UK EPR	Title: PCSR – Sub-chapter 7.3 – Class 1 Instrumentation and Control systems
	UKEPR-0002-073 Issue 04

Total number of pages: 52	Page No.: I / IV
Chapter Pilot: B. WORINGER *Name/Initials* [signature] *Date 05-11-2012*	
Approved for EDF by: A. MARECHAL *Name/Initials* [signature] *Date 05-11-2012*	Approved for AREVA by: G. CRAIG *Name/Initials* [signature] *Date 05-11-2012*

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA review	14.1.2008
01	Integration of technical, co-applicant and INSA review comments	27.4.2008
02	PCSR June 2009 update: - Clarification of text - Reference to the FA3 design being assessed for GDA - References added - Figures updated (Section 7.3.1 - Figures 3 and 6)	30.06.2009
03	Consolidated Step 4 PCSR update: - Minor editorial changes - Clarification of text - Update and addition of references - Update of Safety Function Categorisation and SCC Classification to clearly summarise Category A, B, C and Class 1, 2, 3 for I&C scope - SICS added; changed to Class 1 system - Independence for PS related to lower class systems - Architecture: Class 1 manual control and indication systems in the MCR and RSS - NCSS system added - Electrical and functional isolation for interfaces to systems of different safety class - Text updated to address diversity between PS and back-up/secondary protection system - Addition of the automatic RBS [EBS] actuation upon “SG pressure < MIN4” (Table 4)	27.03.11

Continued on next page

REVISION HISTORY (Cont'd)

Issue	Description	Date
04	Consolidated PCSR update: - References listed under each numbered section or sub-section heading numbered [Ref-1], [Ref-2], [Ref-3], etc - Minor editorial changes - Update and addition of references - Clarification of text, tables and figures (§1.0, §1.0.1, §1.0.2.1, §1.0.2.2, §1.0.2.3, §1.0.3.3.1, §1.1, §1.3.3, §1.3.8, §1.4.1.2, §1.4.1.3.1, §1.4.1.3.2, §1.4.1.4, §1.4.3.1, §1.7.2, , Section 7.3.1 – Tables 1 & 2, Section 7.3.1 – Figures 1 and 3 to 6, §2.0, §2.0.1, §2.0.3.1.2, §2.0.3.2, §2.3.2, §2.3.3, §2.3.4, §2.3.7, §2.3.9, §2.7) - Addition of Protection System Operator Terminal (PSOT) (§1.4.1.3.1, Section 7.3.1 – Tables 1 and 2, Section 7.3.1 - Figure 5, §2.5) - Detail on separation between core sub-systems and interface units added (§1.3.2, §1.3.2.3) - Text on diversity updated consistent with elsewhere in the PCSR (§1.3.4) - Explanation of Non-Class 1 part of the RPR [PS] updated (§1.4.1.3.2) - Rod Pilot updated to Class 2 (Section 7.3.1 – Table 2) - Additional clarification of SICS operating philosophy (§2.5)	05.11.2012

For information address:

AREVA NP SAS
Tour AREVA
92084 Paris La Défense Cedex
France

EDF
Division Ingénierie Nucléaire
Centre National d'Equipement Nucléaire
165-173, avenue Pierre Brossolette
BP900
92542 Montrouge
France

TABLE OF CONTENTS

SUB-CHAPTER 7.3 – CLASS 1 INSTRUMENTATION AND CONTROL SYSTEMS

1. PROTECTION SYSTEM (RPR [PS])

Note: Refer to the quality plans, system specification reports and overall architecture drawings for more detailed information on the RPR [PS] [Ref-1] to [Ref-18].

1.0. SAFETY REQUIREMENTS

The RPR [PS] is subject to safety requirements applicable to Class 1 I&C systems, due to its management of Category A I&C Functions.

The requirements are detailed in several documents, which provide all the required information contained within an IEC 61513 compliant system requirements specification [Ref-1].

1.0.1. Safety functions

The RPR [PS] contributes to ensure the three main safety functions defined in Sub-chapter 3.2, these are:

- Control of fuel reactivity;
- Fuel heat removal; and
- Confinement of radioactive material.

1.0.2. Functional criteria

1.0.2.1. Control of fuel reactivity

The main safety systems actuated by the RPR [PS] and involved in the control of fuel reactivity are:

- the Reactor Trip (rod drop);
- the Safety Injection System (RIS [SIS]);
- the Extra Boration System (RBS [EBS]).

1.0.2.2. Fuel heat removal

When required by the thermal hydraulic conditions, the RPR [PS] initiates the following safeguard systems to ensure the fuel heat removal safety function:

- the Emergency Feed Water System (ASG [EFWS]); or

- the Reactor Coolant System partial cooldown with the secondary side; or
- the Safety Injection System (RIS [SIS]) into the reactor coolant system.

1.0.2.3. Confinement of radioactive material

The RPR [PS] initiates the systems that prevent the violation of specified limits during incidents or accidents.

The measured process variables (e.g. thermal power, temperature and reactor coolant system pressure) are processed to allow monitoring of the limits imposed by neutron physics, thermal hydraulic and mechanical design for PCC-2 events.

The safety systems limit the consequences of PCC-3 and PCC-4 events. The containment isolation system limits radioactive releases following accidents to acceptable values if the integrity of the reactor coolant system is not maintained.

The RPR [PS] detects the accident conditions that could impair primary and secondary coolant system integrity. Reactor trip, in combination with safety features that act by direct pressure limitation, maintains this integrity.

1.0.3. Design requirements

1.0.3.1. Requirements resulting from the safety classification

1.0.3.1.1. Safety classification

The RPR [PS] must be safety classified according to the principles specified in Sub-chapter 3.2.

1.0.3.1.2. Single failure criterion

For RPR [PS] I&C Safety Features actuated under PCC-2 to PCC-4 conditions, a sufficient degree of redundancy must be provided in order to meet the single failure criterion.

