8.3 FIRST SHUTDOWN SYSTEM INSTRUMENTATION

8.3.1 Introduction

The First Shutdown System (FSS) is one of the Safety Category 1 Engineered Safety Features for reactivity control. It is based on the insertion of CRs (see Figure 8.3/1) into the core by means of the Control Rod Drive System. A description of this system can be found in Chapter 5. Details concerning the instrumentation of this system and its connection to the FRPS are presented in this Section.

8.3.2 Design Requirements

The following describes the design requirements applicable to the instrumentation and control components of the FSS.

8.3.2.1 General Requirements

The FSS instrumentation will fulfil the following functional requirements according to its Safety Category 1 classification where required:

1. Provide information to operators to indicate whether its safety functions are being accomplished.
2. Indicate the successful operation of individual systems.
3. Avoid those anticipated operational conditions that may lead to accident conditions thereby preventing safety limits for the fuel from being challenged.
4. Initiate the fast insertion of negative reactivity into the core when a reactor trip signal is received from the First Reactor Protection System (FRPS).

8.3.2.2 Requirements from Codes and Standards

1. Instrumentation for the reactor shutdown systems will be classified as Safety Category 1 where required. This reactor shutdown systems instrumentation will comply with IEEE standards for Class 1E equipment. Instrumentation not related to the safety functions of the FSS will comply with the requirements for Safety Category 2.

8.3.3 Description

8.3.3.1 Control Rod Drive Parameters

The following are the main signals associated with each Control Rod Drive (CRD):

Instrument	Location	System	Indication/Control	Protection Function
Pressure switch (x3)	Storage tank	FRPS	Pressure low indication	Reactor Start Up Interlock
Proximity switch (x 3)	Shock absorber	SRPS	Lower position indication	Failure of the FSS
Proximity switch (x2)	Pneumatic cylinder flange	RCMS	Piston coupled indication	None

Instrument	Location	System	Indication/Control	Protection Function
Proximity switch (x 2)	Guide cylinder	RCMS	Upper position indication & stops CRD motor	None
Proximity switch (x 2)	Guide cylinder	RCMS	Lower position indication & stops CRD motor	None
Encoder	CRD motor	RCMS	CR position	None
Pressure switch	Compressed air supply line	RCMS	Low pressure indication	None
Pressure switch	Compressed air supply line	RCMS	High pressure indication	None
Stepper Motor	CRD mechanism	RCMS	Motor control	None

8.3.3.2 Failure Mode and Effects Analysis

A Failure Modes and Effects Analysis (FMEA) has been conducted for the FSS with results indicating that instrumentation failures do not induce any significant effect on system performance.

8.3.4 Conformance Analysis

8.3.4.1 Conformance to General Requirements

8.3.4.1.1 Conformance to General Requirements 1 and 2

Requirement 1: To provide information to operators to indicate whether its safety functions are being accomplished.

Requirement 2: Indicate the successful operation of individual systems.

The signals handled by the FSS are presented in Section 8.3.3.1. Operators can access all signals through the Main Console (MC) of the RCMS. The signal that indicates success or failure of the FSS, that is the CR inserted signal, is displayed at the PAM, RPS, PAM and RCMS panels and consoles.

8.3.4.1.2 Conformance to General Requirements 3

Requirement 3: To avoid those anticipated operational conditions that may lead to accident conditions thereby preventing fuel limits from being challenged.

The FMEA has shown that no FSS instrumentation failure affects safety. For the unlikely case that more than one instrument fails at the same time, the FSS is based on a fail-safe design and a trip action will be initiated.

8.3.4.1.3 Conformance to General Requirements 4

Requirement 4: Initiate the fast insertion of negative reactivity into the core when a reactor trip signal is received from the First Reactor Protection System (FRPS).

The FSS inserts the CRs into the core by removing power from the electromagnets and the trip valves. These actions cause the CRs to drop. The CRs are inserted in the core in

a nominal time such that 2000 pcm are inserted in the first half second, with only four of the CRs needed to be fully inserted to meet the shutdown margin requirements of at least 1000 pcm. The redundancy of the systems that control the CRs insertion, plus the adequate selection of quality components ensures high reliability of the system. More information on the FSS is contained in chapter 5.

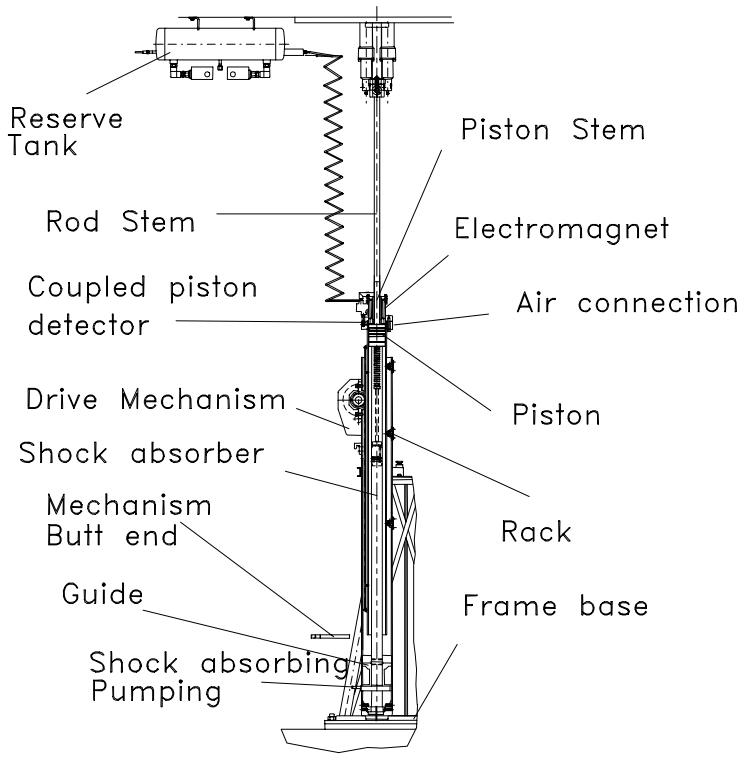
8.3.4.2 Requirements from Codes and Standards

Requirement 1: Instrumentation for the reactor shutdown systems will be classified as Safety Category 1. The reactor shutdown systems instrumentation will comply with IEEE standards for Class 1E equipment.

All instrumentation and control components, related to the safety function, of the FSS are qualified to the same level as the FRPS, which is to IEEE Class 1E standards.

End of Section

Figure 8.3/1 Control Rod



End of Figures

8.4 SECOND SHUTDOWN SYSTEM INSTRUMENTATION

8.4.1 Introduction

The Second Shutdown System (SSS) shuts down the reactor by partially draining the heavy water in the reflector vessel. The absence of moderator in the reflector vessel causes a large decrease in neutron reflection to the core, which makes the reactor highly sub-critical. A description of this system can be found in Chapter 5. Here, details concerning the instrumentation of this system and its connection to the SRPS are presented.

8.4.2 Design Requirements

The following describes the design requirements for the instrumentation and control components of the SSS.

8.4.2.1 General Requirements

The SSS instrumentation will fulfil the following functional requirements according to its Safety Category 1 classification:

1. Provide information to operators to indicate whether its safety functions are being accomplished.
2. Indicate the successful operation of individual systems.
3. Avoid those anticipated operational conditions that may lead to accident conditions thereby preventing safety limits for the fuel from being challenged.
4. Initiate the insertion of negative reactivity into the core when a reactor trip signal is received from the Second Reactor Protection System (SRPS).

8.4.2.2 Requirements from Codes and Standards

Instrumentation for the SSS will be classified as Safety Category 1 where required. This reactor shutdown system instrumentation will comply with IEEE standards for Class 1E equipment.

8.4.3 Description

8.4.3.1 Safety Parameters

The following are the main signals associated with the Second Shutdown System:

Detector	Location	System	Indication	Protection Action
Position switch (x3)	isolation valve	FRPS	Valve open indication	Reactor Start up Interlock
Level switch (x3)	Expansion tank	FRPS	Low water level	Reactor trip
Level transmitter (x2)	Heavy water drain tank	PAM	Level indication	Post Accident Monitoring
Position switches	actuation valves (x 6)	RCMS	Valve position indication	None
Pressure transmitter	Expansion Tank	RCMS	Pressure indication	None

Detector	Location	System	Indication	Protection Action
Level transmitter	Expansion Tank	RCMS	Indication	None
Pressure transmitter	Compressed air tank	RCMS	Indication	None
Pressure switch	Compressed air supply line	RCMS	Low pressure indication	None

8.4.3.2 Failure Mode and Effects Analysis of the Second Shutdown System

A Failure Modes and Effects Analysis (FMEA) has been conducted for the SSS with results indicating that instrumentation failures do not induce any significant effect on system performance.

8.4.4 Conformance Analysis

8.4.4.1 Conformance to General Requirements

8.4.4.1.1 Conformance to General Requirements 1 and 2

Requirement 1: Provide information to operators to indicate whether its safety functions are being accomplished.

Requirement 2: Indicate the successful operation of individual systems.

The signals handled by the SSS are described in Section 8.4.3.1. Operators have access to all indications through the panels and consoles of the RPS, PAM and RCMS.

8.4.4.1.2 Conformance to General Requirements 3

Requirement 3: Avoid those anticipated operational conditions that may lead to accident conditions thereby preventing fuel limits from being exceeded.

In case of a failure of the FSS, the system generates a failure signal that actuates the SSS Trip 2 action, which involves draining enough heavy water from the reflector vessel to make the core sub-critical. This action shuts down the reactor and prevents anticipated occurrences from evolving into accident conditions that could challenge fuel limits.

8.4.4.1.3 Conformance to General Requirements 4

Requirement 4: Initiate the insertion of negative reactivity into the core when a reactor trip signal is received from the Second Reactor Protection System (SRPS).

The actuation of the SSS is automatic and results in the opening of the SSS trigger valves that allow for the partial draining of the reflector vessel. The action is initiated by request of the SRPS when; the FSS fails to fulfil its safety function after 1sec, or a trip parameter exceeds its set point value. The system can also be triggered manually by the operator. Draining of the reflector vessel is passive and occurs under gravity.

The operator cannot interfere with or interrupt the triggering signal generated by the SRPS. The operator cannot reset the SSS until thirty seconds after the trip has occurred. This allows the heavy water drain to be completed.

8.4.4.2 Requirements from Codes and Standards

8.4.4.2.1 Conformance to Additional Requirements 1

Requirement 1: Instrumentation for the reactor shutdown system will be classified as Safety Category 1 where required. This reactor shutdown system instrumentation will comply with IEEE standards for Class 1E equipment.

Where required instrumentation and system components of the SSS are qualified to the same standard as the SRPS, that is, to IEEE Class 1E Standards.

End of Section

8.5 POST ACCIDENT MONITORING SYSTEM

8.5.1 Introduction

The Post Accident Monitoring (PAM) system provides the necessary information for operators to monitor and take actions after an accident condition. In addition, it provides information to indicate whether plant safety functions are being accomplished and it is an important tool for implementing manual recovery actions. The PAM system comprises all the electrical devices and circuitry involved in generating the PAM signals for display in the MCR and ECC.

The PAM system is an ESF and is therefore classified as Safety Category 1. PAM is based on redundant trains. Some primary sensors are shared with the FRPS and SRPS, and isolated PAM signals are used by the RCMS to display the PAM parameters.

8.5.2 Design Requirements

8.5.2.1 General Requirements

The PAM system is designed to meet the following functional requirements:

1. Provide information to operators to indicate whether plant safety functions are being accomplished.
2. Indicate the successful operation of individual safety systems.
3. Alert operators to take safety actions for initiating a system or function that is not automatic.
4. Indicate to operators when barriers to fission product release have the potential for being breached or have been breached.
5. Determine the magnitude of radioactive materials released.

