plant condition requiring a protective action but also prevents action by some RPS channels, the remaining trains of the RPS will meet their functional requirements as described in items 1, 2 and 3 above.
12. Loss of one power supply train will not prevent operation of the RPS.
13. Once initiated, the RPS action is completed. Return to normal operation will require deliberate operator action.

14. There is sufficient electrical and physical separation between redundant instrumentation and control equipment, monitoring the same parameter, to prevent environmental factors, electrical transients, or physical events from impairing the ability of the system to respond correctly.
15. No single failure within the RPS will prevent the proper operation of the RPS when required to satisfy the safety design bases as described in items 1, 2, and 3 above.
16. Any single, maintenance operation, calibration operation, or test to verify operational availability will not prevent the ability of the RPS to respond correctly.
17. Two or more sensors for any monitored parameter exceeding the trip safety system setting will initiate automatic protective actions.

The following requirements reduce the probability of RPS operational reliability being degraded by operator error:

18. Control and monitoring functions will be provided in the MCR for reactor systems, auxiliary systems and all other process systems. The automation of all provided control systems will be optimised.
19. All instrumentation required to allow the safe shutdown of the reactor and maintain it in a safe state, including PAM instrumentation and Closed Circuit Television (CCTV) will be provided in the MCR and in the ECC.
20. Audible and visual alarms will be provided in the MCR, to alert operating personnel to any variations from the normal operating conditions during all modes of operation.
21. Sufficient MCR instrumentation will be provided for recording parameters related to the safe and efficient operation of the reactor facility.
22. UPSs will be provided for the parts of the instrumentation and control systems that are required to operate and maintain essential reactor facility equipment in the event of an interruption in the Normal Power System, following a design basis event. Each of the redundant instrumentation trains will be powered from independent UPSs.
23. Local instrumentation will be provided to monitor the performance of equipment, which requires regular maintenance.
24. Instrumentation and control systems will be designed to meet, as a minimum, the same operational requirements as the system, or equipment, they control. Instrumentation components of the RPS will comply with Safety Category 1 standards regardless of the safety category of the system to which it is connected.
25. The equipment will be selected to ensure that it causes no adverse vibration to other equipment, and is not adversely affected by vibration in its designated location.
26. The instrumentation throughout the reactor facility will be uniform to the extent possible (for standardisation) after taking into account the constraints imposed by the requirement of diversity.
27. Protection will be provided to minimise deterioration of all instrumentation, control systems, enclosures, and control wiring in their service environment.
28. Complete protection against in service environments will be provided. This includes radiation, dust, corrosive vapours and liquids, humidity, mould, corrosion, galvanic action, insulation and thermal cycling.
29. The equipment provided will be designed for an operating life of at least forty years, with the provision that all maintenance procedures will be performed at the proper time in a thorough and proper manner. Recommended surveillance and maintenance

regimes for all equipment will be supplied.

30. Access to trip settings, component calibration controls, test points, and other terminal points will be under the control of plant operations supervisory personnel.

31. Taking a train out of service for maintenance or modification will be under the supervision of the MCR operator. There are no bypasses allowed on the either the SRPS or FRPS. Any work performed on either will result in a train trip on that particular channel and will be continuously monitored by the MCR operator.

32. Selected automatic and manual reactor trip bypasses will be provided, as necessary, to permit particular modes of plant operation (for example physics test state).

33. Manual control switches for initiation of safety actions by plant operators will be provided where necessary.

The following requirements assure the verification, validation and testability of all equipment and components of the RPS (for a detailed list of verification and validation requirements see Tables 8.2/2 to 8.2/8):

34. Verification and validation processes are provided to ensure that the systems meet the functional, performance and reliability requirements.

35. Differing techniques have been employed during the verification and validation process according to the type of design and the stage of the design process.

36. Verification of all instrumentation and control systems is provided, at the component level and at the system level, with validation provided at the system level only. Verification has been applied from the beginning of system design in order to ensure maximum effectiveness. The amount of verification performed depends upon the importance of the system to plant safety or according to safety category classification.

37. All instrumentation and control components have been designed, arranged and suitably located such that they can be adequately inspected, tested, and serviced before commissioning and at regular intervals thereafter.

38. The RPS design ensures that, during in-service testing, those trains remaining in service will be able to accomplish any safety task, as required. The test method will minimise the time interval during which equipment is removed from service.

39. The test program and the test frequency will not cause deterioration of any reactor component beyond that provided for in the design.

40. Appropriate test facilities are provided. Procedures and instructions to carry out test operations, including in-service testing are included in the Operation and Maintenance Manuals.

41. A simple design and a structured development process, including requirement specifications, prototypes, simulations, reviews, and testing for all custom design components has been provided.

8.2.2.2 Requirements from Codes and Standards

Specific requirements from Codes and Standards are:

1. The RPS is classified as Safety Category 1 systems and complies with IEEE standards for Class 1E equipment.

2. Class 1E qualification is in accordance with IEEE and relevant Australian standards.

3. The definitions for independence and redundancy for Class 1E systems contained in IEEE has been applied to the Class 1E systems for the reactor facility.
4. Class 1E instrumentation and control wiring is separated in accordance with IEEE. Additionally control wiring conforms to the wiring requirements of AS 3000, RPS cabling conforms to the requirements of AS 1660.5 and the PAM cabling conforms to the fire requirements of AS 3013.
5. IEEE has been used in the design of all operator interfaces.
6. The equipment provided will not cause adverse electromagnetic interference to other equipment and will not adversely affected by electromagnetic emissions from other equipment, that is, it is compatible with other reactor facility equipment.
7. The FRPS has been designed based on the requirements in the IEEE standards for the application of computer systems in reactor safety systems, associated software Quality Assurance (QA).

8.2.2.3 Additional Requirements

1. The FRPS and SRPS automatically initiate the operation of appropriate systems to ensure that safety limits will not be exceeded during any abnormal plant condition or design basis accident. The systems will be diverse. There will be no common instrumentation components in the two systems.
   a) The FRPS consists of a combination of hard-wired and digital processing modules. The protective functions associated with this system are:
      (i) Protection Interlocks (Start-up + Process Interlocks)
      (ii) Trip 1 (FSS)
      (iii) Containment Isolation
      (iv) CERS Control
   b) The SRPS is based on hard wired technology only. The protective function associated with this system is the Trip 2 action (SSS) and one process interlock.
2. The RPS will initiate all automatic reactor shutdowns and will initiate ESF protective functions.
3. The RPS will protect against operational errors, if process parameters are outside predetermined limits.
4. The RPS will minimise the likelihood that operator actions could defeat the effectiveness of the system during all operational states, but does not negate correct operator actions during abnormal plant conditions.
5. The RPS has sufficient instrumentation for monitoring the operation of the reactor during power, physics test, shutdown, and refuelling states.
6. The RPS has sufficient recording instruments to monitor reactor parameters during and following operational occurrences and accident conditions.
7. The RPS will input all information to the RCMS via approved isolation devices. The use of isolation devices ensures that the RPS can not be affected by signals originating from the RCMS.
8. The RPS includes the following characteristics to ensure a reliable design:
   a) The systems function automatically and independently of other systems.
   b) Detection and actuation mechanisms shutdown the reactor in adequate time to protect the reactor from exceeding safety limits.

c) Following initiation of the trip systems, no manual operator intervention can prevent the trip completing its action

d) Shutdown signals are not generated using automatically reset devices. Once in the tripped state they will require deliberate operator action to be reset.

e) The systems' designs employ diversity to allow all postulated initiating events to be detected in a minimum of two different ways, where physically and technologically possible.

f) The systems comprise redundant trains that are independent and isolated from each other, to prevent a common cause failure.

g) The systems allow trip levels to be set with adjustable margins.

h) The systems have the capability to identify the parameter which initiated the first trip signal.

9. The RPS employs voting logic in the trip circuitry such that maintenance can be carried out on defective channels without the need for the reactor to be shut down. Channels taken out of service will be identified as "tripped", until back in service.

10. Audible and visible alarm systems are provided for early indication of any change that could lead to a reduction in safety while the reactor is operating or shut down.

8.2.2.4 Non Safety-Related Design Basis

1. The RPS is designed with consideration of plant availability. The safety settings, power supplies, and instrumentation and controls are arranged in such a manner as to preclude spurious actions as far as practical and safe.

2. The RPS triggers the required protective actions by request of some Safety Category 2 Systems

8.2.3 Reactor Protection Systems Description

The RPS consists of two independent systems, whose functions are to monitor all safety parameters and trigger protective actions when the trip safety settings are reached, and to initiate protective actions at the operator's request. The RPS is designed to bring the reactor to a safe condition in case of an anticipated operational occurrence or a Design Basis Accident (DBA).

To allow for physical separation and to ensure diversity, the RPS is two functionally independent systems (see Figure 8.2/1):

a) The FRPS consists of a combination of hard-wired and digital processing modules. The FRPS generates protection interlocks, the rapid insertion of CRs that is actuation of the FSS (Trip 1), the isolation of the containment, containment system interlocks and the Containment Energy Removal System safety control functions.

b) The SRPS is based on hard-wired technology. The SRPS generates a protection interlock and shuts down the reactor by the partial draining of the reflector vessel, SSS (Trip 2).

8.2.3.1 Reactor Protection Systems Parameters

The safety parameters monitored by the RPS can be grouped according to their function. Different components (e.g. sensors), measurement principles and methods are employed according to the process parameter monitored. All instrumentation connected to the RPS is qualified to Safety Category 1 requirements.

The RPS monitors parameters from the following systems:

Shutdown systems

Cooling systems

Nucleonic Instrumentation

Seismic System

Reactor Control and Monitoring System

Reactor Containment System

Radiation Monitoring System

Normal Power System

Facilities protection systems

Table 8.2/1 provides a list of these parameters.

Each parameter can trigger Trip 1, Trip 2 or other protective actions by reaching its trip condition (for example high or low level). Details of the RPS logic are provided in section 8.2.3.4.1 and 8.2.3.4.2

8.2.3.1.1 Shutdown Systems

The RPS monitors parameters from the FSS and the SSS.

FSS compressed air storage tank pressure is measured from a pressure switch located in the tank. There is one tank for all five CRs. This signal is used to prevent reactor start-up in case of low pressure.

The open position of the SSS isolation valve is monitored by a limit switch. If this switch is not actuated then the valve is not fully open. This signal is used to prevent reactor start-up.

The position of the CRs is monitored by limit switches located in the shock absorbers of each CR. They indicate that the CRs are in the down position. These indicators are used to determine the correct actuation of the FSS.