In addition to the general requirements related to the single failure criterion given in Sub-chapter 3.1, the RPR [PS] has to fulfil the following specific design rules:

- The RPR [PS] must be designed so that a single failure does not prevent Class 1 I&C Safety Features from being enabled.
- The RPR [PS] must be designed so that a single failure during preventive maintenance or periodic tests does not prevent Class 1 I&C Safety Features from being enabled.
- A single failure must not generate PCC-3 or PCC-4 events even during preventive maintenance or periodic testing (this requirement is met by appropriate design of mechanical equipment and I&C equipment).
- Physical separation and decoupling between redundant trains must be provided.

1.0.3.1.3. Emergency power supply

As for other safety systems, the power supply of redundant components of the RPR [PS] must be backed-up by the Emergency Diesel Generators, so that they carry out their I&C Functions, even if the external power supply is lost.

In addition, the RPR [PS] must be supplied by an uninterruptible power supply at the suitable voltage so that it carries out its I&C Functions without interruption when the external power supply is lost.

1.0.3.1.4. Qualification under operating conditions

Components of Class 1 I&C Safety Features must be qualified to remain functional under the environmental conditions for which their operation is required.

The resulting requirements for components (integrity, operability, functional capacity, etc.) are given in Sub-chapter 3.6.

1.0.3.1.5. Classification of electrical and I&C equipment

The electrical and I&C classification of the system must be consistent with the classification principles given in Sub-chapter 3.2.

Some I&C Safety Features implemented in the RPR [PS] can be performed using I&C equipment of a higher class than is required (Class 1 instead of Class 2 for example). In some cases, this can simplify the design and prevent interference by lower class I&C Safety Features.

The tasks of the different parts of the RPR [PS] are given in section 1.4.1.3 of this sub-chapter.

1.0.3.1.6. Seismic classification

The RPR [PS] is designed with seismic requirements consistent with the principles given in Sub-chapter 3.2.

1.0.3.2. Other requirements

In addition to the general requirements given in Sub-chapters 7.1 and 7.2, requirements applicable to the RPR [PS] are given in section 1.3 of this sub-chapter.

1.0.3.3. Hazards

The RPR [PS] must be protected against the risk of common cause failure resulting from internal or external hazards [Ref-1].

1.0.3.3.1. Internal hazards

The RPR [PS] must be protected against internal hazards, in accordance with the principles in Sub-chapter 3.1.

The Class 1 I&C Safety Features of the RPR [PS] must comply with specific rules and requirements:

- The I&C Safety Features needed to reach the controlled state must be available even in the case of a single failure and preventive maintenance, following an internal hazard independent from PCC-2 to PCC-4 or RRC events;

- Following a PCC-2 event resulting from an internal hazard, the I&C Safety Features required for this PCC-2 must remain available despite a single failure and preventive maintenance or periodic testing within the I&C.

1.0.3.3.2. External hazards

The RPR [PS] must be protected against external hazards, in accordance with Sub-chapter 3.1.

To ensure protection against hazards such as an airplane crash, two divisions are installed in a protected building and the remaining two are geographically separated to limit the consequences of damage to that of a single division. The RPR [PS] equipment of the undamaged divisions has to be protected from any impact generated by the equipment from a division at the site of the impact.

1.0.4. Tests

1.0.4.1. Pre-operational tests

Pre-operational tests must prove the adequacy of the design and the performance of the RPR [PS].

1.0.4.2. Periodic tests

Periodic tests make it possible to detect failures early. Self-tests and periodic tests must be performed on Class 1 and Class 2 I&C Safety Features. The frequency of these tests is defined from a reliability prediction of the tested component. Both sets of tests significantly reduce the probability of failures that may result in the loss of I&C Functions.

The RPR [PS] is designed to allow periodic testing. The system will be designed to minimise the risk of spurious actuation.

1.0.5. Additional requirements

Specific measures are taken to mitigate the failure of the reactor trip in case of an Anticipated Transient Without Scram (ATWS) where the RPR [PS] is expected to operate normally. This sequence is mitigated by actions performed by the RPR [PS] which aim at reducing the reactor power by means other than the control rods: start-up of extra boration systems, isolation of volume control tank, and trip of reactor coolant pumps (this last action increases the reactor coolant temperature and therefore decreases the reactor power).

1.1. ROLE

The RPR [PS] implements automatic, manual and monitoring Category A I&C Functions. It also implements some Category B I&C Functions, as well as Category C I&C Functions specific to the RPR [PS].

The RPR [PS] mainly fulfils the following I&C Functions:

- Automatic reactor trip and turbine trip (see Section 7.3.1 – Table 3);
- Automatic start of safeguard systems and control of related support systems (see Section 7.3.1 – Table 4 to Section 7.3.1 – Table 7);
- Generation of alarms and plant data for the detection of situations that require operator manual actions;
- Actuation of manual Category A or Category B I&C Functions.

1.2. FUNCTIONS PERFORMED

The I&C Functions processed by the RPR [PS] are divided into three categories of functions:

- Logic control or sequential actuation of a system or equipment;
- Automatic closed-loop control of a system or equipment;
- Information to the operator (feedbacks, measurements, alarms).

The application functions that can be performed by the RPR [PS] are:

- Data acquisition and processing;
- Logic control;
- Closed loop controls;
- Sequence controls;
- Drive control functions;
- Alarm and information functions.

Refer to section 1 of Sub-chapter 7.2 for details of how Risk Reduction Category A (RRC-A) functions are allocated to the RPR [PS].

1.3. DESIGN BASIS

1.3.1. Redundancy

The RPR [PS] is designed to withstand any single failure even during maintenance or periodic testing. Moreover, four redundant channels are necessary to tolerate a single failure in addition to maintenance while minimising the risk of spurious actuation. In addition, the four redundant protection channels are installed in separated divisions to prevent common cause failure as a consequence of an internal hazard in one division.