The following general requirements ensure PAM system availability by means of redundancy, separation, and qualified equipment.

6. Redundancy is provided so that undetected failures do not prevent the system functioning.
7. Multiple sets of equipment that cannot be tested individually are not be considered as being redundant.
8. Physical separation by distance, barriers or layout of reactor components is provided to enhance the reliability of systems, in particular with respect to common cause failures.
9. All use of diverse equipment in redundant trains is identified and justified in the design documentation.
10. Signals to the ECC and to the MCR are hard-wired for all designated PAM instrumentation.
11. Outputs from the PAM system to the RCMS are isolated.
12. PAM system equipment and components have been qualified under simulated worst case in-service conditions, and will be of proven technology to provide a high degree of confidence in their operability under all DBA conditions.

8.5.2.2 Requirements from Standards

1. The PAM system is classified as a Safety Category 1 system and complies with IEEE standards for Class 1E equipment.
2. Class 1E equipment has been qualified in accordance with the requirements set out in IEEE and relevant Australian standards.
3. The definitions for independence and redundancy for Class 1E systems contained in IEEE have been applied to the Class 1E systems for the reactor facility.
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 and the fire protection requirements of AS 3013.
5. IEEE has been used in the design of all operator interfaces.
6. PAM equipment will not cause any adverse electromagnetic interference that may affect other equipment. In addition, PAM equipment will not be adversely affected by any electromagnetic emissions from other equipment, that is, it will be compatible with all other reactor facility equipment.

8.5.2.3 Additional Requirements

1. PAM instrumentation will be able to monitor the effectiveness of all ESF.
2. PAM instrumentation will indicate whether the reactor is shutdown.
3. Systems that aid re-entry into contaminated areas following a DBA will be classified as PAM systems. Such systems include Closed Circuit Television (CCTV) and communication systems.
4. Traceable material and test certificates will be provided for components or equipment that is required for PAM functions.
5. Type testing under simulated in-service conditions will be provided for all PAM equipment to provide the required confidence in such a way that equipment will perform its intended function during post-accident reactor monitoring.
6. Hard-wired signals to the ECC and MCR will be provided for all designated PAM instrumentation. Isolated outputs from the PAM system to the RCMS will also be provided.

8.5.3 Post Accident Monitoring System Description

8.5.3.1 Post Accident Monitoring System Parameters

8.5.3.1.1 Post Accident Monitoring System Signal Safety Characteristics

All signals monitored by the PAM system are:

a) Qualified as Safety Category 1.

b) Double redundant with physical separation.

c) Supplied electrical power via UPS.

d) Provided with a dedicated PAM panel in the MCR and ECC.

e) Available in the MCR and the ECC with continuous hardwired display.

f) Have the appropriate range for accident conditions.

g) Provided with electrically and functionally isolated interfaces with the RCMS, FRPS and SRPS.

8.5.3.1.2 PAM Parameters

The parameters monitored by the PAM system are shown in Table 8.5/1. Different components (e.g. sensors), measurement principles and methods will be employed according to the process variable to be monitored.

The PAM parameters associated with each safety system are described in the following paragraphs:

8.5.3.1.2.1 First Shutdown System

a) Control Rod Position.

These five parameters indicate if each of the CRs are fully inserted into the core. The indication of CR fully inserted is via limit switches that are part of the SRPS.

8.5.3.1.2.2 Second Shutdown System

a) Heavy Water Storage Tank Level.

This parameter indicates if the reflector vessel has been drained and that heavy water has been drained into the storage tank. It indicates success or failure of the SSS.

8.5.3.1.2.3 Primary Cooling System

a) Reactor Pool Water Level. Three levels are detected:

(i) The reactor pool low level switches are located below the Hot Water Layer. At this level, the SRPS actuates Trip 2 and the PAM system actuates the reactor evacuation alarm.

(ii) The reactor pool EMWS trip water level switches are located close to the upper edge of the chimney. At this level the EMWS is passively actuated.

(iii) The core water level switches are located approximately one metre above the core level. This parameter provides indication of the availability of coolant to ensure that the fuel is not damaged.

b) Flap Valve Position

The flap valves located on the primary cooling inlet pipelines are monitored for the fully open position to indicate that natural circulation of the pool water is occurring.

8.5.3.1.2.4 Reactor and Service Pool Cooling System

a) Service Pool Water Level

The service pool level switches are located above the fuel storage area.

8.5.3.1.2.5 Emergency Makeup Water System

a) Storage Tank Level

The level switches are located in tank 1230-BR-002 to indicate the amount of water stored.

b) EMWS Flow

The EMWS also monitors the flow, using flow switches to show that the system is working properly.

8.5.3.1.2.6 Nucleonic Instrumentation

a) Neutron Detectors – Wide Range Log Instrumentation System.

Located outside the reflector vessel, this system gives indication of the reactor shutdown condition. These neutron detectors are shared with the FRPS.

8.5.3.1.2.7 Radiation Monitoring System

The following parameters are monitored:

a) Reactor Pool area gamma dose rate.

b) Gamma dose rate (Basement and Reactor Hall) in areas where there is a risk of radiation exposure.

c) Pool top radiation monitors to detect fuel damage.

8.5.3.1.2.8 Reactor Containment Systems

Reactor Containment Systems comprise the following ESF, a physical barrier (the Containment), the Containment Isolation System (CIS), the Containment Energy Removal System (CERS), Containment Pressure Relief and Filtered Ventilation System (CPRFVS) and the Containment Vacuum Relief System (CVRS). The systems have the following PAM parameters:

a) Containment isolation valves open and closed positions

b) Activity detectors in the stack (shared with the FRPS):
   (i) particulate activity detector
   (ii) iodine activity detector
   (iii) noble gas activity detector

c) Reactor Building Pressure

d) SAS Doors Position

8.5.3.1.2.9 General

Other parameters monitored by the PAM system are:

a) ECC ventilation and pressurisation system (ON signal)

b) Diesel Generators (ON signal)

c) Diesel Generators fuel low indications.

8.5.3.2 Post Accident Monitoring System Architecture

The Post Accident Monitoring System (PAM) is a dual redundant system consisting of two independent, redundant trains named Train 1 and Train 2. Each parameter connected to the PAM is provided with dual measurement channels named Channel 1

and Channel 2, where Channel 1 is connected to Train 1 and Channel 2 is connected to Train 2. All PAM channels are completely independent from each other. Some PAM channels share common components with the corresponding RPS channels. In these cases signals are electrically isolated prior to transmission to the SRPS and PAM systems.

8.5.3.2.1 Signal Conditioners

The signal conditioners are sensor specific items that 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 Spec 200 input modules. The types of sensors interfaced by the signal conditioners cover nucleonic instruments, radiation protection monitors and process instrumentation.

8.5.3.2.2 Post Accident Mitigation/Surveillance Devices

The following post accident mitigation/surveillance devices are included:

a) CCTV in areas where there is a risk of radiation exposure

b) Communication system in areas where there is a risk of radiation exposure

c) PAM area radiation monitors around the reactor pool area and in the Basement

8.5.3.3 Environmental Conditions

The PAM system is designed to withstand the conditions of temperature, pressure and humidity that are found in normal operation conditions and post accident.

The PAM system is designed to withstand the design bases seismic event and all equipment is qualified to Class 1E requirements based on IEEE.

8.5.4 Post Accident Monitoring System Design Evaluation and Conformance Analysis

8.5.4.1 Conformance to General Requirement

8.5.4.1.1 Conformance to General Requirements 1 and 2

Requirement 1: Provide information to operators to indicate whether plant safety functions are being accomplished.

Requirement 2: Indicate the successful operation of individual safety systems.

The system fulfils its functional requirements by reliably monitoring a selected set of parameters. The selected monitored parameters indicate, in case of a DBA, if the corresponding plant safety functions are being accomplished.

a) The reactor control rod bottom position parameters indicate success or failure of the FSS. In addition, information about reactor neutron flux is provided to the operator.

b) The D_2O storage tank level parameter indicates success or failures of the SSS.

c) Water level in EMWS storage tanks together with the pool water level for the EMWS emergency level parameter indicates success or failure of the EMWS.

d) Isolation valves and vent valve positions, together with the containment pressure valves, indicate the success or failure of the Reactor Containment.

e) The diesel parameters indicate the success or failure of the Standby Power System.

f) The parameter of the ECC Ventilation and Pressurisation System provides indication that the ECC environment is habitable.

8.5.4.1.2 Conformance to General Requirement 3

Requirement 3: Alert operators to take safety actions for initiating a system function that is not automatic.

All monitored parameters were selected to indicate whether or not the corresponding safety functions are being accomplished. Table 8.5/1 shows a list of PAM system monitored parameters. As the PAM system is a monitoring system, mitigation actions are required from the operators. When an accident condition exists, PAM parameters alert operators to initiate the necessary safety functions that will mitigate the consequences of the accident. Some PAM parameters directly indicate that a given system has not performed its safety function properly and that an operator action is necessary, as in the case of failure of the containment isolation where operators can manually close the isolation valves. In other cases, the manual operations that can be done to mitigate accident consequences are not directly determined by the monitored parameter state and may depend on the state of a set of safety parameters in which case plant personnel decide which actions are pertinent.

8.5.4.1.3 Conformance to General Requirement 4

Requirement 4: Indicate to operators when barriers to fission product release have the potential for being breached or have been breached.

The PAM system monitors several parameters associated with radiological protection of operators and the environment.

A determination of reactor pool top gamma activity will determine the risk for operators, indicating when the protection provided by the pool water column is inadequate.

The PAM system monitors the gamma activity in the Basement to detect activity produced by leaks.

A determination of stack particulate, iodine and noble gas activity informs operators that the barrier to fission products, provided by the containment isolation system, has been breached and allows the operators to prevent product release to the environment by initiating corrective actions.

8.5.4.1.4 Conformance to General Requirement 5

Requirement 5: Determine the magnitude of release of radioactive materials.

The PAM system monitors several parameters associated with radioactive material

release. Measurements of stack particulate, iodine and noble gas activity allow the operators to determine the magnitude of released radioactive materials to the environment through the stack.

8.5.4.1.5 Conformance to General Requirement 6

Requirement 6: Redundancy will be provided so that undetected failures do not prevent the system functioning.

To comply with the requirement of reliability, the PAM system uses redundancy in a wide range of levels, from the high system-level to the lowest level of sensors, units and components. The PAM system is designed so that all parameters are measured by two independent redundant measurement channels. Both channels are physically separated in a way that ensures common cause failures of the system can be neglected. The PAM itself is a dual redundant system composed of two trains. In addition, the PAM system is supplied by two redundant UPSs, one per train. All subsystems are designed to accomplish their monitoring function following all DBA. Undetected single random failures are adequately controlled through system redundancy thus assuring that the system will properly perform its safety actions.

8.5.4.1.6 Conformance to General Requirement 7

Requirement 7: Multiple sets of equipment that cannot be tested individually will be considered as not being redundant.

The two redundant trains of the PAM system are completely independent. Equipment belonging to one channel, even when repeated through that channel, is not considered as being redundant. In the case of testing a single component, the channel it belongs to will be disabled, meaning that all equipment of the same channel cannot be considered redundant. The alternate channel must remain fully functional for the two channels to be considered redundant.

8.5.4.1.7 Conformance to General Requirement 8

Requirement 8: Physical separation by distance, barriers or layout of reactor components will be provided to enhance the reliability of systems, in particular with respect to common cause failures.