8.2.3.1.2 Cooling System Channels

The thermal-hydraulic variables of the RPS are measured in the following systems:

a) Primary Cooling System
b) Reflector Cooling and Purification System
c) Reactor and Service Pools Cooling System

The list of the parameters and the corresponding instrumentation is provided in the following sections.

8.2.3.1.2.1 Primary Cooling System

The RPS parameters measured in the PCS are:

a) core inlet temperature
b) core outlet temperature
c) core temperature difference
d) core pressure difference
e) primary coolant flow
f) pool water level

The core inlet and outlet temperatures are determined from three measurement channels in each position. Core inlet temperature and core temperature difference are parameters of the FRPS while core outlet temperature is a parameter of the SRPS.

The core pressure difference measurement corresponds to the pressure difference between the reactor core inlet and outlet. There are two sets of three differential pressure transmitters; three channels for the FRPS and three channels for the SRPS.

Primary coolant flow measurement is performed by FRPS flow differential pressure transmitters measuring flow in the return pipeline outside the reactor pool.

The pool water level is monitored by two sets of level switches connected to the RPS.

8.2.3.1.2.2 Reflector Cooling and Purification System

The RPS parameters coming from the Reflector Cooling and Purification System are:

a) reflector vessel temperature
b) reflector cooling flow
c) expansion tank very low level

The reflector vessel temperature is measured using three RTDs located inside the reflector vessel. These provide the MCR indication of heavy water temperature and trigger an alarm in the event of high temperature. The signal is input to the SRPS. This also provides a diverse means of tripping the reactor in the event of a loss of heat sink.

The reflector cooling flow measurement is performed with a venturi tube and three differential pressure transmitters located downstream of the heat exchanger. The transmitters provide local and remote indication of heavy water flow rate and trigger an alarm in the event of low flow. The flow signal is an input to the FRPS and triggers a Trip 1 action on low flow.

Three level switches trigger an alarm signal at the MCR and a Trip 1 action in the event of a very low level in the expansion tank.

8.2.3.1.2.3 Emergency Make-Up Water System

The Emergency Make-up Water System is a passive system with no control requirements. Some instrumentation monitors this system associated with Post Accident Monitoring. Refer to the Post Accident Monitoring System section for more information.

8.2.3.1.2.4 Reactor and Service Pools Cooling System

Venturi flow meters located on the rigs cooling branch, within the decay tank room, monitor the rigs cooling flow rate. The flow meters provide local and remote indication.

Three position switches on the flap valves are used to indicate in the MCR that the valves are closed during PCS operation in Forced Circulation Mode.

The signals combine to initiate a Trip 1 action under certain conditions.

8.2.3.1.3 Nucleonic Instrumentation

Nucleonic Instrumentation consists of neutron flux detection systems and a gamma detection system. Neutron flux measurement instrumentation supplies information on physical parameters to the RPS and PAM system, describing the state of the reactor regarding neutron flux and rate. The neutron flux measurement systems consist of measuring channels based on fission chambers, wide range fission chambers and compensated ionisation chambers which are able to monitor neutron flux for the whole operational range of the reactor. There is an overlap between the channels, as well as an adequate margin that is able to measure flux above the full power level for the unlikely event of a power excursion.

Nucleonic Instrumentation comprises:

- Start-up Nucleonic Instrumentation System
    1. Start-up Channel 1
    2. Start-up Channel 2
    3. Start-up Channel 3
- Wide Range Log Nucleonic Instrumentation System
    1. Wide Range Log Channel 1
    2. Wide Range Log Channel 2
    3. Wide Range Log Channel 3
- Power Range Nucleonic Instrumentation System
    1. Power Channel 1
    2. Power Channel 2
    3. Power Channel 3
- Wide Auto-range Linear Nucleonic Instrumentation System
    1. Wide Auto-range Linear Channel
- Linear Nucleonic Instrumentation System
    1. Linear Channel

The Wide Auto-Range Linear and the Linear Nucleonic Instrumentation Systems are connected to the RCMS only, and are discussed in Section 8.7 of this chapter.

The RPS includes Nucleonic Instrumentation systems to cover the neutron flux over the whole range of operation of the reactor, spanning from source level to 125% of full power level. The systems are:

a) First Reactor Protection System

    (i) Start-up Nucleonic Instrumentation System
    (ii) Wide Range Log Nucleonic Instrumentation System

b) Second Reactor Protection System

    (i) Power Range Nucleonic Instrumentation System

In order to comply with safety and reliability requirements, the Start-up and Wide Range Log Nucleonic Instrumentation Systems (FRPS) and the Power Range Nucleonic Instrumentation System, (SRPS) are triple redundant, consisting of three channels which are independent from the detector to the electronic measuring modules. Additionally the SRPS and FRPS trains, to which these channels are connected, are diverse and share no instrumentation in common.

8.2.3.1.3.1 Start-up Instrumentation System

The Start-up Nucleonic Instrumentation System is used to monitor the core neutron flux from the earliest stages of reactor operation (neutron source level), up to 5 measurement decades above source level. The Start-up Nucleonic Instrumentation System is part of the FRPS with one channel connected to each of the FRPS trains.

A test module is provided for all channels. These simulate fission chamber signals. Testing capabilities include the ability to input predefined fixed and rate signals to calibrate the channels.

8.2.3.1.3.2 Wide Range Log Nucleonic Instrumentation System

The Wide Range Log Nucleonic Instrumentation System is used to monitor the core neutron flux over more than 10 decades combining the outputs of two separate pulse and Campbell processing modules that are connected to wide range fission chambers.

Test modules are provided for all channels. They consist of current and pulse signal simulators. Testing capabilities include the input of predefined fixed and rate, frequency signals to calibrate the channels.

8.2.3.1.3.3 Power Range Nucleonic Instrumentation System

The Power Range Nucleonic Instrumentation System is used to monitor the core neutron flux over more than 6 decades to cover the power operation range of the reactor. The Power Range Nucleonic Instrumentation System measures the reactor neutron flux from 5 decades below full power to 125% of full power level and its outputs are fed into the SRPS.

Test systems are provided for all channels. They consist of current signal simulators. Testing capabilities include the input of predefined fixed and variable, that is rate frequency signals to calibrate the channels.

8.2.3.1.4 Seismic System

Two sets of three seismic monitoring systems are provided, one for the FRPS and the other for the SRPS. The seismic system is designed to the same level of performance as the RPS. The testing of the system is to the same standard as the RPS.

8.2.3.1.5 Reactor Control and Monitoring System

The RCMS is continuously running self-check routines that will indicate a failure of the system. The RCMS sends a pulse signal to the FRPS. If the signal is disrupted, the FRPS initiates a reactor trip.

8.2.3.1.6 Reactor Containment Systems

The Reactor Containment Systems (RCS) include:

a) Containment Isolation

   The function of the Containment is to isolate the containment area when a high level of radioactivity is detected in the reactor stack. The system responds to the Particulate, Iodine and Gas monitors of the Radiation Monitoring System. On detection of a very high activity level or activity rate, the FRPS triggers the closure of containment isolation valves.

b) Containment Pressure Relief and Filtered Vent System (CPRFVS)

The function of the CPRFVS is to relieve containment of over pressure by the opening of at least one of the two relief valves, allowing air to flow through active and charcoal filters to the stack. This is a passive system of pressure relief.

The system also has the capability to allow the control of air flow through the filters and into the stack via two valves. One valve is located inside the containment, the other outside. This is called the Filtered Vent System.

Under normal reactor operation, the system is armed by having the inner valve open and the outer valve and pressure relief valves closed.

The Containment Vacuum Relief system (CVRS) has no safety parameters associated with it, and is mentioned here for completeness only.

c) Containment Energy Removal System (CERS)

The CERS is responsible for the control of pressure inside containment in both normal and isolated conditions. It acts as a heat sink for all thermal loads inside the containment.

The systems are described in Chapter 7.

8.2.3.1.7 Radiation Monitoring System

The radiation protection instrumentation connected to the RPS can be divided into two different areas:

a) Reactor Pool Area
b) Stack Monitoring

8.2.3.1.7.1 Reactor Pool Area

The only area radiation parameter used in the RPS is the Reactor Pool Open End Gamma Activity, which consists of three gamma monitors situated around the top of reactor pool.

8.2.3.1.7.2 Stack Monitoring

The RPS parameters coming from the three Radiation Monitoring System stack monitors are:

a) stack particulate activity (3 monitors)

b) stack iodine activity (3 monitors)

c) stack noble gases activity (3 monitors)

The stack monitors are considered part of the FRPS and RCS, (see 8.2.3.1.6). The rates of change of these parameters are also safety variables with associated safety settings.
There is a fourth independent stack monitor for Particulate, Iodine and Gas monitoring which incorporates a Multi Channel Analyser to determine which isotopes are being released. It is not connected to the RPS. In this monitor, aerosol and inert gas channels have additional plastic scintillators in front of the filters (or the gas volume) to detect beta emissions from these isotopes.

8.2.3.1.8 Normal Power System

A reactor trip is initiated on loss of normal power supply.

8.2.3.1.9 Facilities Systems

8.2.3.1.9.1 Cold Neutron Source Protection System (CNSPS)

A system for the protection of the CNS is provided which generates, among other protective actions, a reactor trip request signal to the FRPS. The requirements for Safety Category 1 instrumentation apply only to the input signal to the FRPS, whereas the rest of the Cold Neutron Source Protection System (CNSPS) is classified as Safety Category 2. The CNSPS instrumentation is independent of the FCMS and inputs into the RPS via appropriate isolation devices. In order to facilitate changeover in case of failure, the system is provided with redundant sensors at the same location where instrumentation sensors cannot be replaced or serviced in a normal routine shutdown.

8.2.3.2 First Reactor Protection System Architecture

The FRPS is a triple redundant system consisting of three independent, redundant trains named Train 1, Train 2 and Train 3. Each parameter connected to the FRPS is provided with triplicate measurement channels named Channel 1, Channel 2 and Channel 3. All FRPS channels are completely independent.

Each of the three redundant measurement channels (from the field sensors) is connected to a corresponding train.

Each train sends its connected channel (Channel 1 for Train 1 etc) via fibre optics, to the other two trains. Therefore, the FRPS incorporates the three channels of all the field inputs into each of the three trains prior to voting.

Not only is the FRPS a triple redundant system comprising three trains of equipment, each train is provided with triple redundant voting and protective logic hardware to further increase system reliability and availability.