The number of redundant channels of the I&C Functions must be equal to or higher than that of the mechanical/fluid systems trains, e.g. four medium head safety injection trains also require four trains for the dedicated I&C sub-systems.

1.3.2. Separation

Separation provisions and measures are implemented:

- between redundant equipment of the RPR [PS];
- between RPR [PS] equipment of different safety classes
- between RPR [PS] core sub-systems and interface units;
- between RPR [PS] diverse protection functions.

In addition to these requirements concerning the RPR [PS] itself, separation provisions and measures between the RPR [PS] and the other I&C systems ensure that no failure can impact two systems simultaneously.

1.3.2.1. Segregation of redundant equipment of the RPR [PS]

The redundant I&C Safety Features and their associated equipment, including support systems (e.g. power supply), will be separated from each other in order to limit the consequences of a single failure to the affected redundant equipment [Ref-1].

The following measures are required:

- The redundant equipment of the RPR [PS] must be physically allocated to different divisions.
- Specific protection measures must be provided (e.g. protective walls or tubing) to achieve separation for measuring instruments mounted close to each other.
- Interconnections between divisions are limited to a minimum to prevent internal hazards from spreading across division boundaries thereby limiting the effects of a single failure to the impacted redundant channel.
- Data communication between divisions are electrically (e.g. fibre optic) and physically (e.g. fire barriers) decoupled if connections between different redundant RPR [PS] channels are necessary (e.g. for majority voting).

- Erroneous signals have no impact on divisions other than the ones in which they originate (e.g. by means of majority voting).

1.3.2.2. Separation between equipment of different safety classes

Equipment with a different safety class within the RPR [PS] is segregated in such a way that a failure affecting equipment does not prevent equipment of a higher safety class from performing its I&C Functions.

The following measures are required:

- The common use of components for I&C Functions of different classes is avoided as far as possible. Any common equipment is assigned to the highest class of the I&C Functions that it processes (and is designed and classified as such).
- I&C Safety Features of different safety classes are decoupled from each other.
- Actuation signals from higher class I&C Functions, structures and components take priority over lower class I&C Functions actuation signals (functional isolation principle).

1.3.2.3. Separation between core sub-systems and interface units

The RPR [PS] Class 1 core sub-systems and interface units are segregated in such a way that a failure affecting an interface unit does not prevent core sub-systems from performing their I&C Functions. (The core sub-systems are the RAU, APU and ALU; the interface units are the MSI, DI and PI; see section 1.4.1.3.1)

The following measures are required:

- Physical separation - core sub-systems and interface units are housed in separate cabinets.
- Electrical isolation - each cabinet is supplied with its own power supply units. Communications between the core sub-systems and interface units use fibre optic based networks and there are no hard-wired connections between the core sub-systems and the interface units.
- Communications - the core sub-systems have separate networks for their safety I&C Functions that are not connected to the interface units. The core sub-systems have both network protocol features and application specific validation checks so their safety I&C Functions are functionally isolated from the interface units. The core sub-systems need the activation of a release key before the Service Unit can be used to change operating mode or parameters. The Service Unit is not permanently connected to the RPR [PS].

The RPR [PS] Class 1 core sub-systems and interface units have the same level of production excellence measures. Any plausible erroneous inputs from the interface units would be the same type of situation as operator errors. The state of the RPR [PS] is monitored by the operators.

1.3.2.4. Independence between diverse functions

Sufficient independence must be achieved if functional diversity is required.

The following measures are required:

- RPR [PS] equipment that performs a protection function is independent from RPR [PS] equipment executing the related diverse protection function.

- Equipment diversity for the instrumentation structures and components may be implemented if the diverse I&C Functions have to use the same process variable (decision on a case-by-case basis) [Ref-1].

1.3.2.5. Separation between the RPR [PS] and the other I&C systems

The RPR [PS] belongs to the main line of defence. Sufficient independence from the other lines of defence is necessary.

Adequate decoupling measures must be implemented to prevent failure propagation from a lower safety classified system.

1.3.3. Detection of degraded states

Measures are put in place to detect and identify failures to prevent long periods of operation with degraded RPR [PS] structures and components that might result in loss of function in the event of multiple failures. The measures, self-testing and periodic testing are all included in the FMEAs [Ref-1].

Self-testing and periodic testing of equipment detects failures that could prevent I&C Functions from being carried out.

Upon detection of a failure, the equipment must put itself into a state which is preferable for safety [Ref-2].

1.3.4. Implementation of diverse process variables

The design of the RPR [PS] complies with the diversity principle.

The RPR [PS] measures and processes, where possible, at least two diverse process variables for the reactor trip function. The diverse lines of reactor trip protection are shown in the fault schedule for most frequent events (see Sub-chapter 14.7).

Amongst these frequent initiating events, some Postulated Initiating Events (PIEs) can be mitigated, relying only on equipment performing control, Limiting Conditions of Operation (LCOs) or limitation functions, i.e. without the need for a reactor trip. As demonstrated in Sub-chapter 16.5 and illustrated in Sub-chapter 14.7, frequent faults (PCC-2 and frequent PCC-3 events) are protected by two diverse reactor trips, supported by diverse platforms, supported by diverse technologies (PS [RPR] in TXS, SAS in SPPA-T2000 and NCSS in UNICORN). In addition to this diversity, the RPR [PS] provides functionally diverse reactor trips within its sub-systems for most PCC-2 events. However, if failure of reactor trip does not lead to unacceptable consequences, then a diverse reactor trip is not required; sensitivity studies have been performed to identify and confirm that in such situations the risk targets are met, see Sub-chapter 15.7.

For less frequent events (infrequent PCC-3 and PCC-4 accidents), diverse reactor trips may be provided, if necessary, in order to reach probabilistic targets. In any case, most PCC-3 and PCC-4 transients are likely to challenge plant parameters in such a way that reactor trips from the PS [RPR] or SAS or NCSS would be actuated.