To avoid common cause failures like fires or floods, adequate physical separation of the PAM trains is provided. The two redundant trains are designed according to IEEE where the required criteria to avoid common mode failures are presented. The Reactor Facility design incorporates the separation of trains by using enclosed cable trays. According to IEEE, the required minimum distance between enclosed trays is one inch, which is surpassed in this case by approximately a factor of five. Each redundant train is run to its dedicated room where all its corresponding instrumentation is located. 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 levels using risers, fulfilling the IEEE requirements.

8.5.4.1.8 Conformance to General Requirement 9

Requirement 9: All use of diversity of equipment in redundant trains will be identified and justified in the design documentation.

Although diversity is a useful tool to improve the reliability of systems, diminishing the possibilities of common mode failures, diversity was not applied to PAM system design. PAM system reliability stands mostly on its simplicity, double redundancy and hardwired

design.

8.5.4.1.9 Conformance to General Requirement 10

Requirement 10: Signals to the ECC and to the MCR will be hardwired for all designated post accident monitoring instrumentation.

As shown in Section 8.5.3, PAM instrumentation is based on hardwired technology. This applies to all signals to the ECC and to the MCR.

8.5.4.1.10 Conformance to General Requirement 11

Requirement 11: Outputs from the PAM system to the RCMS will be isolated.

Several parameters monitored by the PAM system are shared with the FRPS, SRPS and RCMS. The PAM system is electrically isolated from other systems by the input and output modules. These modules contain electrical de-coupler devices, such as relays or transformers, to enable the transmission of signals to the PAM consoles located in the MCR and ECC and to share information with the RCMS. The PAM parameters that are shared with the FRPS have their signals generated from different field devices or from different isolated outputs of a transmitter. This is the case for the containment valves positions, wide range log flux, pool open end activity and stack activity parameters. PAM parameters shared with the SRPS have signals that are transmitted firstly to the SRPS. The SRPS then transmits an isolated output, from the output module to the PAM input module, which also provides isolation. This applies to the control rod down position and the reactor pool level parameters. All PAM signals, except those which are already transmitted by the FRPS and SRPS, are transmitted to the RCMS from the isolation output modules and are hardwired to the RCMS field unit.

8.5.4.1.11 Conformance to General Requirement 12

Requirement 12: PAM system equipment and components will be qualified under simulated worst case in-service conditions, and will be of proven technology, to provide a high degree of confidence in their operability under all DBA conditions.

PAM system equipment is qualified to withstand the worst case DBA conditions by type testing certification.

8.5.4.2 Conformance to Requirements from Standards

8.5.4.2.1 Conformance to Requirements from Standards 1 to 3

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

Requirement 2: Class 1E equipment will be qualified in accordance with the requirements set out in IEEE and relevant Australian standards.

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

All equipment and components of the PAM system are IEEE 1E qualified.

8.5.4.2.2 Conformance to Requirements from Standards 4

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 and the fire requirements of AS 3013.

All Class 1E instrumentation and control wiring is separated according to IEEE and AS 3000 requirements. Fire protection requirements are fulfilled according to AS 3013.

8.5.4.2.3 Conformance to Requirements from Standards 5

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

Interfaces are designed according to IEEE.

8.5.4.2.4 Conformance to Requirements from Standards 6

Requirement 6: PAM equipment will not cause any adverse electromagnetic interference which may affect other equipment. In addition, PAM equipment will not be adversely affected by any electromagnetic emissions from other equipment, that is, it will be compatible with all other reactor facility equipment.

PAM system equipment is qualified to ensure it will not cause electromagnetic interference to other equipment and will not be adversely affected by electromagnetic emissions from other equipment.

8.5.4.3 Conformance to Additional Requirements

8.5.4.3.1 Conformance to Additional Requirements 1

Requirement 1: Post Accident Monitoring instrumentation will be able to monitor the effectiveness of all ESF.

As mentioned in 8.5.4.1.1 (requirement 2), the selected parameters for the PAM system ensure the monitoring capability of the relevant ESF, allowing determination that the corresponding safety functions are being accomplished.

8.5.4.3.2 Conformance to Additional Requirements 2

Requirement 2: PAM instrumentation will indicate whether the reactor is shutdown.

As mentioned in the response to General Requirement 1, several parameters indicate the correct performance of shutdown systems. In addition, a measurement of neutron flux allows the operators to determine if the reactor is shutdown.

8.5.4.3.3 Conformance to Additional Requirements 3

Requirement 3: Systems that aid re-entry into contaminated areas following a DBA shall be classified as PAM systems. Such systems include CCTV and communication systems.

The PAM system includes a CCTV and a communication system to critical occupational areas. Both systems are qualified for DBA environmental conditions.

8.5.4.3.4 Conformance to Additional Requirements 4

Requirement 4: Traceable material and test certificates will be provided for components or equipment that is required for PAM functions.

All equipment for PAM functions is qualified according to Safety Category 1 requirements. Test certificates to the required codes and standards for PAM system equipment and components are provided.

8.5.4.3.5 Conformance to Additional Requirements 5

Requirement 5: Type testing under simulated in-service conditions will be provided for all

PAM equipment to provide the required confidence in such a way that equipment will perform its intended function during post-accident reactor monitoring.

Qualification results for all PAM equipment are provided.

8.5.4.3.6 Conformance to Additional Requirements 6

Requirement 6: Hardwired signals to the ECC and MCR will be provided for all designated PAM instrumentation. Isolated outputs from the PAM system to the RCMS will also be provided.

All signals to the ECC and to the MCR coming from the PAM systems are hardwired. In addition, outputs for all signals shared with the FRPS, SRPS, and the RCMS are electrically isolated.

End of Section

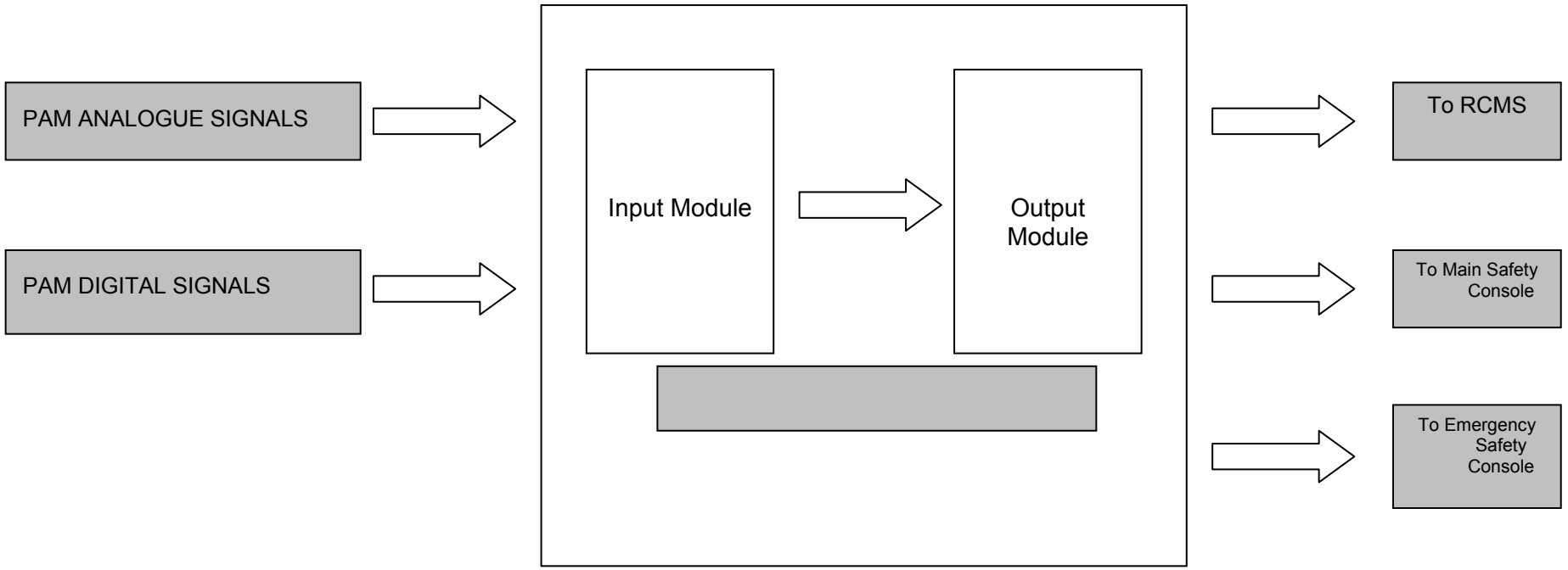
Table 8.5/1 PAM Parameters

Post Accident Monitored Signals (PAMS)
Reactor Core Water Level
Chimney Water Level
Pool Water Level (EVACUATION Trip)
Flap valve
Flap valve
Control Rod 1 Down Position
Control Rod 2 Down Position
Control Rod 3 Down Position
Control Rod 4 Down Position
Control Rod 5 Down Position
EMWS flow rate switch
EMWS tank level
Service Pool Water Level
D2O Storage Tank Level
Wide Range Log Neutron Flux
Reactor Pool Open End gamma activity
Reactor Hall Gamma Activity
Basement Gamma Activity (Process Room)
Stack Particulate activity
Stack Iodine activity
Stack Noble Gases activity
Reactor Pool Area Dose Rate
Reactor Building Containment Pressure
Containment Penetration Group Signal 1-1 Int.
Containment Penetration Group Signal 2-1 Int.
Containment Penetration Group Signal 2-2 Int.
Containment Penetration Group Signal 3-1 Int.
Containment Penetration Group Signal 4-1 Int.
Containment Penetration Group Signal 4-2 Int.
Containment Penetration Group Signal 5-1 Int.
Containment Penetration Group Signal 1-1 Ext.
Containment Penetration Group Signal 2-1 Ext.
Containment Penetration Group Signal 2-2 Ext.
Containment Penetration Group Signal 3-1 Ext.

Post Accident Monitored Signals (PAMS)
Containment Penetration Group Signal 4-1 Ext.
Containment Penetration Group Signal 4-2 Ext.
Containment Penetration Group Signal 5-1 Ext.
Evacuation
Reset Evacuation
ECC Ventilation and Pressurisation System
Diesel Generator
Diesel Generator Fuel Level
SAS Doors Inner
SAS Doors Outer

End of Tables

Figure 8.5/1 Post Accident Monitoring System Block Diagram



8.6 REACTOR CONTROL AND MONITORING SYSTEM

8.6.1 Introduction

The RCMS is a distributed, computer-based, high-availability system which reads all plant and reactor information and presents it to the operator at MCR, ECC, local workstations and local supervision centres. It enables reactor control, process command and overall data-management.

These systems cover all necessary automatic and manual functions to operate and monitor the facility in normal conditions, and to ensure that safety actions are executed under interlock conditions or when limits are exceeded.

From a safety perspective, the RCMS is a safety-related system (Safety Category 2). In all cases, the FRPS and SRPS have priority over the RCMS.

The RCMS, FRPS and SRPS are functionally, physically and electrically independent. FRPS and SRPS signals are only sent to the RCMS without feedback using Class 1E qualified isolation devices. The RCMS does not perform any Safety Category 1 functions.

The RCMS is a reactor control, instrumentation, monitoring, display, alarm and warning system that serves the normal operating requirements of the reactor plant including:

a) Reactor plant open and closed loop control systems.

b) Reactor control and monitoring instrumentation, including isolated inputs from the FRPS, SRPS and PAM.

c) MCR and ECC reactor operator control and monitoring workstations, control and indication panels and instrumentation.

d) Historical data storage and retrieval system.

e) Engineering, development, diagnostics and maintenance system to maintain and upgrade the system.

f) Redundant and separate reactor control and information data networks.

The RCMS complies with applicable ISO and IEEE standards.