8.2.3.2.1 Conditioning Stage

The conditioning stage carries out the following actions:

a) signal amplification

b) signal conversion

c) signal processing

8.2.3.2.2 Trip Generation

The Trip Set Point Input Unit (TSIU) is a peripheral device (laptop PC) used to configure the trip set points. Modification of trip set points is done while the channels are in operation but the related train is tripped.

8.2.3.2.2.1 Interlock Generation

The safety systems require certain operational conditions to be satisfied to enable normal plant operation. Protection interlocks are specified and implemented to prevent erroneous changes in these operational conditions or configurations.

There are two main groups of protection interlocks:

a) interlocks related to the availability of the safety systems

b) configuration changes of the measurement channels

These safety interlocks must be met during different operational states of the reactor.

The FRPS evaluates the interlock conditions in the same way as the trip conditions described above.

8.2.3.3 Second Reactor Protection System Architecture

The SRPS architecture is based on hardwired technology.

The SRPS monitored parameters can be grouped according to:

a) Nucleonic

b) Thermal-hydraulics

c) Seismic

8.2.3.3.1 Signal Conditioners

The signal conditioners are sensor specific items which may be an integral part of a sensor or a separate field mounted transmitter. They perform any or all of the following functions:

a) signal amplification

b) signal conversion

c) signal processing

They deliver a final analogue or digital value, within prescribed ranges, to the input modules. The types of sensors interfaced by the signal conditioners cover nucleonic instruments, radiation protection monitors and process instrumentation.

8.2.3.4 Reactor Protection Systems Functional Overview

8.2.3.4.1 First Reactor Protection System Logic

The FRPS triggers Trip 1 when selected parameters from the various process systems exceed their prescribed safety settings.

8.2.3.4.1.1 First Shutdown System Logic

The following interlock is provided for protection of the FSS:

1. Compressed Air Storage Tank Pressure

   This signal monitors pressure in the air storage tank of the FSS. This signal inhibits reactor start-up when pressure falls below the set value. Once the reactor is in operation, this interlock is inhibited.

   Only one FRPS alarm signal is generated when a low pressure is produced during reactor operation.

8.2.3.4.1.2 Second Shutdown System Logic

The following interlock is provided for protection of the SSS:

1. Isolation Valve Locked

   This digital parameter is acquired at the heavy water evacuation pipe near the reflector vessel, and located before the six valves. Reactor start up is inhibited if the valve is not fully open.

8.2.3.4.1.3 Primary Cooling System Logic

The PCS logic triggers Trip 1 action by input of the following signals:

1. Primary Coolant Flow

   These analogue parameters are acquired in the piping of the PCS that connects the heat exchanger with the reactor pool. They measure the flow of coolant returning to the reactor core and trigger a Trip 1 on low flow when the RPS is in the Power Configuration. Operation of the reactor in the Physics Test state does not require the main primary cooling pumps to be in operation and thus this trip is inhibited in the this state.

2. Core Pressure Difference

   These analogue parameters are acquired in the reactor pool up and down stream of the reactor core. They trigger a Trip 1 on high and low pressure difference when the RPS is in the Power Configuration.

   The Trip 1 initiated by the Core Pressure Difference Low parameter is disabled when the RPS is in the Physics Test Configuration. Operation of the reactor in the Physics Test State does not require the main primary cooling pumps to be in operation.

3. Core Temperature Difference

   These calculated parameters are based on the measured core coolant outlet and inlet temperatures. They trigger a Trip 1 on high Core Temperature Difference when the RPS is in the Power Configuration. In Physics Test there is no PCS flow required so the temperature differential is accurately measured.

4. Core Inlet Temperature

   These analogue parameters are sensed in the pipeline of the PCS that connects the heat exchanger with the reactor pool and measure the temperature of the coolant flowing into the core. They trigger a Trip 1 on high temperature when the RPS is in the Power or Physics Test Configurations.

8.2.3.4.1.4 Reflector Cooling and Purification System Logic

The Reflector Vessel Cooling System logic triggers Trip 1 action by the input of the following parameters:

1. Reflector Primary Cooling Flow

   These analogue parameters are acquired in the heavy water pipe at the entry to the reflector vessel. They trigger a Trip 1 on low flow when the RPS is in the Power or Physics Test Configurations.

2. Expansion Tank Level

   These digital parameters are acquired in the expansion tank of the reflector primary cooling circuit and measure the tank liquid level. They trigger a Trip 1 on low level when the RPS is in the Power or Physics Test Configurations.

8.2.3.4.1.5 Emergency Makeup Water System Logic

This system is completely passive and no RPS action is required to activate the system.

8.2.3.4.1.6 Reactor and Service Pools Cooling System Logic

The Reactor and Service Pools Cooling System logic triggers a Trip 1 action by input of the following parameters:

1. Reactor and Service Pools Cooling Flow

   These analogue parameters are acquired in the RSPCS piping between the heat exchanger and the reactor pool and measure the cooling water circulation flow into the reactor pool. They trigger a Trip 1 by low flow when the RPS is in the Power Configuration. They also trigger a Trip 1 by high flow when the RPS is in the Physics Test Configuration if both Flap Valves are closed.

2. Flap Valves Position

   These digital parameters sense the closed state of the flap valves located in the rigs cooling pipe. These indicate forced circulation cooling in the closed position and natural circulation cooling when not in the closed position. These valves open by the action of gravity when flow is removed from the rigs cooling pipe.

   a) If the RPS is in the Physics Test Configuration and the rigs cooling flow is low, a Trip 1 will occur if both valves are closed.

   b) If the RPS is in the Physics Test Configuration and the rigs cooling flow is high, a Trip 1 will occur if at least one valve is not closed.

   c) If the RPS is in the Power Configuration a Trip 1 will occur if at least one valve is not closed.

8.2.3.4.1.7 Nucleonic Instrumentation Logic

The Nucleonic Instrumentation logic triggers Trip 1 by the input of the following parameters:

1. Start-up Neutron Flux

   Start-up neutron flux is an analogue parameter acquired from the Start-up Instrumentation System. It triggers a Trip 1 when the neutron flux is lower or higher than pre-set values when the RPS is in the Power or Physics Test Configurations and the Wide Range Log Nucleonic Channels are not in range. Once the Wide Range Log Nucleonic Channels are in range, the Start Up Channels trips are disabled. This allows the reactor to increase power without producing any spurious Trip 1 actions due to signals coming from the Start-up Instrumentation System. Fission counters are moved out of the high flux region when they reach their maximum range.

2. Wide Range Log Flux Rate

   This analogue parameter is acquired from the Wide Range Log Nucleonic System. It produces a Trip 1 action if the rate of change of neutron flux is higher than a pre-set value when the RPS is in the Power or Physics Test Configurations. The rate trip is enabled when the Wide Range Log Channels reach a set value at which point the readings become stable.

3. Wide Range Log Flux – Power Configuration

   This analogue parameter is acquired from the Wide Range Log Instrumentation System in the intermediate and full power ranges using fission chambers. It produces a Trip 1 if the neutron flux level exceeds a pre-set value when the RPS is in the Power Configuration.

4. Wide Range Log Flux – Physics Test Configuration

   This analogue parameter is acquired from the Wide Range Log Instrumentation System in the intermediate power range using fission chambers. It produces a Trip 1 if the neutron flux level exceeds a pre-set value when the RPS is in the Physics Test Configuration.

The following interlocks are provided by the Nucleonic Instrumentation systems:

1. Start-up Range Interlock

   An interlock is generated to prevent raising the CRs if the neutron flux rate reading on the Start-up Instrumentation System is high.

2. Intermediate and Power Range Interlocks

   An interlock is provided to disable the Start-Up Instrumentation System high and low Trip 1 actions when the Wide Range Log Instrumentation System is on scale. To allow for the removal of the Start-Up Instrumentation System fission chambers, the low Trip 1 action must be inhibited. This signal is call Wide Range Log Neutron Flux in Range.

   An interlock is provided to enable the Wide Range Log Instrumentation System flux rate trip. This signal is called Wide Range Log Neutron Flux Fluctuation Range.

8.2.3.4.1.8 Seismic System Logic

These digital parameters trigger a Trip 1 on high level when the RPS is in the Power or Physics Test Configuration.

8.2.3.4.1.9 Reactor Control and Monitoring System Logic

On loss of the RCMS such that normal plant operation is affected, a Trip 1 action is initiated. The FRPS monitors the “healthy” signal from the RCMS and when the signal is no longer transmitted, the FRPS requests a reactor trip. Thus the trip does not rely on an active signal from the RCMS.

8.2.3.4.1.10 Reactor Containment System Logic

The following interlocks and controls are provided for the following Reactor Containment Systems:

1. Containment Isolation - Stack Particulate, Iodine and Gas Activity

   These signals are acquired by detectors located in the stack. Very high activity in the stack performs the Containment Isolation and closes the containment Group 1 valves when the RPS is in the Power, or Physics Test Configurations. This is determined by activity in at least two channels. The rate of change of these variables also performs the Containment Isolation when the RPS is in the Power or Physics Test Configurations. The FRPS also allows manual control of Containment Groups 1, 2 and 4 valves, and provides the corresponding reset commands for them.

2. Containment Energy Removal System

   On failure of the RCMS to control the CERS, the FRPS switches the system to a mode of maximum heat removal where heat is removed from the Containment at the full capacity of the system.

   Variables monitored by the RPS in order to take actions are:

   a) Air Cooling Circuit Temperature High

This is a digital signal derived from an analogue input of Air Temperature in the Containment and a corresponding software bistable trip. The signal toggles between Train 1 and Train 2.

b) Air Return CHILLER Circuit Temperature.

This is a digital signal derived from an analogue input of the Air Return Circuit Temperature detector and a corresponding software bistable trip. If Cooling Circuit Temperature is high, the air re-circulation heaters are powered off.

c) CHILLER Air Pressure.

This is a digital input derived from the Air Pressure Containment detector. The signal is used to toggle between Train 1 and Train 2.

d) Select Train 1.

This is a digital signal derived from the pushbutton "Select Unit 1" signal on the MSC and ESC. A light indicator indicates that Train 1 is selected.

e) Select Train 2.

This is a digital signal derived from the pushbutton "Select Unit 2" signal on the MSC and ESC. A light indicator indicates that Train 2 is selected.

Other signals include: Enable CERS, Disable CERS, Heater Reset and Transfer Enable. This system is further described in Chapter 7.

8.2.3.4.1.11 Radiation Monitoring System Logic

1. Reactor Pool Open End Gamma Activity

   These analogue parameters are acquired at the surface of the reactor pool and measure gamma activity in this area. They trigger a Trip 1 by high level when the RPS is in the Power or Physics Test Configurations.