1.3.5. Availability requirements

1.3.5.1. Spurious actuation upstream of the actuation computer (last voter)

A failure anywhere in the RPR [PS] upstream of the last voting element must not generate any spurious command that would initiate a spurious actuation, even during maintenance or periodic testing.

1.3.5.2. Spurious actuation downstream of the last voter

In the event of an equipment failure downstream of (and including) the last voting element, the risk of spurious actuation of actuators controlled by Class 1 I&C Safety Features must be minimised, as far as possible.

1.3.6. Performance requirements

The RPR [PS] must fulfil the performance requirements of the Category A I&C Functions in terms of response time and accuracy. For each Category A function, these performance requirements are derived from the functional requirements. Section 7.3.1 - Tables 3 and 4 contain the preliminary requirement values.

The required performance is achieved by implementing the following design principles:

1.3.6.1. Distribution of functions

If necessary, the individual I&C Functions are distributed over several processing units to achieve the required response time.

The structure of the RPR [PS] takes into account the acquisition and processing of two existing diverse measured process variables in separate acquisition and processing units that can initiate independent protection actions for a given accident (functional diversity).

1.3.6.2. Communication

The RPR [PS] processes Category A I&C Functions with deterministic data transmission.

The equipment of the RPR [PS] that supports Category A I&C Functions has a deterministic behaviour. An I&C system is said to be deterministic if it is possible to know by analysis of its design, architecture and implementation and with a very high degree of accuracy what it does in all required modes of operation.

Some features are:

- pre-determined response time (response time lower than a known value);
- simple testability and failure diagnosis;

- simple software validation.

1.3.7. Environmental requirements

1.3.7.1. Normal and extreme conditions

The equipment must be able to operate in the environmental conditions set out in section 1 of Sub-chapter 9.4.

1.3.7.2. Accident conditions

Components are qualified to remain functional under the post-accident conditions, only if the function it is performing is required during post accident conditions.

This applies mainly to components subject to accident conditions (e.g. sensors and transmitters in the reactor building). The components located in the I&C rooms of the safeguard buildings operate in all plant conditions, including accidents, under the same environmental conditions.

1.3.8. Human-machine interface requirements

The RPR [PS] must interface with an engineering HMI, the service unit, to enable safe, effective and error-free commissioning, maintenance, periodic testing and configuration of the RPR [PS].

Access to video display units, computers, keyboards, mice, disk or CD-ROM drives, hard disks, printers, etc. related to the RPR [PS] equipment is controlled by physical means such as keys, magnetic or chip cards, etc.

This equipment may be unlocked only when needed and must be locked again when no longer in use.

No immediate access is possible to the RPR [PS] software itself. This means that access is possible only through interface equipment used for testing or configuration or data consultation and that the interface equipment is connected to the RPR [PS] without requiring I&C cabinets to be opened. The purpose of this restriction is to limit the overall number of times that physical access is required to the electronic modules of the RPR [PS] [Ref-1].

The operational HMI for the RPR [PS] is provided by the level 2 I&C systems, the PSOT described in section 1.4.1.3.1, and the safety HMI is provided by the MCS [SICS] described in section 2 (also see section 1.1 of Sub-chapter 7.2).

1.4. ARCHITECTURE

1.4.1. Structure and composition

1.4.1.1. Main equipment data

The equipment used to implement the Protection System is the AREVA NP TELEPERM XS digital I&C platform.

The digital TELEPERM XS I&C system is intended for applications relevant to safety in nuclear power plants. These include for example:

- Reactor protection systems;
- Engineered Safety Feature Actuation Systems (ESFAS);
- Reactor control, surveillance and limitation systems;
- Severe Accident I&C system.

Thus, TELEPERM XS covers all functions needed and benefits from modern digital technology.

Outstanding features of TELEPERM XS are the flexible task-oriented architecture, and the advanced design that guarantees long life expectancy by using established interface and communication standards wherever possible and up-to-date methods for engineering and maintenance.

The major advantages of employing digital processors in systems relevant to safety include:

- Early detection of faults by cyclic self-monitoring;
- Early detection of faults by improved monitoring of peripheral equipment (transducers, peripheral interfaces);
- Protection against faulty signals by fault detection;
- Higher fault tolerance compared to hard-wired systems through introduction of a signal status for marking faulty signals;
- Digital signal processing not subject to drift or electronic noise;
- Galvanic decoupling by use of fibre optic cables for serial data transmission;
- Engineering tools for plant and I&C, guaranteeing the best possible consistency of documentation.

1.4.1.2. Functional structure

The RPR [PS] implements the automatic and manual I&C Functions used to reach the controlled state after an accident and to maintain it as long as it is required for safety purposes. The RPR [PS] performs the diesel and support I&C Functions.

The following I&C Functions are Category A, and they are described below (see Section 7.3.1 – Figure 2):

- Reactor trip (RT): The RPR [PS] triggers the Reactor Trip that enables all rods to fall into the reactor core under gravity in order to terminate the core reactivity.
- ESFAS I&C Functions: The RPR [PS] triggers the ESFAS actions (safety injection, containment isolation, extra boration…);
- ESFAS closed loop control I&C Functions: These I&C Functions are dedicated to the management of Class 1 closed loop controls;

- Permissive I&C Functions: The RPR [PS] generates permissive signals which enable or disable the protection channel according to the plant state;
- Diesel I&C Functions: The RPR [PS] starts the emergency diesel generators in the event of loss of offsite power, stops them in the event of component protection and performs the load shedding and reloading sequence;
- Support I&C Functions: These I&C Functions are dedicated to the support systems actuation.

The RPR [PS] also performs some Category B I&C Functions, which are mainly:

- Category B manual controls (memory reset, manual actuation…);
- Saturation margin calculation (for diversity consideration).

The RPR [PS] implements continuous monitoring of protection channels and the transfer of information to the standard I&C (SPPA-T2000) systems. These I&C Functions are Category C. The RPR [PS] also implements some RRC-A functions and some non-categorised I&C Functions.