The RCMS incorporates computer-based reactor operator control and monitoring workstations. Workstations are provided for the MCR, ECC and other specific locations.

RCMS computer devices and equipment are located, where possible, such that they are protected from the effects of DBA that could adversely affect their performance.

The RCMS is equipped with a dedicated redundant Local Area Network (LAN) system. No connection exists to the ANSTO site LAN system.

8.6.2 Design Requirements

8.6.2.1 General Requirements

The RCMS will meet the following functional requirements:

1. To control the plant, keeping the reactor parameters within operational limits without reaching safety limits. This includes data gathering, processing and displaying of information on plant status to the operator to give early warning on plant deviation from normal operation to start control and corrective actions.

2. To control the reactor core reactivity during operational states.

The following requirements assure RCMS simplicity:

3. Low number of hardware components within the system, with low diversity of types.
4. Simple interconnection between system components.
5. Low number of software components due to the use of similar platforms on each processor.
6. Low software complexity due to the reduced number of communication paths between software components.
7. Processor communication will be based on a horizontal logic structure (identical hierarchy level).

The following requirements assure RCMS reliability:

8. The system will have the capability to reach operational requirements with low error rate due to the structured development methodology and intensive verification and validation testing.
9. Highly reliable hardware components.
10. The functions of the system will be permanently distributed among the different units or processors.
11. The system database will be divided and distributed among all processors.

The following requirements assure RCMS availability:

12. The RCMS communication network will be implemented with redundancy.
13. Redundant control units will be provided.
14. Redundant power supplies will be provided on control units to ensure high availability.
15. The RCMS is supplied electrical power from a UPS.
16. A required overall RCMS availability greater than 99.9%.
17. Use of redundant processors and power supplies on units where it is necessary to fulfil availability figures.

The following requirements simplify RCMS maintenance:

18. The RCMS will be designed to facilitate maintenance of hardware components by replacement. The RCMS will be designed to be modular so that board replacement can be done with the system on-line, with only temporary local function degradation.
19. Standardisation to minimise the number of active components with spare active components and the required diagnostics to detect a problem.
20. The RCMS software will include modules to automatically detect errors in most of the runtime processes, including processing and communication modules.
21. Maintenance will be eased by the low diversity of hardware components.
22. The capability will be provided for on-line replacement of I/O modules, rack power supplies and control processors.

8.6.2.2 Requirements from Codes Standards

1. The control system will comply with applicable ISO and IEEE standards.

8.6.2.3 Additional Requirements

1. The control system will incorporate facilities for controlling:
   a) all closed loop controls, for example: reactivity, temperature etc;
   b) All open loop controls, such as starting or stopping of the reactor facility's components.
2. The control system will incorporate computer-based reactor operator control and monitoring workstations. Workstations will be provided in the MCR and ECC.
3. Data storage and retrieval systems will be provided for continuously logging of important reactor facility equipment status including analogue parameters, alarms, operator actions and reactor facility process and control system faults. Redundant storage devices and suitable data handling/logging software will be provided to ensure that mandatory records of all the reactor facility operations are automatically gathered and stored.
4. All microprocessor based control systems and equipment will be located, as far as possible, such that they are protected from the effects of a DBA that could adversely affect their performance.
5. The reactor control system will be equipped with a dedicated LAN system.
6. The control system will have sufficient redundancy to ensure that no single point of failure exists and that the overall system availability is met.
7. The control system will be equipped with dual redundant processor units.
8. The switchover from the failed to the healthy redundant unit will be automatic and seamless.
9. Separated inputs and outputs will be provided for associated duty and stand-by plant whenever it is practical. That is, they will be connected to separate I/O modules and power supply circuits etc.
10. The control system will ensure that failure of any single point on a multiple I/O card has no effect on the other points on that card.
11. The memory update of control processor returned to service after being taken offline or after a failure will be automatic.
12. The RCMS availability will be greater than 99.9%.
13. The availability of the installed control systems will be tested after final commissioning and before practical completion.
14. The reactor facility control system will have sufficient dedicated resources including: memory, processor speed and network bandwidth etc to perform the control functions, point scanning, online diagnostics and other requirements without exceeding 40% of system resources under worst case conditions.
15. A minimum of 20% spare carded, installed and terminated I/O points will be provided at the time of practical completion for each of the reactor facility control system's input-output cubicles.
16. The RCMS input and output cubicles provide for an expansion capacity in addition to

the installed spare capacity. A minimum 20% spare capacity will be provided for all aspects of the control system.

17. Expansion capability will be provided such that I/O modules, internal cubicle wiring, I/O cards, signal interfacing or conditioning equipment and running of cables can be added or changed without having to upgrade any processors, operator work station hardware or software, power supplies or cubicles.
18. Operator workstations will be provided to centralise the task of controlling and monitoring the reactor plant. They will communicate with the reactor control and monitoring system and provide the interface between the operator, control functions and the plant.
19. Operator workstations will be provided to represent the status of the plant in a modern, graphical environment. An open systems architecture employing state-of-the-art hardware and software including operating system technology will be provided.
20. Operator workstations equipped with keyboard, mouse and/or touch screen etc will be provided to allow the operator to navigate and interact with the graphics screens as well as perform data entry operations.
21. Multiple 48cm or larger, colour Visual Display Units (VDU) for the display of operator information in the MCR will be provided.
22. An arrangement whereby all colour Visual Display Units are capable of displaying all reactor information will be provided.
23. A minimum of three colour Visual Display Units for the ECC with the capability of displaying all reactor information will be provided.
24. Operator workstations will include a warning and alarm system.
25. Operator workstation displays will incorporate a form of data quality coding (for example, colour coded data displays) so that a judgement can be made by the operator about the reliability of the information being presented on the screen. The data quality indication system will also cover computed parameters, which may rely on the status of more than one data point.
26. The maximum time lag will be no greater than three seconds for a screen display or window to be updated when selected, under the worst possible computer and network loading conditions.
27. The maximum time lag will be no greater than two seconds for a screen to update any variable change under the worst possible computer and network loading conditions.
28. A dedicated engineering workstation will be provided to allow screen and database development. It will also allow maintenance, testing and diagnostic checks on control systems, networks and peripherals etc to be carried out.
29. Maintenance work will be able to be performed from the engineering workstation on the control system, database and graphic screens etc while the system is operational and without affecting online operation. MCR and ECC workstations will have priority for control at all times.
30. The control system will be able to down load database information as well as update graphical information while the system is being used without affecting normal operation.

31. The control system will be able to use relational database search techniques to allow for engineering analysis of real-time, historical/archival and database parameter information.
32. No limits will be placed on the ability to expand the size of the database and the number of graphical screens developed for display. All the graphical and database editing software will be included with the engineering workstation.
33. The control system will be able to save all its database points at the same rate as their respective scan rate and time-stamped with the scanned time. Archiving of data will be automatic to a suitable medium (magnetic tape, optical disc etc). A warning message to operators will be provided when the archive medium is at 75% and 90% of capacity.
34. Scanning of all sequence-of-events inputs following a change of state will be provided. Such inputs will be time-stamped (at the control system or associated sequence-of-events hardware) within 5 ms of the time of the occurrence of the event.
35. Fast access to short term (up to 12 months) historical data will be provided.
36. A long term archive storage medium will be provided which is easy to load and operate and is convenient to store. It will be of a suitable capacity to hold at least one year's information.
37. On-line dual redundant historical and archival data storage will be provided.
38. Interfacing and signal-conditioning equipment to instrumentation, field devices, switches, actuators, motors etc, will be provided to enable open and closed loop control and monitoring of the reactor facility.
39. Redundant serial communication field buses will be provided for the connection of all Safety Category 3 control and monitoring instrumentation signals to the RCMS.
40. The reactor protection and shutdown systems will be equipped with serial communications capabilities, unidirectional, send only, data interfaces to allow the reactor protection and shutdown systems to send data to the RCMS. All interconnection of reactor protection, shutdown and ESF signals to the RCMS will be via appropriate isolation devices to ensure the complete separation of Safety Category 1 from Safety Category 2 and 3 systems.
41. LAN interface hardware (for example isolation gateways) and software will be provided to enable communication with other systems such as the BMCS network. This will provide remote access facilities to selective data from the ECC such as for example following an evacuation.
42. All hardware and software required for configuring and maintaining the network and networking interfaces will be provided.

8.6.3 Reactor Control and Monitoring System

8.6.3.1 Architecture

The system comprises the MCR console and supervision desks, the ECC console and supervision desks, local supervision centres, processing hardware and software, wiring and networking and plant instrumentation. Dedicated workstations are included for the Radiation Monitoring System (RMS) and Facilities Control and Monitoring System (FCMS).

The RCMS is a distributed computer-based system with an open architecture of three hierarchical processing levels:

Supervision level

Control level

Field level

And three communication levels:

Supervision communication network level

Control communication network level

Field communication network level

The RCMS possesses the following units:

a) Supervision Units (SUs): These units which run the man-machine interface are used for reactor process supervision, command and plant data recording and management. These units are located in the MCR console, ECC console and in the local supervision workstations and desks.

b) Control Units (CUs): These units are used to collect and centralise plant data from all field units, to execute overall operational control algorithms and to output all actuation signals corresponding to control loops.

c) Field Units (FUs): These units are within the boundary of the system and constitute the link between CUs and intelligent devices, sensors and actuator devices. Input data are acquired from plant sensors and processed here before sending the information to upper levels in the hierarchy. Plant output data generated in a CU is sent to the appropriate FU and then to the appropriate plant actuators or intelligent devices.

The RCMS possesses three dedicated communication networks or LAN that are responsible for data link communication between the different processing levels. Each unit is treated as a node into the LAN system that it is connected to. The three networks are:

a) Supervision Network: This LAN performs the data link connection between SUs and the Control Network. Its main function is to distribute information and supervision data.

b) Control Network: This LAN performs the data link communication between CUs and is connected to the Supervision Network and the Field Network. Its main function is to distribute monitoring and control data.

c) Field Network: This individual LAN performs the data link communication between each CU and a set of FUs. Its main function is to distribute local monitoring and control data.

The Supervision, Control and Field Networks are physically redundant.

8.6.3.1.1 Supervision Level

All man-machine interactions between operators and the RCMS take place at the supervision level. This level includes displays, controls, and operator support interfaces to link operating staff with the RCMS.

Supervision level functions include: alarm presentation, plant status visualisation through

various displays, operator notification of transients, operations or mode selection, and manual equipment control (pumps, valves, etc.).

There are two operating modes in the supervision level: interactive and monitoring mode. In the interactive mode, all functions and supervision capabilities for start-up, operation, maintenance and refuelling are available. Within this mode there are various levels of access to differentiate between operator tasks and engineering tasks. In the monitoring mode displays can only be viewed.

The SUs implement all information management functions, such as historic database update, alarm generation and operations sequences.

The RCMS can also access safety parameters from the RPS to provide the operators with safety system status information. Safety settings cannot be changed from the Sus.

The communication links with the Facilities Control and Monitoring System takes place at this level. This connection is implemented by means of an isolated gateway and fibre optic cable link.

The supervision level uses a highly reliable duplicated supervision network for communication between SUs.

8.6.3.1.2 Control Level

Reactor plant process control functions take place at this level.

Redundant CUs, are responsible for data collection and transmission, control algorithm execution, process interlocks, health verification, reactor state determination and control states transition.

Both CUs work in a redundant fault tolerant configuration. While one CU acts as the operating unit the other remains in a hot standby state. The hot standby CU continuously checks the operation of the duty CU. If the hot standby unit detects that the duty unit has deviated from the normal functioning mode it immediately takes control and disables any control function from the failed unit.