2. Pool Water Level

   These digital parameters are acquired within the hot water layer in the reactor pool. A low level triggers Trip 1 when the RPS is in the Power or Physics Test configurations and is also an indication that the radiation protection offered by the hot water layer is degraded.

8.2.3.4.1.12 Normal Power System Logic

Although the FSS is designed to be fail-safe, the FRPS provides a trip signal on loss of normal power supply. This ensures that the FSS is actuated with the assistance of compressed air and that the SRPS is armed in the case of FSS failure.

8.2.3.4.1.13 Facilities Logic

Trip 1 actions are provided from the following systems:

1. Cold Neutron Source
2. Hot Neutron Source (reserved for future use)

8.2.3.4.1.14 FFAL Request

There are a number of signals that are direct inputs to the FFAL. When these signals cause a reactor Trip 1 the FFAL Request signal is true and is indicated on the safety wall panels in the MCR and ECC. When a trip is requested in the FFAL, a signal is sent to the corresponding train of the TRICON to ensure that the PLC is also tripped. The FFAL Request signal is generated by:

1. MSC Trip 1 pushbutton
2. ESC Trip 1 pushbutton
3. Pool Area Trip 1 pushbutton
4. Start-up and Wide Range Log Nucleonic Channels
5. SFAL

8.2.3.4.1.15 Safety Operation Signals

8.2.3.4.1.15.1 FRPS System Assembly Enable

This signal provided through a pushbutton on the MSC enables the assembly of the First Shutdown System by the RCMS.

The assembly of First Shutdown System is possible only if reactor operation is in the Disabled Configuration.

8.2.3.4.1.15.2 Reset Trip 1

This manual command is provided by a pushbutton on the MSC, and resets the FRPS.

8.2.3.4.1.15.3 Reactor Operation Enabled/Disabled

This command allows selecting the configuration of the RPS. The Disabled Configuration ensures the de-energisation of the electromagnets. The Enabled Configuration allows the energisation of the electromagnets provided the FRPS and RCMS start-up interlocks are satisfied. The changeover selector is a keyed switch on the MSC.

8.2.3.4.1.15.4 Physics Test

This command provided through a pushbutton on the MSC enables the RPS Physics Test Configuration.

8.2.3.4.1.15.5 Power

This command provided through a pushbutton on the MSC enables the RPS Power Configuration.

8.2.3.4.2 Second Reactor Protection System Logic

The SRPS triggers the SSS using a Trip 2 when selected parameters exceed their safety settings.

8.2.3.4.2.1 First Shutdown System

1. Failure of the FSS

The signal that determines the failure of the FSS is generated from the combination of the FRPS trip signal, the CRs down position signals from the five CRs and time.

8.2.3.4.2.2 Second Shutdown System

1. Heavy Water Makeup Pumps Interlock

   This signal is generated from the MCR console and allows the operation of the Heavy Water Makeup Pumps.

   In addition in the Shutdown State, the pumps are disabled if one or more CRs are not in the down position.

8.2.3.4.2.3 Primary Cooling System

1. Core Pressure Difference

   This analogue parameter is acquired in the reactor pool, up and downstream of the reactor core. It triggers a Trip 2 on low pressure on the condition that 2 out of 5 CRs fail to reach the down position when required. This prevents the Trip 2 actuation if the FSS has operated successfully.

2. Core Outlet Temperature

   This analogue signal is derived from the core outlet temperature detectors. A high level triggers a Trip 2 when the RPS is in the Power or Physics Test Configurations.

8.2.3.4.2.4 Reflector Cooling and Purification System

1. Reflector Vessel Temperature

   This analogue parameter is acquired from the reflector vessel. This parameter triggers a Trip 2 on high reflector D_20 temperature when the RPS is in the Power or Physics Test Configurations.

8.2.3.4.2.5 Nucleonic Instrumentation

1. Power Range Nucleonic Instrumentation System Neutron Flux

   This analogue parameter is acquired from the Power Range Nucleonic Instrumentation System using compensated ion chambers. The linear outputs of the channels produce a Trip 2 if the neutron flux level exceeds a pre-set value when the RPS is in the Power or Physics Test Configurations. The Trip 2 associated with the RPS Physics Test Configuration uses the Log output of the Power Instrumentation System.

2. Power Range Nucleonic Instrumentation System Flux Rate

   This analogue parameter is derived from the Power Range Nucleonic Instrumentation System. It produces a Trip 2 action if the neutron flux rate level exceeds a pre-set value when the RPS is in the Power or Physics Test Configurations.

8.2.3.4.2.6 Seismic System Logic

This digital parameter triggers a Trip 2 action by high level when the RPS is in the Power or Physics Test Configurations.

8.2.3.4.2.7 Pool Water Level Logic

These digital parameters are acquired below the hot water layer in the reactor pool. A low level triggers Trip 2 when the RPS is in the Power, or Physics Test Configurations, and is indication of a loss of coolant from the reactor pool. This signal also initiates the Reactor Hall Evacuation Alarm from the Post Accident Monitoring System.

8.2.3.4.2.8 Reset Trip 2

This manual command is provided by a pushbutton on the MSC, and resets the SRPS.

8.2.3.4.3 Operator Interface Functions

The RPS presents all safety information to the operator through dedicated Safety Displays in the wall panels, and on the MSC in the MCR, and on the ESC in the ECC. This presentation of safety parameters is independent of the RCMS and permits the operator to evaluate the safe state of the reactor.

8.2.3.4.4 Data Communication to Reactor Control and Monitoring System

Safety parameters, trip settings and the results of the self-checking process of the RPS are provided to the RCMS through one way read only electrically isolated interfaces.

8.2.3.5 Reactor Protection Systems Software Development Verification and Validation Process

Independent verification and validation tasks have been performed as a required stage in software design and are executed by members of the design team not involved in the software development.

Verification and validation personnel maintain a close working relationship with development personnel to ensure that the verification and validation process findings and recommendations are integrated into the development process.

FRPS software development activities have been divided into production and review groups. The production group has the responsibility for software development and documentation. The reviewers have the responsibility for verification and validation tasks. These activities are allocated to individuals and teams from different sections in order to achieve independence throughout the process.

The following list presents the areas of responsibility for the activities related to software verification and validation:

Project Management

FRPS Development

FRPS Software Development/Production

FRPS Software Review

Quality Assurance

8.2.3.5.1 Verification and Validation Processes

Verification and validation processes support the development, operation, and maintenance processes.

The results of verification and validation activities and tasks are documented in task reports, anomaly reports, test documents, and the final report.

All outputs of verification and validation tasks became inputs to subsequent development processes and activities. At each phase, all documentation from previous phases was available.

The following verification and validation reports have been generated:

a) Task Reports: verification and validation task results are documented in task reports. The following task reports have been generated:

   (i) Software Requirements Evaluation Report
   (ii) Software Development Evaluation Report
   (iii) Source Code Evaluation Report
   (iv) Installation Configuration Audit Report
   (v) Test Results
   (vi) Evaluation of New Constraints
   (vii) Proposed Change Assessment

b) Anomaly Reports: Each anomaly detected by the verification and validation effort has been documented as an Anomaly Report and was evaluated for its impact on the system. An anomaly report contains the following:

   (i) description and location in the document or code
   (ii) impact of the anomaly
   (iii) cause of the anomaly and description of the error scenario
   (iv) observations/recommendations

c) Verification and Validation Final Report: This report will be issued at the end of the Installation and Commissioning Activity. The verification and validation final report will contain the following:

   (i) summary of all life cycle verification and validation activities
   (ii) summary of task results
   (iii) summary of anomalies and resolutions
   (iv) lessons learned
   (v) recommendations

8.2.3.5.2 Reactor Protection Systems Software Development Verification and Validation Process Status

In accordance with the V&V Plan the RPS Engineering has been audited and tested to ensure compliance with design goals. As part of the first stages of V&V the RPS design has been audited by independent sources, as experts and the client. The RPS software was reviewed four times and the last revision was performed directly on the version to be used during the factory acceptance test for the system. During the V&V Phase corresponding to design implementation, several test cases were carried out on the RPS, verifying and validating the logic and functional performance of the system. The whole process of integration and testing was followed up in accordance with auditable procedures and all tests were successfully passed by the system. At this stage the phase of design implementation was finished and the V&V plan has shown that the system fulfils its design requirements as expected.

8.2.3.6 Reactor Protection Systems Testability

In accordance with IEEE, the safety systems are designed such that they can be tested while the reactor is operational, as well as during those intervals when the reactor is shutdown. The RPS design allows the independent testing of redundant trains and load groups while maintaining the capability of these systems to respond to on-line process trip signals. Testing of individual trains while the reactor is operating is accomplished by

tripping the output of the channel being tested. The design provides the capability for periodic surveillance testing that simulates as closely as practicable the required safety function. The components are designed and organised so that they may be adequately inspected and checked.

8.2.3.7 RPS Failure under Demand Analysis

An analysis of the probability of failure under demand was conducted for the RPS (both FRPS and SRPS) in order to demonstrate that the system will reliably perform its intended safety function. To analyse the way the system may fail to perform its safety function a Fault Tree was developed for the system that was later solved using Boolean algebra.

The selected method for analysis of the RPS was the Fault Tree Analysis (FTA) method because of its efficiency and because it is widely used in nuclear industries following IEEE recommendations.

The Fault Tree methodology is a graphical logical model of the various parallel and serial combinations of faults that will result in the occurrence of the predefined undesired event.

The aim of the FTA method is to determine the probability and/or the frequency of a specified state of the system that is usually a fault state.

A Fault Tree thus depicts the logical interrelationships of basic events that lead to the undesired event, called the “top event” of the fault tree.

The faults can be events that are associated with component hardware failures, human errors, or any other pertinent events that can lead to the predefined undesired event.

As a result of this analysis, a graphical fault tree was constructed from which an algorithm can easily be derived to calculate the probability of system failure under demand.

Software Tools for the quantification of ‘Probability of Failure under Demand’ for complex systems have been developed and are commercially available to perform this type of fault tree analysis.

8.2.3.7.1 Analysis Methodology

During the probabilistic system analysis the input data are the failure rates of the components, and the probability value or the frequency of an event of the system is examined. In this sense the examined events are actually fault events, which are described by the probability of failure states.

The frequency of an event under a defined time interval gives the number of the failures.

Both the frequency and the probability are time dependent, which means that the values of them can be described by functions of time.

For the RPS the investigated failure probability requirement relates only to its main function, namely the actuation of the FSS through the FFAL (voted 2oo3) configuration outputs that drive the actuation devices, including the input signals for tripping.