The following sections apply to the four divisions of the plant and for the four redundant channels of the RPR [PS].

1.4.1.2.1. Sensor(s) and transmitter(s)

Depending on the type of sensors, the I&C cabinets provide the power supply to the detectors, the decoupling modules if necessary and perform the required conditioning to provide different types of standardised signals that can be processed by A/D converters.

1.4.1.2.2. Measurement data acquisition

<u>A/D converters:</u>

The RPR [PS] converts analogue measurement signals to digital values.

<u>Data transmission:</u>

In most cases, downstream of the A/D conversion, there is no data exchange between the four redundant channels of the RPR [PS]. However, the algorithm that computes power distribution inside the core requires that the digitalised neutron flux values from all four divisions are distributed to all the redundant channels (see Section 7.3.1 – Figure 2).

<u>First level of processing:</u>

Each signal is checked. In the event of violation of the measuring range limits or in the event of detection of a fault in acquisition, the signal is invalidated for processing. Each digitised input is computed to get the corresponding physical value of the measurement that is processed. The results of the digitisation and the conversion into a physical value are also transmitted to other systems and to the service equipment.

1.4.1.2.3. Initiation processing

The first step is the collection of data coming from the measurement data acquisition of its division, and from the three other divisions (for neutron flux distribution). The digital data are processed according to the functional requirements.

The last step of the initiation processing is the comparison with one or more thresholds. The result is logic information, hereafter called the initiation signal, indicating whether the threshold is exceeded.

In the event of detected failure in the initiation processing, the initiation signal is identified as not valid.

1.4.1.2.4. Actuation processing

Each division collects the redundant initiation signals from the four divisions. These signals are computed in a 2 out of 4 voting logic to provide initiation orders. Such 2 out of 4 voting logic downgrades itself in the appropriate way if one or more signals are not valid.

All the initiation orders from the different initiation channels are computed together with the permissive/interlock signals to derive an actuation signal.

The results of the majority voting (i.e. the initiation order) as well as the actuation signal are also transmitted to other systems and to the service equipment.

1.4.1.2.5. Closed loop control processing

This function is specific to control loop processing (see Section 7.3.1 – Figure 2). The physical parameter that is controlled is acquired by the data acquisition equipment in each division and processed to provide closed loop control.

1.4.1.3. Composition

1.4.1.3.1. Class 1 part of the RPR [PS]

For the Class 1 part of the RPR [PS], refer to Section 7.3.1 – Figure 3, Section 7.3.1 – Figure 5 and Section 7.3.1 – Figure 6 for further information regarding the "Equipment Architecture".

This architecture applies to the four divisions of the plant. It can be split into the following types of units:

Rod Position Instrumentation computer (RPI)

The RPI units are not part of the RPR [PS]. They are part of the Control Rod Drive Mechanism (RGL). These units are involved in processing of Category A I&C Functions; they are on the RPR [PS] Core network. They are dedicated to the acquisition and digital processing of the analogue rod position measurements.

They transmit rod positions measurements of a division to the Actuation Logic Unit (ALU) of the same division and to the RCSL.

Remote Acquisition Units (RAU)

The RAU are part of the RPR [PS]. They are dedicated to the acquisition of Self Powered Neutron Detector (SPND) measurements. In each division, one RAU acquires the 18 SPND measurements assigned to its division and transmits them to the 4 divisions, so that the totality of the 72 SPNDs measurements are transmitted to APU1 of each division.

Acquisition and Processing Units (APU)

The APU are dedicated to the acquisition of signals from the Class 1 sensors (via the PIPS) and to the processing related to acquisition such as signal conversion, signal validation or threshold detection.

In addition, APU perform analogue calculation for some safety functions (e.g. Departure from Nucleate Boiling Ratio (DNBR) calculation).

Actuator Logic Units (ALU)

The ALU are dedicated to voting and actuation management (e.g. ESFAS, Reactor Trip and support functions) and to control loop processing.

Interface cabinets

The interface cabinets implement the hardwired interface between the RPR [PS] processing units and the external actuated devices (RT device, actuators switchgear, diesel I&C). There is no processing unit in the RPR [PS] interface cabinets.

Monitoring and Service Interface (MSI)

A Monitoring and Service Interface (MSI) is implemented in each division. The MSI is dedicated to the monitoring of the RPR [PS], In-core Neutron Flux Detector (RIC), Ex-core Neutron Flux Measurement System (RPN [NIS]) and Process Instrumentation Pre-processing System (PIPS) cabinets self monitoring management and to the management of the interfaces.

Panel Interfaces architecture (PI)

The Panel Interfaces (PI) ensure the interface between RPR [PS] and MCS [SICS]. It manages the manual control and the MCS [SICS] display (alarms, acknowledgment, flashing, etc).

Data Interfaces architecture (DI)

The Data Interfaces (DI) ensure two interfaces:

- between Monitoring and Service Interface (MSI) and Protection System Operator Terminal (PSOT) (bidirectional exchanges);
- between MSI and GateWay (GW) interface with SPPA-T2000 (unidirectional from MSI to GW interface with SPPA-T2000).

The link from the DI to the GW is a simple point-to-point unidirectional Class 3 network link. The DI does not receive any data from the network and only requires a ‘ready’ status to be able to send data. Therefore, the only function of the DI that can be affected by the network is the transmission of data over that network. In this case, the DI is able to raise an error status via the independent link to the PSOT.

The interfaces also perform some processing functions (e.g. redundancy reduction).