Automatic and manually controlled output parameters (driving signals for process actuators) are handled at this level. Each CU has the capability to send command signals to the FU connected to it. These output values are also stored in the real-time database for that unit.

The connections from the FRPS are made to the RCMS at the control level except Nucleonics Instrumentation, which is made at the Field Level.

The control level uses a highly reliable duplicated network for communication between CUs.

8.6.3.1.3 Field Level

The field level comprises the FUs, all reactor plant data acquisition, primary data handling processes, execution of local interlock algorithms and final generation of actuator commands.

Signal conditioning takes place at this level for all acquired signals through field sensors, and for all actuation signals (field actuator excitation). This conditioning includes scaling, linearisation and local validation.

Active or passive sensors carry on physical process measurements. Intelligent devices can be either smart sensor/actuators or small programmable logic controllers.

The field level uses a highly reliable duplicated network for communication between FUs.

The sensors and actuators that are connected to the RCMS are safety-related sensors (Safety Category 2) or non-safety sensors (Safety Category 3). They are typically not redundant and their signals are of different types, for example: on or off, digital or analogue. These sensors can be connected directly to the FU conditioning modules or through a signal transmitter.

In the case of intelligent signal transmitters, they access the FU via a communication channel. The use of intelligent or smart sensors and actuators has the advantage of self-calibration and self-diagnostic features and provides this information at the supervision level.

8.6.3.1.4 Modularity

The RCMS is a modular system both in software and hardware that allows simple handling of possible configuration variations, modifications, replacements and extensions.

The RCMS architecture allows for functional divisions to be made between different subsystems, retaining an integrated supervision method.

8.6.3.1.5 Redundancy

The RCMS includes sufficient redundancy to ensure that no single point of failure exists and the overall system availability is met. For that purpose the system possesses:

a) dual redundant network at the Supervision Communication level

b) dual redundant network at the Control Communication level

c) dual redundant network at the Field Communication level

d) dual redundant power supply in CU

e) dual redundant power supply in the FU

f) dual redundant CU control processors

g) dual redundant equipment for historical data storage

All control processors are dual redundant and configured in fault tolerant mode. The redundant processor units will have an automatic and seamless changeover from the failed to the healthy processor unit.

The RCMS does not perform any Safety Category 1 protection or trip functions. However in the case of a fault or malfunction which affects normal operation, an isolated hardwired trip request signal is sent to the RPS requesting reactor trip.

The input and output signals associated with duty and standby plant are kept separated wherever practical. This is fulfilled by the connection of these signals to separate I/O modules.

The design of input and output points and the selection of components consider the use of isolated I/O modules, independent I/O fuses and separated field power supplies to avoid a failure of any point on a multipoint I/O card having an affect on other points of the same card.

8.6.3.1.6 Availability

The RCMS availability will be greater than 99.9%.

The availability of the installed RCMS will be tested after final commissioning and prior to

the practical completion stage.

8.6.3.1.7 Spare Capacity

The RCMS includes sufficient dedicated resources including memory, processor speed and network bandwidth to perform the control functions, point scanning, on-line diagnostics and other requirements without exceeding 40% of system resources under worst case conditions.

The RCMS input and output cubicles will include a minimum of 20% spare installed and terminated I/O points at the time of Practical Completion.

The RCMS input and output cubicles provide expansion capacity in addition to the installed spare capacity.

A minimum of 20% spare capacity is provided for all aspects of the RCMS

The expansion capability may require additional I/O modules, internal cubicle wiring, I/O cards, signal interfacing or conditioning equipment and running of cables, but does not require upgrading of any processors, operator workstation hardware or software, power supplies or cubicles.

8.6.3.1.8 Control Room Workstations

The systems SUs are the operator workstations that centralise the task of controlling and monitoring the reactor plant. The SUs provide the interface between the operator, the control functions and the plant.

SUs represent the status of the plant in a graphical environment. The RCMS uses an open system architecture employing state-of-the-art hardware and software, including operating system technology.

SUs are equipped with touch screens, keyboards and trackball to allow the operator to navigate and interact with the graphic screens as well as perform data entry operations. The MCR console and ECC console consist of a number of SUs with high quality industrial colour monitors.

All SUs include a warning and alarm system that is managed by the alarm management system. During reactor operation one SU at the MCR is devoted to displaying all the reactor plant alarm information and to interact with operators while the remaining SUs are able to display alarm information when requested.

8.6.3.1.9 Engineering Workstation

The RCMS has two dedicated SUs, the Engineering Workstations, for engineering functions. This unit allows maintenance, testing and diagnostic checks to be performed on the RCMS, networks and peripherals and also allow system level configuration such as screen and database development.

Maintenance activities include on-line testing and diagnostic checks on the SUs, CUs, FUs, communication networks and peripheral devices.

Configuration tasks are related with modification or changes in databases, control functions, graphic screens, historic data and reports, system access control, logic and interlock function, operational state conditions, alarm system and process supervision. All update tasks such as database information download and graphical information are carried out without affecting system operation.

Database search and query techniques are applied to allow engineering analysis of real time data, system parameters and historic files.

Maintenance and configuration software packages and all graphical and database editing software are included in the Engineering Workstation.

The system is designed to allow future expansion of the database and to increase the number of graphical screens to accomplish any future requirement or plant update or upgrade.

8.6.3.1.10 Reactor Control and Monitoring System Historical and Archival Storage

The RCMS historical data module saves all important system database points. Data can be saved at the same rate as their respective scan rate (scan rate is based on the acceptable industry standard at the time of procurement of the system) and time-stamped.

Archiving of data to a suitable medium (for example magnetic tape) is automatic. An operator warning message is provided when the archive medium is at 75% and 90% capacity.

All sequence-of-event inputs related with reactor parameters are scanned following a change of state and are time-stamped at the RCMS within 5 ms of the event. These events are stored in an intermediate buffer before being transferred for historical data recording.

The information is classified as short-term and long-term historical storage. The short-term (up to 12 months) historical storage facility is immediately accessible on the system.

Access to long-term archived data will require loading the appropriate storage medium. Long-term historical storage devices have the capacity to hold at least one year's information.

The RCMS includes a dual redundant storage device for all historical and archival data storage. Both devices operate concurrently.

8.6.3.1.11 System Interfaces

The RCMS is provided with interfacing and signal-conditioning equipment for instrumentation such as field devices, switches, actuators and motors to enable open and closed loop control and monitoring of the reactor plant.

The FRPS is equipped with digital communication capabilities to interface with the RCMS. This communication interface carries out data collection from the safety systems and the ESF in a uni-directional mode; sent only from the FRPS to the RCMS.

The RCMS has an interface to acquire SRPS and PAM data. This interface is hardwired and uni-directional. In addition, the SRPS and PAM output modules, which generate the signals fed to the RCMS, are qualified Class 1E isolation devices to ensure complete separation between the SRPS and PAM systems and RCMS.

The ECC console, in addition to the RPS and PAM consoles, is part of the RCMS and is connected to the supervision LAN system. The RCMS is responsible for data administration that is required in the ECC console.

8.6.3.2 Reactor Control and Monitoring Systems

8.6.3.2.1 Automatic Reactor Power Control System

The Automatic Reactor Power Control System (ARPCS) is implemented as a software module within the RCMS. This system is responsible for the regulation of reactor power

to within its setting limits, compensating for normal reactivity changes due to, for example, effects associated with temperature, xenon, target insertion/removal and fuel burn-up, and to perform power changes to new levels upon modification of the power setting.

The ARPCS has two inputs:

a) Wide Auto-Range Linear Instrumentation System

b) Linear Instrumentation System

The Wide Auto-Range Linear Instrumentation System is used to monitor the reactor neutron flux from source level up to 125% of reactor nominal full power level. It provides the neutron flux and flux rate to the Automatic Reactor Power Control System (ARPCS) to allow the automatic control of reactor power.

The Wide Auto-Range Linear Instrumentation System comprises a single neutron flux measuring channel: Wide Auto-Range Linear Channel. This channel provides a measure of the neutron flux over ten decades

The Linear Instrumentation System measures the effective core global power and is used as a complimentary system to the Wide Auto-Range Linear Instrumentation System for the power regulation function of the ARPCS.

The Wide Auto-Range Linear Channel provides a fast input to the ARPCS based on local flux measurement whereas the Linear Channel provides a delayed value of the core global power, sensitive to cooling flow.

The ARPCS can be overridden by operator manual control at any time.

8.6.3.2.2 Radiation Monitoring System

The Radiation Monitoring System (RMS) forms part of the RCMS, FRPS and PAM, providing all radiation monitoring functions for the Reactor Facility. The RMS provides continuous monitoring of processes involving potentially radioactive liquids and gases, as well as area and personnel monitoring inside the Reactor Facility. The RMS transmits data to the RCMS and also directly to the FRPS and PAM system consoles.

The RMS includes sensors, cabling, intelligent processing monitors and controlling software and communication protocols. All radiation surveillance tasks related to reactor operation are performed by the RMS. The RMS surveillance tasks include monitoring of liquid effluents and liquid streams inside the reactor (PCS, RSPCS and SCS included), air effluents at the reactor stack and at specific locations (namely Heavy Water Room and Chemistry Blue Lab), fuel integrity condition, area radiation monitoring (both gamma and neutron) and personnel contamination monitoring (walk-through monitors).

The systems of the RMS that form part of the RCMS, FRPS and PAM are detailed below. Dedicated RCMS VDUs are provided for the RMS displays in the MCR, ECC and the health physics office to display real time values, automatic alarming of abnormal releases or contamination events and automatic compiling, logging and integration of releases. Systems related to the FRPS and PAM include redundant detection units and the indications and alarms are presented on the RPS and PAM wall panels.

8.6.3.2.2.1 Liquid Systems Monitoring

The continuous on-line sampling of all potentially radioactive liquid streams inside the reactor facility is performed by the Liquid Monitoring System (LMS). This system consists

of three separate subsystems: Waste Streams Monitor (WASMO), Active Liquids Monitor (ALMO) and Secondary Water Activity Monitor (SAMO).

WASMO includes two gamma sensing heads directly connected to the waste water streams prior to delivery to the corresponding storage tank.

ALMO comprises two gamma sensing units directly connected to the Reactor and Service Pool Cooling System and the Primary Cooling System. These detectors are provided to monitor activity in the cooling water streams that may arise from damaged fuel or irradiation targets.

SAMO monitors the Secondary Cooling System for possible leaks in the heat exchangers that could lead to contamination of the normally non-active Secondary Cooling System water. SAMO consists of a gamma sensing head installed to achieve high sensitivity, as the activity levels are expected to be very low.

The three monitoring systems trigger local as well as remote alarms (via the RCMS) in the MCR and ECC if the authorised activity concentration level or activity concentration rate of the water exceeds the preset limits.

These systems are categorised as Safety Category 2

8.6.3.2.2.2 Liquid Effluent Monitor

The Liquid Effluent Monitor (LEM) provides local and remote alarms which provide warning if the radioactive liquids approach or exceed the authorised limits prior to and during tank discharge. Prior to discharge of the waste tanks the LEM monitors the tank contents through a recirculation line. In parallel with this operation, manual samples are taken to confirm the LEM readings. During discharge the LEM acts as an online monitor able to stop the discharge if the activity concentration being released is exceeding the authorised limit.

The system is categorised as Safety Category 2.

8.6.3.2.2.3 Failed Fuel and Irradiation Target Monitors

The operation principle of the failed fuel element monitor and the failed irradiation target monitor is based on the detection of neutrons.

The monitor uses a neutron counter to detect the presence of thermal neutrons emitted by fission products. In addition there is a fixed gamma monitor (ALMO) in series with each neutron counter as a backup.