The failure criterion for the FRPS is the failure of the Trip 1 signal when required (non-opening of 2oo3 of the relay contacts of the FFAL), which is defined as the Top Event for the Fault Tree.

8.2.3.7.2 Identification and Selection of Basic Events

The initial procedure is the development of a qualitative RPS Fault Tree up to its Basic Events. For each of the Basic Events identified in the Fault Tree, a failure criterion is established. Upon this failure criterion and taking as a base the Process and Instrumentation (P&I Loop Diagrams) and the Operational Limits and Conditions, where known, of each branch of the safety System, a quantitative Fault Tree is developed.

8.2.3.7.3 Common Cause Events

Frequently encountered common cause effects considered for this system are:

Human errors:

Maintenance, Testing, Surveillance and Design Human error (including software) common causes were included and modelled using the Beta Factor Model.

A protection system common cause failure probability estimated as β = 2% in Marcov Models PFDavg calculation (ISA SP84 committee) Memorandum, Dr. A. Anton Frederickson, August 31 - 2000) was included in the fault tree.

Electromagnetic Interference (EMI) will not prevent the FRPS from tripping. Therefore EMI will not be considered a common cause event in this system.

Seismic Basic events will not prevent the FRPS from tripping because of its 1E seismic qualification. These events have been described in the SAR and are excluded from the present fault tree.

There are several models for quantifying Systems subject to common cause failures.

The chosen Model was the Beta Factor model, was used to solve the FT.

8.2.3.7.4 Analysis Conclusions

Each Basic Event unsafe failure (time dependant) probability was calculated by the program and periodically tested components were modelled by using Module Failure Rate (or MTBF) and Module Inspection Time.

The calculations were used not only as a mean to ensure compliance with failure rates targets for the systems but also as a design tool to determine maintenance and surveillance frequencies.

The unavailabilities of the FRPS and SRPS were conservatively estimated as $9.2\ 10^{-4}$ and $9.0\ 10^{-5}$ respectively.

8.2.4 Conformance Analysis

This section presents an analysis of how the various functional requirements and the specific regulatory requirements of the RPS design bases are satisfied. Due to the complexity of this system, which interacts with most systems of the reactor, and the great number of requirements it has to fulfil, demonstration of conformance will be approached by addressing each requirement individually. For the same reason the approach is also extended to the rest of this chapter, including the instrumentation of Safety Category 2 systems.

8.2.4.1 Conformance to General Requirements

8.2.4.1.1 Conformance to General Requirements 1 and 2

Requirement 1: To start protective actions in order to shutdown the reactor.

Requirement 2: Initiate protective actions reliably to prevent or limit reactor fuel damage following abnormal operational transients.

The RPS is designed to provide protection against the onset and consequences of conditions that threaten the integrity of the reactor. Chapter 16 analyses all postulated initiating events and the corresponding system actions. The methods of assessing barrier damage and releases of radioactive material, along with the methods by which abnormal events are sought and identified, are presented in that chapter.

The design basis requires that the reliability of the initiation of a Trip 1 action is sufficient to prevent or limit fuel damage. In addition, the design basis requires that the reliability of the initiation of a Trip 2 action is sufficient to prevent or limit fuel damage in case of failure of Trip 1. The Containment Isolation action is also initiated by the FRPS in the case of an abnormal release of radioactive materials through the stack.

Table 8.2/1 provides a list of selected parameters that initiate protective actions.

The selection of the trip settings has been developed through analytical modelling, and experience gained in the development of the initial safety settings. The preliminary method of selecting safety settings provides for settings that are conservative enough to protect the reactor but with sufficient margin from the normal operating levels to preclude the possibilities of spurious actions.

8.2.4.1.2 Conformance to General Requirement 3

Requirement 3: To limit the uncontrolled release of radioactive materials by reliably initiating protective actions on detection of the release of fission products from the PCS.

When the release of radioactive materials to the environment is detected by the FRPS (by measuring particulate, iodine, and/or gas activity in the stack in triplicate channels) it initiates the protective action for containment isolation. In addition, the FSS action initiated by the reactor pool area radiation monitors satisfactorily limits the radiological consequences of failure of the fuel plates and irradiation facilities by initiating a Trip 1 action. These protective actions cover cases from minor to gross failure of fuel cladding (Chapter 16 evaluates gross failure of the fuel). In no case does the release of radioactive material to the environment result in exposures exceeding the guidelines of the applicable regulations.

8.2.4.1.3 Conformance to General Requirement 4

Requirement 4: Detect conditions that threaten the reactor from process parameters that are direct measures of operational conditions.

The process parameters that ensure a reactor trip if proper core cooling is jeopardised are; PCS flow, core pressure difference and core inlet and differential temperature. The safety analysis in Chapter 16 demonstrates that the set points for all these parameters are appropriate and prevent the fuel and rigs from reaching the safety limits.

8.2.4.1.4 Conformance to General Requirement 5

Requirement 5: Respond correctly to process parameters over the expected range and to rates of change of those process parameters.

The RPS instrumentation has been designed to cover the expected range of the parameter and its rate of change during all identified situations, from normal operation to abnormal operational transients. Chapter 16 identifies and evaluates the events that challenge reactor and rig integrity and shows how the safety systems respond to those situations.

8.2.4.1.5 Conformance to General Requirement 6

Requirement 6: Reliably monitor essential parameters that have spatial dependence.

Parameters monitored by the RPS have no significant spatial dependence. Nucleonic channels, for example, have no spatial dependence on the location of detectors due to the use of only the central rod for reactivity regulation and control during normal operation.

8.2.4.1.6 Conformance to General Requirement 7

Requirement 7: Redundancy will be provided, based on the potential for undetected failures that could degrade reliability.

To comply with the requirement for reliability, the RPS contains redundancy in a wide range of levels, from system level (FRPS and SRPS) to the low level of sensors, units and components. The RPS is supplied by triplicate measurement channels. Three trains in both RPSs, together with triplicate voting level circuitry assure the ability of the systems to perform their protective actions. Thus, undetected single random failures are adequately controlled ensuring system reliability is not degraded.

8.2.4.1.7 Conformance to General Requirement 8

Requirement 8: Multiple sets of equipment that cannot be tested individually will not be considered redundant.

Each of the three trains of the RPS is completely independent of each other. There is no redundancy within a given single train. In the case of testing a single component, the entire channel is put into the trip condition. The remaining two channels must remain operational.

8.2.4.1.8 Conformance to General Requirement 9

Requirement 9: Physical separation by distance, barriers or layout of reactor components will be provided as appropriate, to enhance the reliability of systems, particularly with respect to common cause failures.

To avoid common cause failures, like fires or floods, adequate physical separation of redundant channels and trains is a design criterion. The three channels and trains are designed according to IEEE standards where the required criteria to avoid common mode failures are presented. The Reactor Facility's design incorporates adequate separation by using enclosed cable trays for the entire cable path followed by each channel and train. Each channel is routed via cable trays and ducts (according to the IEEE requirements) to its particular dedicated room where all corresponding instrumentation is placed. Room walls provide enough physical separation to ensure that common cause failures do not affect more than one train at a time. Signals are transferred through different building levels using risers, which are enclosed cable trays fulfilling the IEEE requirements.

The system is designed to successfully face common cause failures by providing adequate physical separation by barriers, and by the distance between equipment in redundant trains.

8.2.4.1.9 Conformance to General Requirement 10

Requirement 10: All use of diverse equipment in redundant systems will be identified and justified in the design documentation.

Although diversification contradicts the requirement of standardisation, it is a useful tool to improve the reliability of the systems, by diminishing the possibilities of common mode failures. Diversity is used in the RPS design at different levels:

a) system level

b) event-initiation level

c) sensor level

Diversity in the RPS design resides primarily at the systemic level, with the FRPS and the SRPS based on different technologies (digital and hard-wired).

At the event-initiation level, the RPS considers the possibility of initiating the same given action (e.g. Trip 1) from different parameter states or situations (e.g. loss of coolant flow or low core pressure difference). Chapter 16 lists the parameters that initiate protective actions from various initiating events.

At the sensor level, a given parameter can be determined by more than one method (e.g. ionisation chambers or fission counters in the Nucleonic Instrumentation System).

8.2.4.1.10 Conformance to General Requirement 11

Requirement 11: If a single random failure can cause a RCMS action that generates a plant condition requiring a protective action but also prevents action by some RPS channels, the remaining trains of the RPS will meet their functional requirements as described in items 1, 2 and 3 above.

The RPS measurement channel components are not physically shared with the RCMS, thus a failure of one system cannot induce a failure of the other. The RPS measurement channels provide isolated outputs to the RCMS only. Conversely, RCMS dedicated components and signals are not used for generating RPS signals. Also physical separation between the RPS and the RCMS ensures that the probability of the control system preventing operation of the RPS is also negligible.

If a failure of the RCMS and a random single failure of the RPS were to occur simultaneously, the RPS operational trains will initiate the required protective action if necessary.

8.2.4.1.11 Conformance to General Requirement 12

Requirement 12: Loss of one power supply train will not prevent operation of the RPS.

In case of loss of one power supply train and even in the case of a complete black-out of the reactor, alternate power is available to the RPS. Failure of the Normal Power Supply will result in de-energising the solenoids that couple the CRs to the control rod drives, the CRDs motors and the solenoid valves of the compressed air system. The result is therefore a Trip 1 action, i.e. the fast insertion of CRs (and the corresponding negative reactivity) into the core. The reactor design is based on a fail-safe criterion against loss of energy, which ensures that the FSS will correctly perform its protective action during a loss-of-power condition.

8.2.4.1.12 Conformance to General Requirement 13

Requirement 13: Once initiated, the RPS action will be completed. Return to normal operation will require deliberate operator action.

The RPS is designed such that when trip parameters exceed their trip safety settings, the associated trip logic is latched. Once this is accomplished, the protective action goes

on to completion regardless of the state of the parameter that has initiated the protective action.

Normal operation is returned by manual operator action to reset the initiating device once it has returned to the normal operating range.

8.2.4.1.13 Conformance to General Requirement 14

Requirement 14: There will be sufficient electrical and physical separation between redundant instrumentation and control equipment monitoring the same parameter to prevent environmental factors, electrical transients, or physical events from impairing the ability of the system to respond correctly.

All RPS cabling is routed in separated cable trays or conduits for each channel, including routing to and from sensors, racks, panels, and CR solenoids.