Protection System Operator Terminal (PSOT)

The PSOT is a Class 1 dedicated interface located in the MCR and the RSS. Each PSOT is connected directly to the RPR [PS] by means of an individual dedicated Class 1 TXS Ethernet network [Ref-1]. The PSOT is implemented on the Qualified Display System (QDS) platform. The PSOT is a computer-based touch-screen unit located adjacent to the MCP [PICS] workstations. The PSOT presents information to the operator by means of display formats and can receive orders via its screen interface. In the framework of the UK EPR, it is used to provide the operator with necessary information and to implement operator manual commands for the RPR [PS] when the plant is operated from the MCP [PICS]. There are four PSOTs located in the MCR and two located in the RSS. Each of the terminals will have the same functionality and scope and will operate independently of the other terminals and of the MCP [PICS] workstations. The scope of the functionality of the PSOT is defined in [Ref-2].

To prevent the possibility of spurious command generation from MCR PSOTs in the situation where an MCR hazard forces evacuation to the RSS, specific measures are taken as part of the evacuation procedures to disable the four PSOTs located in the MCR.

1.4.1.3.2. Non-Class 1 part of the RPR [PS]

Service unit's architecture (PS and PSOT)

The RPR [PS] Service Unit (PS SU) provides the maintenance and diagnosis function for the RPR [PS]. The service unit of the RPR [PS] is able to communicate with all TXS processing units of the RPR [PS] via the service network. The classification of the tools and the equipment will support class 2 maintenance and testing functions

The PSOT Service Unit (PSOT SU) is used for loading the PSOT on-line software and as a diagnostics device. It is based on the same hardware and operating system software as the RPR [PS] SU. The classification of the tools and the equipment will support class 2 maintenance and testing functions

The PS SU and PSOT SU are connected only during maintenance and diagnosis activities.

If either or both of the PS SU and the PSOT SU cannot comply with the relevant classification requirements, compensatory measures (such as operational maintenance and testing procedures) will be established to ensure the overall categorisation of the maintenance and testing functions

GW interface with SPPA-T2000 architecture

The TXS Gateways (TXS GW) are dedicated to implementation of the exchanges from the RPR [PS] to the SPPA-T2000. In particular, they transfer the information for display and archiving. They also perform some processing functions (e.g. redundancy reduction). The TXS GWs are Class 3.

Each TXS GW is connected to the DI of its own division with unidirectional Class 3 TXS Ethernet networks.

1.4.1.4. Diversity and common cause failures

To take advantage of the existence of two signals for a given safety action (functional diversity), and to ensure mitigation of the consequence of a common cause failure impacting the RPR [PS] software, each redundant channel is organised in two independent sub-systems (A and B).

The functional diversity principle is implemented as follows:

- As far as possible, the RPR [PS] measures at least two diverse process variables.
- The implementation of two diverse I&C Functions is possible for reactor trip for PCC-2 incidents. The loss of the protection function by the Engineered Safety Features (ESF) due to common cause failures in a PCC-3 or PCC-4 accident is addressed in the same way as the loss of the safety systems actuated by them, i.e. on a probabilistic basis. In the event of a complete loss of an ESF protection function due to common cause failure (in the fluid system or in the I&C), diverse back-up systems with diverse I&C Functions are provided only if the probabilistic target can be achieved with such back-up I&C Functions. These diverse back-up functions are implemented in I&C systems that use different technologies from the TELEPERM XS [Ref-1][Ref-2].

1.4.2. Installation

To meet separation requirements, the four redundant channels of the RPR [PS] and I&C electrical equipment are located in the I&C cabinet rooms of the four safeguard buildings.

1.4.3. Interfaces with other I&C systems

The RPR [PS] is part of level 1 of the I&C architecture. Its interfaces and relationships with other systems of levels 0, 1 and 2 are shown on Section 7.3.1 – Figure 1.

The input and output modules of the RPR [PS] are designed to ensure the required electrical separation [Ref-1].

1.4.3.1. Inputs

The RPR [PS] receives inputs from level 0, level 1 and level 2 systems and devices. Inputs from lower class systems are implemented using a hardwired link in order to protect the Class 1 RPR [PS] from interference. Links from lower class systems are restricted as far as possible.

For the Category A I&C Functions implemented by the RPR [PS], any erroneous input sent to the RPR [PS] via these hardwired links will have no effect on their processing, or an effect oriented towards safety [Ref-1] [Ref-2]. Specifically, directly complementary inputs that are in the same state will cause an alarm to be raised. All other inputs that are discrepant, but have no immediate potential functional impact will be detected during the next periodic test of the RPR [PS].

For other communications with systems and devices, the interfaces are implemented using network connections.

See Section 7.3.1 – Table 1 for an overview of the inputs provided by the other I&C systems.

1.4.3.2. Outputs

The RPR [PS] sends information to level 0, level 1 and level 2 systems and devices using both hardwired and network links.

See Section 7.3.1 – Table 2 for an overview of the destination of the RPR [PS] outputs.

1.5. TECHNOLOGY

The equipment used to implement the RPR [PS] is the AREVA NP TELEPERM XS digital I&C platform, described in section 1.4 of this sub-chapter and in section 1 of Sub-chapter 7.7.

1.6. POWER SUPPLY

For the power supply to the RPR [PS], the I&C cabinets of the RPR [PS] get a separate double in feed with 24V DC via independent AC/DC converters and DC/DC converters. The DC voltage is derived from an I&C power supply converter cabinet, connected to the 400V AC busbar or to the 220V DC batteries busbar.

During maintenance of the division power supply, one of the incoming feeders can be connected to the uninterrupted power supply of another division (1 and 2, 3 and 4).

To reduce the effects of the loss of the on-site and off-site power supply, the uninterrupted power supply is supplied by 2 hour capacity batteries.

The description of the power supply distribution of the NI is given in Sub-chapter 8.3.

1.7. PROVISIONS FOR MAINTENANCE AND I&C TESTS

1.7.1. Maintenance

For maintenance purposes (software downloading, parameter modification, component replacement), the maintenance team is able to act on the RPR [PS] without impairing the operability of the system. It is possible to switch off a unit by means of the RPR [PS] SU and hardware release keys in order to perform maintenance, internal tests or diagnosis [Ref-1].