These systems are categorised as Safety Category 2.

8.6.3.2.2.4 Monitoring of Gases

The Air Effluent Monitoring System (AEM) consists of four independent Particulate, Iodine and Gas detectors that monitor the stack discharge. Three sets of these are connected directly to the FRPS as part of the containment isolation function on stack releases reaching the safety setting. They are classified as Safety Category 1 and are designed to the requirements of IEEE Class 1E. The fourth monitor (AEMi) is used for routine stack emission monitoring and includes a gross Beta and gross Gamma detection channel as well as a spectrum analyser that enables the system to generate real time data regarding the isotopes and quantity released in stack emissions. This monitor is categorised as Safety Category 2.

8.6.3.2.2.5 Area Radiation Monitoring System

The Area Radiation Monitoring System (ARM) comprises both safety and safety related channels. Three FRPS monitors provide a reactor trip if radiation levels above the reactor pool exceed the safety setting. Two of the FRPS channels are also used for PAM indication. In addition to these, there are dedicated PAM monitors located in the reactor hall and in the Basement for aiding in accident analysis and re-entry operations. They are classified as Safety Category 1 and are designed to the requirements of IEEE Class 1E. The remainder of the area monitors are Safety Category 2 and are located to provide sufficient coverage for the area around the reactor and any area where radiation may be present.

Area monitors are detectors with local readout, lights and audible alarms. The PAM and RPS monitors are analogue units while the others are based on microprocessor technology.

8.6.3.2.2.6 Neutron Monitoring System

The Neutron Monitoring System (NMS) consists of a set of fixed radiation monitors able to measure the neutron dose rate in the Beam Hall for the purpose of protection of personnel. The system is based on a set of neutron detectors connected to a local dose rate indicator that can support two probes each. Dose rate is displayed at each probe location. Two neutron dose rate monitoring modules with two probes each are installed in the Beam Hall. The system is categorised as Safety Category 2.

8.6.3.2.2.7 Monitoring of Personnel

Two fixed portal monitors are installed in the Reactor Facility at the exits from blue areas on the main building entry level. Complementing these portal monitors is a set of portable monitors (not included within the RMS). These can be used as a backup in case of failure of a portal monitor and enables a detailed surveillance of the personnel exiting from contamination risk areas. The portal monitors can be operated alternatively in two different modes: walk-through and stop-count-go.

8.6.3.2.3 Vibration Monitoring System

The Vibration Monitoring System (VMS) is a system connected to the RCMS.
The VMS is designed such that automatic shutdown of equipment can be performed as a result of a vibration value that indicates a dangerous situation. Vibration monitoring is performed on all motors with a large rating. On-line monitoring is applied to the PCS pumps, the RSPCS pumps and the SCS pumps.

The VMS is designed to perform the following functions:

a) continuous indication
b) warning generation
c) alarm generation
d) shutdown of motors

The VMS is classified as Safety Category 2 system.

8.6.3.2.4 Facilities Control and Monitoring System

The Facilities Control and Monitoring Systems (FCMS) consist of the Irradiation

Facilities, Beam Facilities and Cold Neutron Source Control and Monitoring Systems. It also includes the Cold Neutron Source Protection System.

The instrumentation provided for Irradiation Facilities include neutron flux, rotational monitoring, coolant flow, pressure and temperature. The design of the systems is such that all instrumentation and computerised controls associated with all Irradiation Facilities is separated from the Reactor Control and Monitoring System. The design is based on a distributed computer system with high availability and independence. The FCMS is provided by the same vendor and has the same basic architecture as the RCMS. The RCMS and FCMS networks are connected by a fibre optic carrier band link.

Local control stations for Irradiation Facilities are located as close as possible to the loading stations. Separate programmable controllers in a distributed control system are used. Inputs from the beam shutter positions to the Reactor Control and Monitoring System for indication are provided. Additionally an indication of primary and secondary beam shutter position is provided on large and easy to read local annunciators near each port to alert staff.

Separate instrumentation and computerised controls for the Cold Neutron Source (CNS) are provided. The CNS local controls are located as close as possible to the CNS equipment.

The FCMS is designed with the same level of performance as the RCMS. Testing of the system will meet the same standards as the RCMS. 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.

The FCMS is categorised as Safety Category 2

8.6.3.2.5 Simulator Training System

The Simulator Training System for the Reactor Facility allows operators to familiarise themselves with the systems, screen displays and alarms etc without the need for a fully replicated MCR. The Simulator Training System is designed to realistically replicate the Reactor Facility performance characteristics including process parameters. The following design features have been incorporated:

a) Under transient conditions, the simulated parameters do not violate physical laws.

b) Transient accuracy is such that alarms and trips will not occur during simulation if they do not occur on the real plant. Alarms and trips are identical to the real plant.

c) Trend curves of simulated plant parameters follow the same trends as their corresponding real plant parameters.

d) Software development tools and documentation are provided which ensure that any future changes in the real plant can be appropriately modelled on the simulator.

e) The simulator computer has availability greater than 99.9% and has the same testing requirements as the RCMS.

The Simulator Training System has the capability to simulate all aspects of all reactor DBA, refuelling and normal plant operations.

8.6.3.3 Reactor Control and Monitoring System Functional Overview

The RCMS performs several functions that are described in the following section.

8.6.3.3.1 Plant States

All reactor plant operational states and the transition between states are controlled and supervised through the RCMS.

The Reactor States are:

Power

Physics Test

Shutdown

Refuelling

The system continuously checks plant process conditions to identify reactor state and checks the logic conditions for state transitions.

The RCMS guides the operator by means of an administrative control and logic condition display to fulfil the conditions to perform reactor plant state transitions.

8.6.3.3.2 Automatic Reactor Limitation System

The Automatic Reactor Limitation System has limit control mechanisms that protect the plant from operational perturbations that could occur if operational parameters were allowed to be outside predetermined ranges.

The Automatic Reactor Limitation System is designed using a layered approach of protective actions culminating in a full Bank Insertion. The safety settings for these actions are set conservatively compared to the RPS safety settings such as to catch any undesirable plant behaviour before reaching the RPS Trip Safety Settings. The Automatic Reactor Limitation System comprises three protection actions that are designed to be affective in a layered approach in the order given:

1. Control Rod Withdrawal Interlock (CRWI)
2. Power Reduction (PR)
3. Bank Insertion (BI)

The Control Rod Withdrawal Interlock protective action prevents the ARPCS from raising any Control Rod while the initiating conditions are active. The initiating conditions for the Control Rod Withdrawal Interlock are based on high neutron flux and neutron flux rate parameters.

The Power Reduction protective action causes a reduction in reactor power level to 80% of the current reactor power level.

The Bank Insertion protective action is independent of the ARPCS and inserts all five Control Rods simultaneously from their current location at maximum controlled insertion velocity using the control rod drive motors until all Control Rods are fully inserted. This action essentially brings about an automatic reactor shutdown before the Reactor Protection System is called upon.

8.6.3.3.3 Plant Control

Reactor operators have direct and simple access to the control commands for different plant processes.

Software modules included in the RCMS handle regulating control loops, interlocking logic, execution of logical sequences and manual control commands.

Individual control commands are generated by the operator via supervision units and are

sent to field units that activate the plant actuators.

8.6.3.3.4 Manual Reactor Power Control System

The RCMS includes a Manual Reactor Power Control System function that allows operators to manually control the movement of each control rod one at a time through a dedicated Module 4 – Control Rods on the Main Control Room main console. Module 4 consists of a hardwired panel of control rod commands including control rod raise and lower push buttons and an associated Visual Display Unit (VDU).

Using the Manual Reactor Power Control System the operator can accurately monitor and control the position of each control rod. Feedback information is presented in numerical and graphical form on the VDU. All commands generated by operators through the Manual Reactor Power Control System override any signal generated by the Automatic Reactor Power Control System. Use of any Manual Reactor Power Control System command automatically disconnects the Automatic Reactor Power Control System.

8.6.3.3.5 Control Rod Functions

Operation of the Automatic Reactor Power Control System requires that of the four Safety and Compensating control rods; two control rods are selected as Safety only while the remaining two are selected as Compensating control rods or control absorbers. The two control rods selected as control absorbers can be used alongside the central regulating control rod in the ARPCS to control reactor power. The position of the two Safety control rods is kept fixed during normal operation.

The assignment of control rod function and control rod movement is continuously supervised by the RCMS that monitors sequences and movements of control rods with interlock logic also provided.

Special functions for testing control rod insertion time are implemented. This allows periodic measurement of the drop time of each control rod under the same condition as a Trip 1.

The CRD reset function (initial positioning and control rod movement system ready) after a Trip 1 event is performed by the RCMS.

8.6.3.3.6 Alarm Management System

The RCMS includes an advanced Alarm Management System that presents all information related to reactor plant system alarm status.

The Alarm Management System has the capabilities for detection, prioritisation and presentation of real-time process alarms and provides the operator with understanding of the current plant state without an overload of presented information.

The Alarm Manager System detects alarm activation and clearance at different levels. Alarms are generated on digital, analogue or computed parameters. They can be categorised according to process requirements:

a) alarm priority according to alarm relevance

b) alarm masking on cause-effect relationship

c) chronological alarm storage

d) alarm differentiation by means of colours

The system provides several notifications means to alert the operator on an alarm condition such as; message presentation on monitors, indicators on console, graphical presentation in system context and audible indications.

The operator must acknowledge all activated alarms. An explanatory message is available for each alarm.

The use of different colours and attributes in the display information allows the operator to assess the plant status clearly.

All alarm condition events, alarm clearing or acknowledge actions are stored chronologically along with the time of occurrence and relevant additional information in the historical database.

Plant alarm status can be displayed on screen panel graphics. Each graphic shows a summary of the current alarm state of a particular plant system. In that way a top-down approach to alarm presentation is used.

Detailed alarm information about the related process is shown on the alarm pages. On each alarm page events are presented in chronological order displaying: message descriptions, alarm tags, trigger or normalisation times, alarm state conditions and relation to safety.

The Alarm Management System has dedicated printers that are devoted to producing hard copies of all requested alarm events in a chronological order. The printers print messages with alarm information including date and time, safety importance, trigger, acknowledgement and clearance events.

A VDU at the MCR console is dedicated to managing alarm information. Its primary functions are system alarm status display, detailed alarm information display and the main interface that enables the operator to perform the associated alarm tasks.

8.6.3.3.7 Report Generation

The RCMS has a printed report generator management module. This module can generate spreadsheets with fixed text along with process and operators data.

Report generation can be triggered by operator request or periodically by an automated procedure at specified time intervals, for example at shift rotation or experiment completion.

8.6.3.3.8 Event Recording

The system has the capability to record events produced during control and supervision of different plant processes. They are stored chronologically in the database.

8.6.3.3.9 Historic Data Recording

The RCMS includes a Historic Data Recording System that generates an historic database including safety, safety related and non-safety data.

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, plant parameters and plant and control system faults.

The main data recording methods available are at periodic frequencies (at scanning rate or lower), value or state changes exceeding the dead band and events. A redundant storage device is used in order to ensure that all records are automatically stored in the case of one device failure. Redundant storage devices and suitable data handling software are provided to ensure that records of all reactor plant operations are

automatically gathered and stored.

All selected archived data are automatically saved on a permanent medium. The system generates messages to the operator warning when the medium capacity is almost full.

The system has short term historical data storage saved in the system for fast data retrieval. To work with long term historical data, the data is loaded from the permanent storage medium.

8.6.3.3.10 Supervision Interface

The system provides the operator overall plant status information by means of several diagrams and tables (for example mimics, histograms, graphs and alphanumeric and audible information) and time trend graphics of selected parameters (i.e. reactor power, rod position, neutron flux and temperature).