Physical separation and electrical isolation between trains of the RPS is achieved by physically separating process instrumentation, instrument cabinets, panels and cabling. Separate panels are provided for each train except for the MCR main console, which has internal metal barriers for separation. Where equipment from more than one channel or train is in a panel, divisional separations are provided by fire barriers and/or physical distance of 152mm or more. Where wiring must be run between trains, separation is provided by qualified isolation techniques such as fibre optic digital communication cables and opto isolators.

The RPS logic circuits are designed so that an automatic FRPS or SRPS trip is initiated when the required number of sensors for any monitored parameter exceeds the safety setting.

Separate instrument cabinets are provided for the RPS instrumentation for each train and are installed in different locations.

8.2.4.1.14 Conformance to General Requirement 15

Requirement 15: No single failure within the RPS will prevent the proper operation of the RPS, when required, to satisfy safety design bases as described by requirements 1, 2 and 3.

See Sections 8.2.4.1.10 to 8.2.4.1.13

8.2.4.1.15 Conformance to General Requirement 16

Requirement 16: Any single maintenance operation, calibration operation, or test to verify operational availability will not prevent the ability of the reactor protection system to respond correctly.

During any operational state, any single component of the RPS can be taken out of service to be tested, maintained or calibrated without preventing the RPS from performing its protective functions. The modular design of the RPS minimises the time involved in maintenance, calibration and testing to verify operational availability; thus reducing the failure possibilities. During this time, the RPS displays to the operators that the channel or train under test is unavailable and sets the channel or train to the tripped state. The remaining operational channels or trains not undergoing maintenance or test are therefore working in a one out of two voting logic. These characteristics ensure that the RPS can cope with any single channel or train maintenance operation, calibration operation, or test, without affecting operational availability.

8.2.4.1.16 Conformance to General Requirement 17

Requirement 17: Two or more sensors for any monitored parameter exceeding the trip safety setting will initiate automatic protective actions.

All trip logic is based on a two-out-of-three criterion. The voting logic initiates the trip signal only when two or more channels for any monitored parameter exceed the trip Safety Setting. This two-out-of-three criterion to initiate the protective action prevents the RPS from generating spurious actions that could degrade operational availability.

8.2.4.1.17 Conformance to General Requirement 18

Requirement 18: Control and monitoring functions will be provided in the MCR for reactor systems, auxiliary systems and all other process systems. The automation of all provided control systems will be optimised.

All signals and safety-parameters handled by the RPS, together with status information are communicated to the ECC and MCR.

The RPS presents all safety information to the operator through dedicated displays in the MCR and the ECC. This presentation of safety parameters is independent of the RCMS and permits the operator to evaluate the state of the reactor. The operator can manually request the protection actions from these panels within the MC and the EC.

Safety parameters, trip Safety Settings and self-check results of the RPS are provided to the RCMS through a read only, electrically isolated interface. This allows the efficient use of reactor instruments, avoiding duplication, while improving presentation by the use of the RCMS visual display units, and allowing enhanced recording and analysis of safety events.

8.2.4.1.18 Conformance to General Requirement 19 and 20

Requirement 19: All essential instrumentation to allow the safe shutdown of the reactor and maintain it in a safe state, including PAM instrumentation, and CCTV will be provided in the MCR and in the ECC.

Requirement 20: Audible and visual alarms will be provided in the MCR, to alert operating personnel to any variations from the normal operating conditions during all modes of operation.

Operators are able to manually initiate protective actions from the MCR and ECC. The MCR and the ECC include dedicated safety displays and control panels, independent of the RCMS, to allow operators to evaluate the status of the reactor. The safety displays include the necessary alarms and annunciators to warn operators of abnormal conditions during all reactor states of operation. The control panel allows the operators to perform the following manual protective actions and enable the protection interlocks:

a) Trip 1

b) Trip 2

c) Containment Isolation

d) CERS Control

8.2.4.1.19 Conformance to General Requirement 21

Requirement 21: Sufficient MCR instrumentation will be provided for recording parameters related to the safe and efficient operation of the reactor facility.

All signals handled by the RPS are shared with the RCMS. Although the signal acquisition, the decision-making process and the protective actions of the RPS are considered Safety Category 1, the on-line storage of data is classified as Safety Category 2. Thus, the RPS information is saved through the RCMS historical data storage facility that is described in Section 8.6.3.3.4. The historic data recording system is a storage and retrieval system that continuously logs important plant status, including digital and analogue parameters, alarms, events, operator actions, operative parameters and plant and control system faults.

Redundant storage devices are used in order to ensure that all records are automatically stored in case of failure of one device. Redundant storage devices and suitable data handling software are provided to ensure that mandatory records of all reactor plant operations are automatically gathered and stored.

All selected archiving data are automatically saved on a permanent medium (for example magnetic tape).

The system has short-term historical data storage (of less than 12 months) saved inside the system for fast data retrieval. To work with long-term historical data (older than 12 months) the system needs to be loaded with the appropriate disk containing the data.

8.2.4.1.20 Conformance to General Requirement 22

Requirement 22: UPSs will be provided for the parts of the instrumentation and control systems that are required to operate and maintain essential reactor facility equipment in the event of an interruption in the Normal Power System following a design basis event.

Each of the three RPS trains is powered by an independent UPS. These UPSs comply with the relevant IEEE standards.

8.2.4.1.21 Conformance to General Requirement 23

Requirement 23: Local instrumentation will be provided to monitor the performance of equipment, which requires regular maintenance.

A regular surveillance and maintenance program for all equipment requiring periodic support is provided. Regular maintenance of instrumentation and control systems consists mainly of the calibration of instruments and instrument circuits. Local instrumentation is provided to monitor the performance of components that are critical for plant operation and safety.

8.2.4.1.22 Conformance to General Requirement 24

Requirement 24: Instrumentation and control systems will be designed to meet, as a minimum, the same operational requirements as the system or equipment they control. Instrumentation components of the RPS is of Safety Category 1 standards, regardless of the category of the system to which it is connected.

The design of the instrumentation and control systems meet, as a minimum, the same operational requirements as the systems they control. In the case of the RPS, the systems are classified as Safety Category 1 regardless of the process systems to which they are connected.

8.2.4.1.23 Conformance to General Requirement 25

Requirement 25: The equipment will be selected to ensure that it does not cause the adverse vibration of other equipment, and is not adversely affected by vibration in its designated location.

All the RPS equipment is designed to ensure it does not cause any adverse vibration of other equipment and is not adversely affected by vibration in its designated location. RPS equipment is seismically tested or certified, to ensure proper operation in the event of a Safe Shutdown Earthquake as specified in Chapter 2 of the SAR. RPS equipment is compliant with IEC Standard for EMI/RFI Criteria.

8.2.4.1.24 Conformance to General Requirement 26

Requirement 26: The instrumentation throughout the reactor facility will be uniform to the extent possible (for standardisation) after taking into account the constraints imposed by the requirement of diversity.

The provided instrumentation throughout the reactor facility was standardised to the extent possible, to assist in the support of maintenance, after taking into account the constraints imposed by the requirement of diversity.

8.2.4.1.25 Conformance to General Requirements 27 and 28

Requirement 27: Protection will be provided to minimise deterioration of all instrumentation, control systems, enclosures, and control wiring in their service environment.

Requirement 28: Complete protection against in service environments will be provided. This includes radiation, dust, corrosive vapours and liquids, humidity, mould, corrosion, galvanic action, insulation and thermal cycling.

All instrumentation, control systems, enclosures and control wiring are provided with adequate protection against their service environments, thereby minimising in-service deterioration. The design of the RPS limits the amount of equipment in demanding conditions, to the sensors and cables of the three channels. The components located in demanding environments are qualified such that they will perform their safety function in the worst case environmental conditions that they would be subjected to following a Design Basis Accident. Cable trays are of the enclosed type fulfilling the IEEE requirements. The instrument racks of the three trains of the RPS are located in dedicated rooms that are classified as mild environments. Also, there are no equipment rooms classified as harsh environments.

8.2.4.1.26 Conformance to General Requirement 29

Requirement 29: The equipment provided will be designed for an operating life of at least 40 years, with the provision that all maintenance procedures are performed at the proper time in a thorough and proper manner. Recommended surveillance and maintenance regimes for all equipment will be supplied.

All instrumentation, components and equipment have been designed, where possible to have an operating life of at least 40 years. All maintenance procedures to allow the equipment to comply with this requirement are being provided as part of the detailed engineering. In cases where that objective cannot be fulfilled, all the corresponding surveillance and replacement regimes are provided.

8.2.4.1.27 Conformance to General Requirements 30, 31 and 32

Requirement 30: Access to trip Safety Settings, component calibration controls, test points, and other terminal points will be under the control of plant operations supervisory personnel.

Requirement 31: Taking a train out of service for maintenance or modification will be under the supervision of the MCR operator. There are no bypasses allowed on either the

SRPS or FRPS. Any work performed on either will result in a train trip on that particular channel and will be continuously monitored by the MCR operator.

Requirement 32: Selected automatic and manual operational trip bypasses will be provided, as necessary, to permit particular states of plant operation (for example Physics Test State).

Access to trip settings, component calibration controls, test points and other terminal points are under the control of supervisory operations personnel.

If some essential part of the system is disabled, this will be continuously displayed in the MCR. If other components are disabled (for example by taking a sensor out of service for calibration or testing) this condition is also continuously displayed in the MCR, through the administratively controlled manual actuation of the RPS out-of-service indicator associated with that sensor, and the channel is then in the trip condition.

8.2.4.1.28 Conformance to General Requirement 33

Requirement 33: Provide manual control switches for initiation of safety actions by plant operators where necessary.

Manual trip switches to initiate the Trip 1 action are provided in several key locations of the plant. Conformance to General Requirement 34

Requirement 34: Verification and validation processes will be provided to ensure that the systems meet the functional, performance and reliability requirements.

A detailed verification and validation process, for all the design stages, is provided to ensure the systems reliably meet their functional requirements. The major objective of the verification and validation process is to prove that the system performs its intended functions correctly, that it performs no unintended functions, and provides information about its quality and reliability. The verification and validation process evaluates how well the system is meeting its technical requirements and its safety, security, and reliability objectives. It also helps to ensure that system requirements are not in conflict with any standards or requirements applicable to other systems or components. Verification and validation tasks analyse, review, demonstrate and test all system development outputs.

8.2.4.1.29 Conformance to General Requirement 35

Requirement 35: Differing techniques will be employed during the verification and validation process according to the type of design and the stage of the design process.

The verification and validation process relies on different techniques according to the type of design and the stage of the design process.

An example is Software verification and validation, done during qualification of base software.