1.7.2. Tests

The self-test features of the TXS hardware and the use of the RPR [PS] SU for periodic testing fulfil the periodic test requirements.

Periodic testing is performed at a frequency determined by the probabilistic safety requirements for the equipment that processes the safety I&C Functions. The various types of tests are performed in an overlapping manner in such a way that the instrumentation, the processing equipment, the actuator control and the interfaces between these are all tested. This method prevents multiple operations of actuators, maintains full plant availability, takes benefit from the best environmental conditions and tests the actuators smoothly.

Any equipment used to test the RPR [PS] will be at least Class 2. If the maintenance and testing equipment cannot comply with the relevant classification requirements, compensatory measures (such as operational maintenance and testing procedures) will be established to ensure the overall categorisation of the maintenance and testing functions.

SECTION 7.3.1 - TABLE 1

Input data for the RPR [PS] supplied by other I&C systems

Input source	Class	Data type	Connection type
PAS	Class 3	- Data for periodic tests, although not for periodic tests of Category A functions processed in the RPR [PS]. - Data for support functions.	Hardwired
SAS	Class 2	- Data for periodic tests, although not for periodic tests of Category A functions processed in the RPR [PS]. - Hardwired exchanges are used for Category B signals, signals requiring a short response time and for reactor trip check back.	Hardwired
Diesel I&C	Class 1	- Test check backs for periodic tests	Hardwired
Turbine I&C	Class NC	- Test check backs for periodic tests	Hardwired
Switchgear	Class 1*	- Test check backs of the switchgear for periodic tests	Hardwired
PIPS	Class 1	- Protection I&C Functions and for the DTsat calculation. - Monitoring signals of the PIPS cabinets	Hardwired
RPI	Class 1	- Conditioning of the Rod Position measurement instrumentation - Monitoring signals of the RPI cabinets	Hardwired and Network
RPN [NIS]	Class 1	- Ex-core Instrumentation, consisting of:- - Three source range detectors, - Four intermediate range detectors, - Four pairs of power range detectors - Monitoring signals of the RPN [NIS] cabinets	Hardwired
BCMS	Class 1	- Measurements used for boron concentration computation	Hardwired
RIC	Class 1 & 2	- In-core Instrumentation, consisting of:- o SPND o Thermocouples - Monitoring signals of the RIC cabinets	Hardwired
MCS [SICS]	Class 1	- Manual control orders initiated by the operators	Hardwired
PSOT	Class 1	- Manual control orders initiated by the operators	Network

* The actuators connected to the switchgear are Classes 1, 2 and 3. Any feedback from these actuators to the RPR [PS] is managed by the Class 1 switchgear

SECTION 7.3.1 - TABLE 2

Destination of output data from the RPR [PS]

Destination	Class	Data type	Connection type
PAS	Class 3	- Process parameters (analogue and binary) in case of shared instrumentation. - Status of automatic actions (e.g. reactor trip, start of RIS [SIS])	Network
RCSL	Class 2	- Process signals (e.g. ATWS signal, partial trip signals, etc.).	Hardwired
SAS	Class 2	- Network exchanges are unidirectional from RPR [PS] to SAS and are used for Category C or NC classified signals.	Hardwired and Network
MCP [PICS]	Class 3	- Information (alarms, status, etc) needed by the operators or for archiving	Network
MCS [SICS]	Class 1	- Information (alarms and indication displays)	Hardwired
PSOT	Class 1	- Information (alarms, status, etc) needed by the operators	Network
RPI	Class 1	- Interface to perform maintenance and periodic tests	Hardwired and Network
RDTME[1]	Class NC	- Reactor trip commands	Hardwired
Switchgear	Class 1	- Commands and test initiation signals	Hardwired
Trip Devices	Class 1	- Opening commands to the Trip Breakers, the Trip contactors	Hardwired
RodPilot	Class 2	- Opening commands to the electronic part of the RodPilot	Hardwired
Diesel I&C	Class 1	- Start and stop signals	Hardwired
Turbine I&C	Class NC	- Turbine trip commands - Test initiation signals	Hardwired
PSIS	Class 2	- Synthesis information about its status	Hardwired

[1] RDTME = Rod Drop Time Measurement Equipment

SECTION 7.3.1 - TABLE 3

Reactor trip functions performed by the RPR [PS]

PROTECTION FUNCTION	PCC/RRC	RESPONSE TIME	ACCURACY
REACTOR TRIP (AND TURBINE TRIP)			
on Steam Generator pressure drop > MAX1	PCC-2/3/4	500 ms	1.5 bar
on Steam Generator pressure < MIN1	PCC-2/3	500 ms	1.5 bar
on Pressuriser pressure < MIN2	PCC-2/3/4	500 ms	1.5 bar
on Steam Generator level (A) < MIN1A	PCC-2/3/4	500 ms	2% MR
on Steam Generator level (A) > MAX1A	PCC-2/3/4	500 ms	2% MR
on Pressuriser pressure > MAX2	PCC-2/3	500 ms	1.5 bar
on Pressuriser level > MAX1	PCC-2	500 ms	2% MR
on Steam Generator pressure > MAX1	PCC-2/3	500 ms	1.5 bar
on Containment pressure > MAX1	PCC-3/4	500 ms	0.2 bar
on Hot Leg Pressure < MIN1p	PCC-3/4	500 ms	1.5 bar
on High linear power density	PCC-2	500 ms	1% MR
on Low Departure from Nucleate Boiling Ratio (Low DNBR)	PCC-2	1000 ms	1% MR
on High core power level	PCC-2/3	500 ms	10% NP
on Ex-core high neutron flux rate of change	PCC-4	300 ms	2% NP
on Low Reactor Coolant Pumps speed (four reactor coolant pumps)	PCC-2/3	300 ms	0.1%
on Low reactor coolant flow rate (one loop) (**)	PCC-2/4	600 ms	3%
on High neutron flux (intermediate range)	PCC-2/4	300 ms	10%
on Low doubling time (intermediate range)	PCC-2/4	300 ms	10%