The system supervises operator actions during component manipulation such as valve opening or closing, pumps start-up or shutdown, parameter or safety setting changes, command sequences and provides guidance for operators.

The RCMS displays information in the MCR and ECC to assist reactor operators during normal or abnormal conditions, providing them with clear and concise information. This information is arranged hierarchically in the VDU according to functionality and priority.

8.6.3.3.11 On-line Help

The system has the capability to display documents on line to help operators with screens' symbols interpretation and system navigation.

8.6.3.3.12 Status and Self Diagnosis

The RCMS has a set of routines to verify overall system performance and to diagnose its functional status.

Self-diagnostic software detects and alerts the operator of hardware faults and enables easy identification and replacement of failed components. Components or units with online replacement capability can be replaced without disrupting system operation.

The RCMS is continuously self-checked and an active healthy signal is generated. In the case of a fault or malfunction affecting normal operation, the signal is lost and a trip request signal is generated by the FRPS for a reactor trip.

8.6.3.3.13 Access Control

The purpose of the Access Control System is to avoid unauthorised personnel from accessing the RCMS and performing control activities that could affect reactor security. An access control level is assigned to each person of the operational staff according to their duties. User identification and passwords are requested on each Supervision Unit, for login or logout functions and to perform restricted activities.

8.6.3.3.14 Reactor Control and Monitoring System Performance

System resources allocated to the RCMS possess the necessary capabilities to fulfil all functions and tasks under maximum system load.

Under the worst operating conditions (maximum load) the RCMS never exceeds 40% of system resources.

8.6.3.4 Reactor Control and Monitoring System Software Development Verification and Validation Process

A verification and validation process is provided to ensure that the RCMS meets its functional, performance and reliability requirements. Differing techniques are employed during the verification and validation process according to the type of software and the stage of the development process. All systems are verified at the unit and system level, and validated at the system level only. Verification is applied from the beginning of system development in order to ensure maximum efficiency. The amount of verification to be performed depends upon the importance of the system to plant safety. All development work is reviewed by individuals or groups not involved in carrying out the development work. The adequacy of the software including development tools, inputs and outputs is verified or validated by individuals or groups other than those who originally performed the work.

8.6.3.4.1 Software Verification and Validation Plan

All Software modules are compliant with the Software verification and validation plan. Confidence is ensured by means of peer reviews along the software life cycle and testing of the software at different stages of the development. Review participants have system, interface, sub-system hardware and software backgrounds from INVAP together with designated ANSTO personnel. The reactor instrumentation and control system reviews include software reviews that comprise:

a) Software Requirements Review

b) Software Development Review

c) Implementation Review

d) Validation Review

During each phase of system development test plans for the next phase were developed. As a result, the test plans have been captured in the verification process. See Tables 8.6/1 through 8.6/7 for further details of the Verification and Validation Plan for the RCMS.

8.6.3.4.2 Verification and Validation Reports

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

The following verification and validation reports are generated:

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

   (i) Software Requirement Verification Reports
   (ii) Software Development Verification Reports
   (iii) Test Results
   (iv) Evaluation of New Constraints
   (v) Proposed Change Assessment

b) Anomaly Reports: Each anomaly detected by the verification and validation effort is documented as an Anomaly Report and is evaluated for its impact on the system.

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 contains 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

8.6.4 Conformance Analysis

8.6.4.1 Conformance to General Requirements

8.6.4.1.1 Conformance to General Requirement 1

Requirement 1: To control the plant, keeping the reactor parameters within operational limits without reaching safety limits. This includes data gathering, processing and displaying of information on plant status to the operator to give early warning on plant deviation from normal operation to start control and corrective actions.

The RCMS is a reactor control, instrumentation, monitoring, display, alarm and warning system. The adopted design serves the normal operating requirements of the reactor plant including:

a) Reactor plant open and closed loop control systems.

b) Reactor control and monitoring instrumentation, including isolated inputs from the FRPS, SRPS and PAM.

c) MCR and ECC, reactor operator control and monitoring workstations, control and indication panels and instrumentation.

d) Historical data storage and retrieval system.

e) Engineering, development, diagnostics and maintenance system to maintain and upgrade the system.

f) Redundant and separate reactor control and information data networks.

8.6.4.1.2 Conformance to General Requirement 2

Requirement 2: To control the reactor core reactivity during operational states.

A thorough explanation of the effectiveness of reactor core reactivity control by the RCMS can be found in section 8.6.3.2.1.

8.6.4.1.3 Conformance to General Requirement 3

Requirement 3: Low number of hardware components within the system, with low diversity of types.

Standardisation is a basic Reactor Facility design criterion. For the RCMS, where possible according to the safety criteria, the number of hardware components has been reduced to a minimum. Furthermore, wherever possible hardware components of the same type have been chosen.

8.6.4.1.4 Conformance to General Requirement 4

Requirement 4: Simple interconnection structure between system components.

The RCMS structure has a horizontal logic thus allowing for a simple interconnection structure between system components.

8.6.4.1.5 Conformance to General Requirement 5

Requirement 5: Low number of software components due to the use of similar platforms on each processor.

All processors use similar platforms thus minimising the number of software components according to the simplicity criterion.

8.6.4.1.6 Conformance to General Requirement 6

Requirement 6: Low software complexity due to the reduced number of communication paths between software components.

The number of communication paths has been minimised thereby reducing software complexity.

8.6.4.1.7 Conformance to General Requirement 7

Requirement 7: Processor communication will be based on a horizontal logic structure (identical hierarchy level).

Supervision, Control and Field levels are based on a horizontal logical structure where all components have the same hierarchical level.

8.6.4.1.8 Conformance to General Requirement 8

Requirement 8: The system will have the capability to reach operational requirements with low error rate due to structured development methodology and intensive verification and validation testing.

The RCMS development is organised following a structured development methodology to minimise the possibility of error. Appropriate validation and verification processes for each stage of the development are applied. See section 8.6.3.4 for the RCMS Validation and Verification Development Process.

8.6.4.1.9 Conformance to General Requirement 9

Requirement 9: Use of highly reliable hardware components.

All hardware complies with the reliability requirements. In the case of commercially available off the shelf components, conformance certificates are provided. In the case of INVAP manufactured hardware, tests are performed and the results reported to ensure the required reliability is achieved.

8.6.4.1.10 Conformance to General Requirement 10

Requirement 10: The functions of the system will be permanently distributed among the different units or processors.

Modularity has been a basic design criterion in the RCMS development. Both hardware and software components are modular allowing simple handling of configurations and modifications. Additionally the RCMS allows functional division in different but interconnected subsystems. Field Units are distributed physically and functionally. For further information see Section 8.6.3.1.4.

8.6.4.1.11 Conformance to General Requirement 11

Requirement 11: The system database will be divided and distributed among all processors.

The control database is distributed across the control processor level so that control software is relevant to the function of the particular processor.

8.6.4.1.12 Conformance to General Requirement 12

Requirement 12: The RCMS communication network will be implemented with redundancy.

There are three different communication networks that are implemented using double redundancy.

8.6.4.1.13 Conformance to General Requirement 13

Requirement 13: Simple redundant Control Units will be provided.

Control Units are used to collect and centralise plant data from the field units. In the RCMS and FCMS control processor pairs manage the complete data collection and transmission, control algorithms, reactor state determination and control states transition. Each unit works in a fault tolerant configuration: one operative and the other in a hot standby state. In case of a fault of the operating unit, a changeover in the task execution takes place from the operating unit to the standby unit.

8.6.4.1.14 Conformance to General Requirement 14

Requirement 14: Simple redundant power supplies will be provided on control units to ensure high availability.

CUs have redundant power supplies to ensure a high degree of availability.

8.6.4.1.15 Conformance to General Requirement 15

Requirement 15: The RCMS will be supplied electric power from a UPS.

The RCMS is fed power from a UPS. In case of failure of the normal power supply, the UPS guarantees the electric supply to the RCMS for sufficient time to start the support diesel generators allowing the normal performance of all safety systems without affecting RCMS availability.

8.6.4.1.16 Conformance to General Requirement 16

Requirement 16: A required overall RCMS availability greater than 99.9%.

The RCMS is designed to achieve an overall RCMS availability equal to or greater than 99.9%.

8.6.4.1.17 Conformance to General Requirement 17

Requirement 17: Redundant processors and power supply units will be used where necessary to fulfil availability figures.

All control processors are redundant. Rack power supplies are also redundant. The use of redundant processors and power supplies contribute to the availability requirement of 99.9%.

8.6.4.1.18 Conformance to General Requirement 18

Requirement 18: The RCMS will be designed to facilitate the maintenance of hardware components by replacement. The RCMS will be designed to be modular so that board replacement can be done with the system online, with only temporary local function degradation.

Modularity has been applied to all designs where possible. Modularity and the redundancy make online replacements a simple task that only temporarily affects local system availability without necessarily affecting system availability.

8.6.4.1.19 Conformance to General Requirement 19

Requirement 19: Standardisation to minimise the number of active components, the spare active components and the required diagnostics to detect a problem.

Standardisation has been a basic design criterion that has been applied to every system where possible. The use of standardisation within the RCMS allows for easier maintenance and diagnostics.

8.6.4.1.20 Conformance to General Requirement 20

Requirement 20: The RCMS software will include modules to automatically detect errors in most of the runtime processes including processing and communication modules.

The RCMS software has a set of routines that verify overall system performance and diagnose its functional status. The results are displayed to operators through SU alarms. For further information on RCMS self-diagnosis see Section 8.6.3.3.12.

8.6.4.1.21 Conformance to General Requirement 21

Requirement 21: Maintenance will be eased by the low diversity of hardware components.

See Section 8.6.4.1.3.

8.6.4.1.22 Conformance to General Requirement 22

Requirement 22: The capability will be provided for online replacement of I/O modules, rack power supplies and control processors.

See Section 8.6.3.1.5.

8.6.4.2 Conformance to Requirements from Codes and Standards

Requirement 1: The control system will comply with applicable ISO and IEEE standards.

All equipment and components of the RCMS are qualified to Safety Category 2 requirements and meet the requirements of ISO and applicable IEEE standards.

8.6.5 Conformance to Additional Requirements

8.6.5.1 Conformance to Additional Requirements

8.6.5.1.1 Conformance to Additional Requirement 1

1. Requirement 1: The control system will incorporate facilities for controlling:
   a) all closed loop controls, for example: reactivity and temperature etc;

b) All open loop controls such as starting or stopping of the Reactor Facility components.

The RCMS incorporates facilities for controlling closed and open loop controls.

Since the RCMS is a Safety Category 2 system, none of these closed control loops are required to maintain the plant in a safe shutdown state. Similarly, none of the control actions credited to the RCMS are considered an Engineered Safety Feature. Closed control loops are provided to increase plant operability and availability. Open loop controls include such actions as starting and stopping pumps and opening and closing valves.

8.6.5.1.2 Conformance to Additional Requirement 2

Requirement 2: The control system will incorporate computer based reactor operator control and monitoring workstations. Workstations will be provided for the MCR and ECC.

The systems SUs are the operator workstations that centralise the task of controlling and monitoring the reactor plant. The SUs provide the interface between the operator, control functions and the plant. They are available in the MCR, ECC and at other key areas.

8.6.5.1.3 Conformance to Additional Requirement 3

Requirement 3: Data storage and retrieval systems will be provided for continuous logging of important reactor facility equipment status including analogue parameters, alarms, operator actions and reactor facility process and control system faults. Redundant storage devices and suitable data handling/logging software will be provided to ensure that mandatory records of all the reactor facility operations are automatically gathered and stored.