Some software verification and validation techniques used during software development tasks are control flow analysis, data flow analysis, algorithm analysis, and simulation. Control and data flow analysis is mostly applicable for real time and data driven systems. Flow analysis transforms logic and data requirements text into graphic flows that are easier to analyse than the text. PERT, state transition and transaction diagrams are examples of control flow diagrams. Algorithm analysis involves re-derivation of equations or evaluation of the suitability of specific numerical techniques. Simulation is used to evaluate the interactions of large complex systems where there are much hardware, users, and other interfacing software units.

Some software verification and validation techniques used during software design tasks include algorithm analysis, database analysis, sizing and timing analysis, and simulation. Algorithm analysis examines the correctness of the equations or numerical techniques as in the software requirement activity, but also examines truncation and round-off effects, numerical precision of word storage and variables (e.g., single- vs. extended-precision arithmetic), and data typing influences. Database analysis is particularly useful for programs that store program logic in data parameters. A logic analysis of these data values is required to determine the effect these parameters have on program control. Sizing and timing analysis is useful for real-time programs having response time requirements and constrained memory execution space requirements.

Some software techniques used during code verification and validation tasks are control flow analysis, database analysis, regression analysis, and sizing and timing analysis. For large code developments, control flow diagrams showing the hierarchy of main routines and their sub-functions are useful in understanding the flow of program control. Database analysis is performed on programs with significant data storage to ensure common data and variable regions are used consistently between all call routines. Data integrity is enforced, and no data or variable can be accidentally overwritten by overflowing data tables. Data types and use are consistent throughout all program elements. Regression analysis is used to re-evaluate software requirements and software design issues whenever any significant code change is made. This technique ensures project awareness of the original system requirements. Sizing and timing analysis is done during incremental code development and compared against predicted values. Significant deviations between actual and predicted values are an indication of possible problems or the need for additional examination.

Code reading is another technique that may be used for source code verification. This is accomplished by having an expert programmer read through another programmer's code to detect errors.

8.2.4.1.30 Conformance to General Requirement 36

Requirement 36: Verification of all instrumentation and control systems will be provided, at the component level and at the system level, with validation provided at the system level only. Verification will be applied from the beginning of system design in order to ensure maximum effectiveness. The amount of verification to be performed will depend upon the importance of the system to plant safety or according to safety category classification.

The verification process is performed at the component level and at the system level. The verification process is applied in all stages of the design process to achieve maximum effectiveness. Identification of critical components allows the increase of the amount of verification to be performed in those systems that could impact a safety function.

8.2.4.1.31 Conformance to General Requirement 37

Requirement 37: All instrumentation and control components will be designed, arranged and suitably located so that they can be adequately inspected, tested and serviced as appropriate before commissioning and at regular intervals thereafter.

The safety systems are designed to be testable during operation of the reactor as well as during those intervals when the reactor is shutdown. This testability allows the independent testing of redundant channels and trains and load groups while maintaining the capability of these systems to respond to real process signals. The output of a channel being tested is tripped, if required, consistent with safety requirements and

operational limits and conditions. As mentioned earlier, the triple redundant trains of the RPS can be tested individually, without affecting the ability of RPS to perform their protective actions. Instrumentation and control trains of the RPS are placed in separate rooms accessible to operators and classified as mild environments. The design of the front and rear panels and consoles facilitate the testing and inspection processes. All equipment is organised in the corresponding rooms taking into account accessibility considerations. Equipment requiring operator manual actions is located taking into account ergonomic measures.

The size and weight of the equipment involved determine the space required for handling and accessing it in case of maintenance or replacement.

Any instrument to be monitored by personnel is installed such that it is easy to read from a position that is easily accessible by the personnel involved, (those instruments in the control consoles are a special case and are analysed separately).

In a similar way, the position of any valve or mechanism to be handled by operators or maintenance personnel was evaluated considering ease of access.

8.2.4.1.32 Conformance to General Requirement 38

Requirement 38: The RPS design will ensure that, during in-service testing, those trains remaining in service are able to accomplish any safety task, as required. The test method will minimise the time interval during which equipment is removed from service.

The RPS is based on two-out-of-three logic. Each of the three redundant trains can be separately tested, and are physically separated to avoid common cause failures (see Sections 8.2.4.1.9 and 8.2.4.1.31). This allows for in-service testing of each train without degrading the capability of the RPS to fulfil their functional requirements. The modular design of the RPS minimises the time needed to perform tests, during which the RPS will work on one out of two logic.

8.2.4.1.33 Conformance to General Requirement 39

Requirement 39: The test program and the test frequency will not cause deterioration of any reactor component beyond that provided for in the design.

The design of the RPS takes into account the necessity of testing the components. The test program and test frequency is based on the requirements of the RPS design and components chosen.

8.2.4.1.34 Conformance to General Requirement 40

Requirement 40: Appropriate test facilities will be provided. Appropriate procedures and instructions to carry out these test operations, including in-service testing will be included in the Operating and Maintenance Manuals.

An electronics workshop to perform testing and maintenance operations is provided. The Operations and Maintenance Manuals include all appropriate procedures and instructions to carry out these testing operations including in-service testing.

8.2.4.1.35 Conformance to General Requirement 41

Requirement 41: A simple design and a structured development process, including requirement specifications, prototypes, simulations, reviews, and testing for all custom design components will be provided.

The RPS is based on an “as-simple-as-possible” criterion relying on a structured development process that includes; requirement specifications, prototypes and

simulations when needed, as well as reviews and testing for all custom design components.

8.2.4.2 Conformance with Requirements from Standards

8.2.4.2.1 Conformance with Requirements from Standards 1 to 4

Requirement 1: The RPS will be classified as a Safety Category 1 system and will comply with IEEE standards for Class 1E equipment.

Requirement 2: Class 1E qualification will be in accordance with IEEE and relevant Australian standards.

Requirement 3: The definitions for independence and redundancy for Class 1E systems will be applied to the Class 1E systems for the reactor facility.

Requirement 4: Class 1E instrumentation and control wiring will be separated in accordance with IEEE. Additionally control wiring will conform to the wiring requirements of AS 3000, RPS cabling will conform to the requirements of AS 1660.5 and the PAM cabling will conform to and the fire requirements of AS 3013.

All equipment and components of the RPS are qualified to IEEE Class 1E requirements as applicable in accordance to a qualification plan.

8.2.4.2.2 Conformance with Requirements from Standards 5

Requirement 5: IEEE will be used in the design of all operator interfaces.

The human-machine interface requirements of IEEE are met by the design of the operator interfaces.

8.2.4.2.3 Conformance with Requirements from Standards 6

Requirement 6: The equipment provided will not cause adverse electromagnetic interference to other equipment and will not be adversely affected by electromagnetic emissions from other equipment.

All equipment has been properly tested and qualified to ensure it will not cause any electromagnetic interference to other equipment and will not be adversely affected by electromagnetic emissions from other equipment.

8.2.4.2.4 Conformance with Requirements from Standards 7

Requirement 7: The FRPS will be designed based on the requirements in the IEEE standards for the application of computer systems in reactor safety systems, associated software QA.

The computer-based FRPS is designed based on the requirements in the IEEE standards for the application of computer systems in reactor safety systems, associated software QA.

8.2.4.3 Conformance to Additional Requirements

8.2.4.3.1 Conformance to Additional Requirements 1 and 2

Requirement 1: The FRPS and SRPS will be provided, so that they automatically initiate the operation of appropriate systems to ensure that safety limits are not exceeded during any abnormal plant condition or design basis accident. The systems will be diverse in

that the FRPS will be computer-based, and the SRPS will be a hard-wired system. There will be no common instrumentation in the two systems.

a) The FRPS consists of a combination of hard-wired and digital processing modules. The protective functions associated with this system are:

   (i) Trip 1: Insertion of CRs
   (ii) Protection Interlocks (Start-up and Process Interlocks)
   (iii) Containment Isolation
   (iv) CERS Control

b) The SRPS is based on hard-wired technology. The protective function associated with this system is:

   (i) Trip 2: Partial draining of the heavy water reflector vessel and Trip 1 request
   (ii) Protection Interlock (Process Interlock)
   (iii) There is no common instrumentation in these two systems.

Requirement 2: The RPS will initiate all automatic reactor shutdowns and will initiate all ESF protective functions.

The conformance to these requirements follows from the RPS description in Section 8.2.3. Passive components such as cables trays and some instrument piping (that measuring core pressure difference) are shared between the FRPS and SRPS while maintaining separation of the three redundant trains.

8.2.4.3.2 Conformance to Additional Requirements 3

Requirement 3: The RPS will protect against operational errors, if process parameters are outside predetermined limits.

Operational errors are avoided by using a sufficient number of interlocks and an adequate selection of safety settings, which prevent process parameters from being outside their limits.

8.2.4.3.3 Conformance to Additional Requirements 4

Requirement 4: The RPS will minimise the likelihood that operator actions could defeat the effectiveness of the system during all operational states, but not negate correct operator actions during abnormal plant conditions.

Once initiated, the protective actions performed by the RPS cannot be stopped, up to their complete conclusion. Operators cannot defeat the effectiveness of the protective action. Similarly operators can manually initiate a protective action but cannot terminate the requested action once initiated.

8.2.4.3.4 Conformance to Additional Requirements 5

Requirement 5: The RPS will have sufficient instrumentation for monitoring the operation of the reactor during power, physics test, shutdown and refuelling.

The RPS is able to perform protective actions and monitoring functions during any operational state of the plant: Shutdown, Power, Physics Test and Refuelling. In all cases, the safety parameters are presented to the operators in the consoles of the MCR and ECC.

8.2.4.3.5 Conformance to Additional Requirements 6

Requirement 6: The RPS will have sufficient recording instruments to monitor reactor parameters during and following operational occurrences and accident conditions.

The RPS communicates its status information on all of its parameters to the RCMS, where the information is displayed and stored for future retrieval.

8.2.4.3.6 Conformance to Additional Requirements 7

Requirement 7: The RPS will input all information to the RCMS via approved isolation devices. The use of isolation devices will ensure that the RPS can not be affected by signals originating from the RCMS.

The RPS transmits all its safety information to the RCMS via Class 1E qualified unidirectional and electrically isolated interfaces. The RCMS acquires all the safety data to be processed, with the purpose of providing the operators displays of; system and equipment states, logic calculations, historical registering and alarm detection. This interconnection of the RPS to the RCMS is carried out using appropriate isolation devices to ensure the complete separation of Safety Category 1, from Safety Category 2 and 3 systems.