The RCMS historical data module stores all selected data and signals handled by the RCMS, FRPS, SRPS and PAM systems. All reactor operations tasks are automatically logged and stored.

8.6.5.1.4 Conformance to Additional Requirement 4

Requirement 4: All microprocessor based control systems and equipment will be located, as far as possible, such that they are protected from the effects of DBA that could adversely affect their performance.

The RCMS is a distributed control system and as such, field units are located in all plant areas. They are located such that the effects of a DBA are reduced as much as possible. The control units and control room supervision units are located outside of the reactor containment boundary so they are protected from the effects of a DBA.

8.6.5.1.5 Conformance to Additional Requirements 5 to 12

Requirement 5: The RCMS will be equipped with a dedicated LAN system.

Requirement 6: The RCMS will be based on distributed control architecture. If the design incorporates more than one node, redundant data buses interconnecting the nodes with no single point of failure will be provided.

Requirement 7: The control system will have sufficient redundancy to ensure that no single point of failure exists and that the overall system availability is met.

Requirement 8: The control system will be equipped with dual redundant processor

units.

Requirement 9: Switch over from the failed unit to the healthy redundant unit will be automatic and seamless.

Requirement 10: Separated inputs and outputs will be provided for associated duty and stand-by plant whenever it is practical. That is; they will be connected to separate I/O modules and power supply circuits etc.

Requirement 11: The control system will ensure that failure of any single point on a multiple I/O card will have no effect on the other points on that card.

Requirement 12: The memory update of a control processor returned to service after being taken offline or after a failure will be automatic.

See Section 8.6.3.1

8.6.5.1.6 Conformance to Additional Requirement 13

Requirement 13: The RCMS availability will be greater than 99.9%.

The RCMS is designed such that overall availability is greater than or equal to 99.9%. A thorough surveillance and maintenance programme to fulfil this requirement is provided as part of the detailed engineering.

8.6.5.1.7 Conformance to Additional Requirement 14

Requirement 14: The availability of the installed control systems will be tested after final commissioning and before practical completion.

The availability of the installed control system will be tested after final commissioning and prior to practical completion.

8.6.5.1.8 Conformance to Additional Requirements 15 to 18

Requirement 15: The reactor facility control system will have sufficient dedicated resources including: memory, processor speed and network bandwidth etc to perform the control functions, point scanning, online diagnostics and other requirements without exceeding 40% of system resources under worst case conditions.

Requirement 16: A minimum of 20% spare carded, installed and terminated I/O points will be provided at the time of practical completion for each of the reactor facility control system’s input-output cubicles.

Requirement 17: The RCMS input and output cubicles will provide for an expansion capacity in addition to the installed spare capacity. A minimum 20% spare capacity will be provided for all aspects of the control system.

Requirement 18: Expansion capability will be provided such that I/O modules, internal cubicle wiring, I/O cards, signal interfacing or conditioning equipment and running of cables can be added or changed without having to upgrade any processors, operator workstation hardware or software, power supplies or cubicles.

See Sections 8.6.3.1.7 and 8.6.3.1.8.

8.6.5.1.9 Conformance to Additional Requirements 19 to 28

Requirement 19: Operator workstations will be provided to centralise the task of controlling and monitoring the reactor plant. They will communicate with the reactor control system and provide the interface between the operator, control functions and the plant.

Requirement 20: Operator workstations will be provided to represent the status of the plant in a modern graphical environment. An open system architecture employing state-of-the-art hardware and software including operating system technology will be provided.

Requirement 21: Operator workstations equipped with keyboard, mouse or touch screen will be provided to allow the operator to navigate and interact with the graphics screens as well as perform data entry operations.

Requirement 22: Multiple 48cm or larger colour VDUs for the display of operator information in the MCR will be provided.

Requirement 23: An arrangement whereby all colour VDU will be capable of displaying all reactor information will be provided.

Requirement 24: A minimum of three colour Visual Display Units for the ECC with the capability of displaying all reactor information will be provided.

Requirement 25: Operator workstations will include a warning and alarm system.

Requirement 26: Operator workstation displays will incorporate a form of data quality coding (for example: colour coded data displays) so that a judgement can be made by the operator about the reliability of the information being presented on the screen. The data quality indication system will also cover computed parameters that may rely on the status of more than one data point.

Requirement 27: The maximum time lag will be no greater than three seconds for a screen display or window to be updated when selected under the worst possible computer and network loading conditions

Requirement 28: The maximum time lag will be no greater than two seconds for a screen to update any input change under the worst possible computer and network loading conditions.

See section 8.6.3.1.9

8.6.5.1.10 Conformance to Additional Requirements 29 to 34

Requirement 29: A dedicated engineering workstation will be provided to allow screen and database development. It will also allow maintenance, testing and diagnostic checks on control systems, networks and peripherals etc to be carried out.

Requirement 31: Maintenance work will be able to be performed from the engineering workstation on the control system, database and graphic screens etc while the system is operational and without affecting online operation. MCR and ECC workstations will have priority for control at all times.

Requirement 32: The control system will download database information as well as update graphical information while the system is being used without affecting normal operation.

Requirement 33: The control system will be able to use relational database search techniques to allow for engineering analysis of real time, historical/archival and database parameter information.

Requirement 34: No limits will be placed on the ability to expand the size of the database and the number of graphical screens developed for display. All the graphical and database editing software will be included with the engineering workstation.

See Section 8.6.3.1.10

8.6.5.1.11 Conformance to Additional Requirements 35 to 39

Requirement 35: The control system will save all its database points at the same rate as their respective scan rate (scan rate will be based on the acceptable industry standard at the time of procurement of the system) and time-stamped with the scanned time. Archiving of data will be automatic to a suitable medium (magnetic tape, optical disc). A warning message to operators will be provided when the archive medium is at 75% and 90% of capacity.

Requirement 36: Scanning of all sequence-of-events inputs following a change of state will be provided. Such inputs will be time-stamped (at the control system or associated sequence-of-events hardware) within 5ms of the time of the occurrence of the event.

Requirement 37: Fast access to the short term (up to 12 months) historical storage facility will be provided.

Requirement 38: A long term archive storage medium will be provided which will be easy to load and operate and convenient to store. It will be of a suitable capacity to hold at least one year's worth of information.

Requirement 39: Online dual redundant historical/archival data storage will be provided.

See Sections 8.6.3.1.10

8.6.5.1.12 Conformance to Additional Requirements 40

Requirement 40: Interfacing and signal conditioning equipment to instrumentation, field devices, switches, actuators and motors etc will be provided to enable open and closed loop control and monitoring of the Reactor Facility.

See Section 8.6.3.1.11

8.6.5.1.13 Conformance to Additional Requirements 41

Requirement 41: Redundant serial communication field buses will be provided for the connection of all Safety Category 3 control and monitoring instrumentation signals to the RCMS.

All communication field buses for the connections between the RCMS and Safety Category 3 systems are double redundant. The connection of Safety Category 3 systems is done by upgrading the relevant equipment from Safety Category 3 to Safety Category 2.

8.6.5.1.14 Conformance to Additional Requirements 42

Requirement 42: The reactor protection and shutdown systems will be equipped with serial communications capabilities, uni-directional, send only data interfaces to allow the reactor protection and shutdown systems to send data to the RCMS. All interconnections of reactor protection, shutdown and ESF signals to the RCMS will be via appropriate isolation devices to ensure the complete separation of Safety Category 1 from Safety Category 2 and 3 systems.

Isolation Units are provided to establish connections between the FRPS, SRPS, PAM and RCMS.

End of Section

Table 8.6/1 Software Requirements Verification and Validation Tasks

Tasks	Description	Methods and Tools	Required Inputs	Outputs
Traceability Analysis	Trace requirements in SRS and RCMS System Description (Preliminary version) to SRS and the updated version of RCMS System Description. Trace requirements stated in Control Requirement Specifications documents and their corresponding source documents.	Documentation reviews	SRS SRS RCMS System Description (Preliminary version) RCMS System Description (updated version) CRS(s) Traceability Matrix	Traceability Matrix Requirements Evaluation Report 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 Test Plan Generation	INVAP generates the plan for FAT testing.		SRS RCMS System Description CRS(s)	FAT Test Plan
SAT Test Plan Generation	INVAPS generates the plan for SAT testing. This plan will verify the correct and safe operation of the software in the operational environment.		SRS RCMS System Description CRS(s)	SAT Test Plan

Table 8.6/2 Software Design 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	RCMS System Description SRS Design Document Traceability Matrix	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	SRS RCMS 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	SRS RCMS System Description Design Document	
Unit and Pre-FAT Test Plan Generation and Verification	Foxboro developed the Unit Test Plan and the Pre-FAT Test Plan. These plans were reviewed and approved by INVAP.		RCMS System Description SRS Design Document Unit Test Plan Pre-FAT Test Plan	Unit Test Plan Pre-FAT Test Plan Anomaly Report(s)

Table 8.6/3 Implementation Verification and Validation Tasks

Tasks	Description	Methods and Tools	Required Inputs	Outputs
Traceability and Interface Analysis (Software Configuration Review)	Trace the software configuration 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 (a) RCMS System Description	Traceability Matrix Anomaly Report(s)
Test Procedure Generation and Verification	Develop test procedures for unit testing, Pre-FAT and FAT testing. Foxboro developed the unit and FAT USA test procedures. These procedures were reviewed and approved by INVAP. INVAP developed the FAT test procedures and unit test procedures of in house developed software.		RCMS System Description SRS Design Document Unit, Pre-FAT and FAT Test Procedures	Unit Test Procedures Pre-FAT Test Procedures FAT 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. Conduct re-testing as necessary.	Software Configuration Items test	Source Code (In-house software) Software Configuration items (Third-party software) Unit Test Plan Unit Test Procedures Unit Test Results	Unit Test Results Anomaly Report(s)

Table 8.6/4 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, FAT and Pre-FAT Test Plans and Test Procedures Traceability Matrix Software Configuration Items	Traceability Matrix Anomaly Report(s)
Interface & Communication Test	Test interfaces with hardware, user, and operator for completeness, consistency, and correctness. Test all communication channels.	Interface tests Communication tests	SRS RCMS System Description Design Document	Anomaly Report(s)
SAT Test Procedure Generation and Verification	Develop SAT test procedures.		SRS RCMS System Description Design Document SAT Test Plan SAT Test Procedures	SAT Test Procedures Anomaly Report(s)
Pre-FAT Test Execution and Verification	This testing was performed at the Foxboro Headquarters in Buenos Aires. INVAP analysed and documented the test results.		RCMS Software(b) Pre-FAT Test Plan Pre-FAT Test Procedures Pre-FAT Test Results	Pre-FAT Test Results Anomaly Report(s)

Tasks	Description	Methods and Tools	Required Inputs	Outputs
FAT Test Execution and Verification	This test was performed in Bariloche. INVAP and ANSTO analysed and documented the test results.		RCMS Software (c) FAT Test Plan FAT Test Procedures FAT Test Results	FAT Test Results Anomaly Report(s)

Table 8.6/5 Validation 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.		Software Configuration Acceptance Test Plan Acceptance Test Procedures Acceptance Test Results	Test Results Anomaly Report(s)

Table 8.6/6 Installation and Commissioning Verification and Validation Tasks

Tasks	Description	Methods and Tools	Required Inputs	Outputs
Installation Configuration Audit	Verify that all software products required to correctly install and operate the software are present in the installation package. Verify all site-dependent parameters or conditions to verify that supplied values are correct.		Installation Package (e.g., RCMS software, Installation procedures, site-specific parameters, installation procedures, etc.)	Anomaly Report(s)
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.		RCMS SVVP V&V Task Results	V&V Final Report

Table 8.6/7 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 Figures