8.2.4.3.7 Conformance to Additional Requirements 8

Requirement 8: The RPS will include the following characteristics to ensure a fail-safe design:

a) The systems function automatically and independently of other systems.

b) Detection and actuation mechanisms shutdown the reactor in adequate time to protect the reactor from exceeding safety limits.

c) Following initiation of the trip systems, no manual operator intervention can prevent the trip completing its action.

d) Trip signals will not be generated using automatically reset devices. Once in the tripped state they will require deliberate operator action to be reset.

e) The systems' designs employ diversity to enable all postulated initiating events to be detected in a minimum of two different ways, where physically practicable.

f) The systems will comprise redundant trains that are independent and isolated from each other, to prevent a common cause failure.

g) The systems will allow trip levels to be set with adjustable margins.

h) The systems will have the capability to identify the parameter which initiated the first trip signal.

The RPS provides those characteristics as follows:

a) The FRPS and SRPS function automatically and independently of other systems and each other.

b) Detection and actuation mechanisms trip the reactor in adequate time to protect the reactor from exceeding safety limits. The response time of the FRPS, SRPS, FSS and SSS ensure that reactor shutdown is achieved in adequate time to protect the reactor from all design basis accidents.

c) Following initiation of either or both trip systems, no manual operator intervention is required.

d) Trip signals are generated using latching devices and require deliberate operator action to reset. Trip signals are reset by manual operator action in the MCR and in the ECC.

e) The FRPS and SRPS employ diversity to enable all postulated initiating events to be detected in a minimum of two different ways. Chapter 16 identifies the alarms and RPS trips for each postulated initiating event.

f) The FRPS and SRPS comprise redundant trains that are independent and isolated from each other, to prevent a common cause failure.

g) Instrumentation and trip systems enable trip levels to be set with adjustable margins. The design considers instrument drift, testability, and repeatability in the selection of instrumentation and controls and in the determination of safety settings. Adequate margins between safety limits and instrument safety settings are provided. Instrument error is known by its specification. The safety setting is fixed based on operational limits and the known error.

h) The FRPS, SRPS and RCMS have the capability to identify the parameter which initiated the first trip signal. When the RPS initiates a protective action the corresponding safety parameter that exceeded its corresponding safety setting appears highlighted and remains in that state until the operator resets the condition.

8.2.4.3.8 Conformance to Additional Requirements 9

Requirement 9: The RPS will employ voting logic in the trip circuitry such that maintenance can be carried out on defective channels without the need for the reactor to be shut down. Channels taken out of service will be identified as “tripped”, until back in service.

All trip circuits actuate a protective action on two-out-of-three voting logic. This allows one channel to be tripped while the other two are left in service and the reactor remaining operational. The Trip 1 or 2 actions would then be initiated if one of the remaining channels tripped.

8.2.4.3.9 Conformance to Additional Requirements 10

Requirement 10: Audible and visible alarm systems will be provided for early indication of any change that could lead to a reduction in safety while the reactor is operating or shut down.

Audible and visual alarms are provided in the MCR and ECC through the RPS safety panels and the RCMS.

End of Section

Table 8.2/1 RPS Safety Signals

	FRPS Safety Plant Signals
1	Start-up neutron flux
2	Wide Range Log Neutron Flux
3	Wide Range Log Neutron Flux Rate
4	Core temperature difference
5	Core inlet temperature
6	Core pressure difference
7	Primary cooling flow
8	Reflector cooling flow
9	Expansion tank low level
10	Rigs Cooling flow
11	RSPCS Flap Valve 1 closed
12	RSPCS Flap Valve 2 closed
13	Pool water level (Trip 1 level)
14	Pool open-end gamma activity
15	Seismic level
16	Compressed air storage tank pressure
17	Stack particulate activity
18	Stack iodine activity
19	Stack noble gas activity
20	Stack particulate rate
21	Stack iodine rate
22	Stack noble gas rate
23	Hot Neutron Source (SPARE)
24	Cold Neutron Source
25	Normal Power Supply Unavailability
26	RCMS Unavailability
27	SSS locked
28	Air Pressure CERS
29	Air Cooling Temperature CERS Circuit
30	Air Return Temperature CERS Circuit
31	FFAL request
32	CIFAL-G1-request
33	CIFAL-G2-request

	SRPS Safety Plant Signals
1	Power Log Neutron Flux Rate
2	Power Log Neutron Flux
3	Power Linear Neutron Flux
4	Core Outlet Temperature
5	Core Pressure Difference (Trip 2)
6	Pool Water Level (Trip 2)
7	Reflector Vessel Temperature
8	Seismic level
9	Control Rod 1 Down Position
10	Control Rod 2 Down Position
11	Control Rod 3 Down Position
12	Control Rod 4 Down Position
13	Control Rod 5 Down Position
14	Failure of Trip 1
15	SFAL Request

Table 8.2/2 Software Requirements Verification and Validation Tasks

Tasks	Description	Methods and Tools	Required Inputs	Outputs
Traceability Analysis	Trace requirements in the DSRS and the RPS System Description and the preliminary version of these documents.	Documentation reviews	SRS (Preliminary Version) RPS System Description (Preliminary Version) DSRS RPS System Description	Requirements Evaluation Report Traceability Matrix Anomaly Report(s)
Software Requirements Evaluation	Ensure that software requirements are correct, complete, consistent, accurate, and testable, and will satisfy the system requirements.			
Interface Requirements Analysis	Verify that the requirements for software interfaces with hardware, user/operator and other systems are correct, consistent, complete, accurate, and testable.			
FAT BRC Test Plan Generation	INVAP generates the plan for FAT BRC testing.		DSRS RPS System Description	FAT BRC Test Plan
SAT Tests Plan Generation	INVAP generates the plan for SAT testing. This plan will verify the correct and safe operation of the software in the operational environment.		DSRS RPS System Description	SAT Test Plan

Table 8.2/3 Software Development Verification and Validation Tasks

Tasks	Description	Methods and Tools	Required Inputs	Outputs
Traceability Analysis	Trace software design to system requirements and vice versa. Check for correctness, consistency, and completeness.	Documentation reviews	DSRS RPS System Description Design Document	Traceability Matrix Anomaly Report(s)
Software Design Evaluation	Evaluate the software design and the decomposition of the system into functional modules for correctness, consistency, completeness, accuracy, and testability.	Documentation reviews Design Walkthroughs	Configuration Item tests DSRS RPS System Description Design Document	Software Design Evaluation Report Anomaly Report(s)
Interface Analysis	Verify interfaces with hardware, user, and operator for completeness, consistency, testability, and correctness.	Documentation review	DSRS RPS System Description Design Document	
Unit and FAT USA Test Plan Generation and Verification	Foxboro developed the Unit Test Plan and the FAT USA Test Plan. These plans were reviewed and approved by INVAP.		RPS System Description DSRS Design Document Unit Test Plan FAT USA Test Plan	Unit Test Plan FAT USA Test Plan Anomaly Report(s)

Table 8.2/4 Code and Implementation Verification and Validation Tasks

Tasks	Description	Methods and Tools	Required Inputs	Outputs
Traceability and Interface Analysis (Software Configuration Review)	Trace the software configuration items to software design and vice versa. Analyse relationships for correctness, consistency, and completeness. Check the interfaces with hardware, software, and other systems.	Document Review Inspection of software configuration items	Design Document Software Configuration items DSRS RPS System Description	Traceability Matrix Anomaly Report(s)
Test Procedure Generation and Verification	Develop test procedures for unit testing, FAT USA and FAT BRC. INVAP developed the FAT BRC test procedures.		DSRS RPS System Description Design Document Unit, FAT USA and FAT BRC Test Procedures	Unit Test Procedures FAT USA Test Procedures FAT BRC Test Procedures Anomaly Report(s)
Unit Test Execution and Verification	At this level, software configuration items are not integrated into the system; therefore, it can be extensively tested. The objective is to show that each configuration item performs its intended function and does not perform unintended functions. Document the test results and analyse it to verify anomalies.	Software Configuration Items test	Software Configuration Items (item (a)) Unit Test Plan Unit Test Procedures Unit Test Result	Unit Test Results Anomaly Report(s)

Table 8.2/5 Integration and Test Verification and Validation Tasks

Tasks	Description	Methods And Tools	Required Inputs	Outputs
Traceability Analysis	Trace the software configuration items to test plans and procedures and vice versa.		SAT and FAT USA Test Plans and Test Procedures Traceability Matrix Software Configuration Items	Traceability Matrix Anomaly Report(s)
Interface & Communication Tests	Test interfaces with hardware, user, and operator for completeness, consistency, and correctness. Test all communication channels.	Interface tests Communication tests	DSRS RPS System Description Design Document	Anomaly Report(s)
SAT Test Procedure Generation and Verification	Develop SAT Test Procedures.		DSRS RPS System Description Design Document SAT Test Plan SAT Test Procedures	SAT Test Procedures Anomaly Report(s)
FAT USA Test Execution and Evaluation	This testing was performed in the USA. Analyse and document test results.	Systematic Tests	RPS Software (**b**) FAT USA Test Plan FAT USA Test Procedures FAT USA Test Results	FAT USA Test Results Anomaly Report(s)

Tasks	Description	Methods And Tools	Required Inputs	Outputs
FAT BRC Test Execution and Verification	This testing was performed in Bariloche. Analyse and document test results.		RPS Software (**c**) FAT BRC Test Plan FAT BRC Test Procedures FAT BRC test results	FAT BRC Test Results Anomaly Report(s)

Table 8.2/6 Verification and Validation Tasks

Tasks	Description	Methods and Tools	Required Inputs	Outputs
Acceptance Test Execution and Verification	Perform acceptance testing. Analyse test results to validate that the software satisfies the system requirements. Document the test results.		Source Code Executable Code Acceptance Test Plan Acceptance Test Procedures Acceptance Test Results	Test Results Anomaly Report(s)

Table 8.2/7 Installation and Commissioning Verification and Validation Tasks

Tasks	Description	Methods and Tools	Required Inputs	Outputs
Availability Test Execution	Perform Availability Test.			Anomaly Report(s)
V&V Final Report Generation	Summarise in this report the V&V activities, tasks and results.		RPS SVVP V&V Task Results	V&V Final Report

Table 8.2/8 Operation and Maintenance Verification and Validation Tasks

Tasks	Description	Methods and Tools	Required Inputs	Outputs
Proposed Change Assessment	Assess proposed changes to determine the effect of the changes on the system. Determine the extent to which V&V tasks would be iterated.		Proposed Changes Installation Package	Proposed Change Assessment

End of Tables

Figure 8.2/1 First Reactor Protection System and Second Reactor Protection System Actions