(**): action related to one Steam Generator (SG)

MR = Measuring Range, NP = Nominal Power

SECTION 7.3.1 - TABLE 4 (1/2)

Safeguard functions performed by the RPR [PS]

PROTECTION FUNCTION	PCC/RRC	RESPONSE TIME	ACCURACY
RIS [SIS] ACTUATION			
on Pressuriser pressure < MIN3	PCC-2/3/4	500 ms	1.5 bar
on Reactor Coolant System loop level < MIN1	PCC-3/4	500 ms	0.03 m
on ΔPsat < MIN1	PCC-3/4	500 ms	5 bar
PARTIAL COOLDOWN			
on Safety Injection System signal	PCC-2/3/4	See SIS	See SIS
on Steam Generator level (A) > MAX2A	PCC-3/4	500 ms	2% MR
MSIV CLOSURE			
on Steam Generator pressure drop > MAX1	PCC-2/3/4 RRC-A	500 ms	1.5 bar
on Steam Generator pressure < MIN1	PCC-2/3	500 ms	1.5 bar
on Steam Generator level (A) > MAX2A if partial cooldown is finished (**)	PCC-3/4	500 ms	2% MR
ASG [EFWS] ACTUATION			
on Steam Generator level (B) < MIN2B (**)	PCC-2/3/4	500 ms	2% MR
on Loss of Offsite Power signal		(***)	(***)
CONTAINMENT ISOLATION			
Containment isolation stage 1 on Safety Injection System signal	PCC-2/3/4	See SIS	See SIS
Containment isolation stage 1 on containment pressure > MAX1	PCC-2/3/4	500 ms	0.2 bar
Containment isolation stage 2 on containment pressure > MAX2	PCC-3/4	500 ms	0.2 bar
ASG [EFWS] ISOLATION			
on Steam Generator level (B) > MAX1B if Emergency Feedwater System has started (**)	PCC-3/4	500 ms	2% MR
VDA [MSRT]			
Main Steam Relief Train isolation on Steam Generator pressure < MIN3 (**)	PCC-2	500 ms	1.5 bar
Main Steam Relief Train opening on Steam Generator pressure > MAX1	PCC-2/3	500 ms	1.5 bar
Main Steam Relief Train setpoint increase on Steam Generator level (A) > MAX2A if partial cooldown is finished	PCC-3/4	500 ms	1.5 bar
REACTOR COOLANT PUMP TRIP			
Reactor Coolant Pumps trip on ΔP over reactor coolant pump < MIN1 and RIS [SIS] signal	PCC-3/4	500 ms	0.2 bar
On containment isolation stage 2 signal	PCC-3/4	500 ms	0.2 bar

(**): action related to one Steam Generator (SG)

(***): to be defined as part of the detailed design

SECTION 7.3.1 - TABLE 4 (2/2)

Safeguard functions performed by the RPR [PS]

PROTECTION FUNCTION	PCC/RRC	RESPONSE TIME	ACCURACY
LHSI/ RHR TRAIN ISOLATION			
LHSI/ RHR train isolation on high sump level and/or high SAB pressure	PCC-4	500 ms	(***)
ARE [MFWS] ISOLATION			
Main Feedwater low load isolation on Steam Generator pressure drop > MAX2 (**)	PCC-2/3/4 RRC-A	500 ms	1.5 bar
Main Feedwater low load isolation on Steam Generator pressure < MIN2 (**)	PCC-2/3	500 ms	1.5 bar
Main Feedwater/Start-up and Shutdown System isolation on Steam Generator level (A) > MAX1A	PCC-2/3/4	500 ms	2% MR
Main Feedwater full load isolation on Reactor Trip signal (**)	PCC-2/3/4	1000 ms	Binary information
PSV OPENING			
1st Pressuriser Safety Valve opening for brittle fracture protection of RPV	PCC-2	500 ms	2.5 bar
RCV [CVCS] ISOLATION			
Anti-dilution in shutdown conditions with reactor coolant pump not in operation	PCC-2	500 ms	(***)
Anti-dilution in standard shutdown states conditions	PCC-2	500 ms	(***)
Anti-dilution in power conditions	PCC-2	500 ms	(***)
Shutdown of RCV [CVCS] charging line on high PZR level	PCC-2	500 ms	2% MR
Shutdown of RCV [CVCS] charging line on high Hot Leg Pressure	PCC-2	500 ms	1.5 bar
Shutdown of RCV [CVCS] charging line on Steam Generator level (A) > MAX2A if partial cooldown is finished	PCC-3/4	500 ms	2% MR
Shutdown of RCV [CVCS] charging line on Steam Generator Pressure < MIN4 and Safety Injection Signal	PCC-2/3/4	500 ms	1.5 bar
RBS [EBS] ACTUATION			
on SG pressure < MIN4	PCC-4	500 ms	1.5 bar
Category A ALARM (operator action)			
High neutron flux (source range)	PCC-2	300 ms	11%

(**): action related to one Steam Generator (SG)

(***): to be defined as part of the detailed design

SECTION 7.3.1 - TABLE 5

Control functions of the safeguard systems performed by the RPR [PS]

PROTECTION FUNCTION	PCC/RRC
VDA [MSRT]	
VDA [MSRT] control function (Closed loop control)	PCC-2/3/4
ASG [EFWS]	
ASG [EFWS] pump overflow protection	PCC-2/3/4

SECTION 7.3.1 - TABLE 6

Trip functions of the auxiliary safeguard systems performed by the RPR [PS]

PROTECTION FUNCTION	PCC/RRC
RRI [CCWS]	
Component Cooling Water System configuration on containment pressure > MAX1	PCC-3
DIESEL ACTUATION	
Diesel actuation on 10 kV busbar voltage < MIN1	PCC-2/3

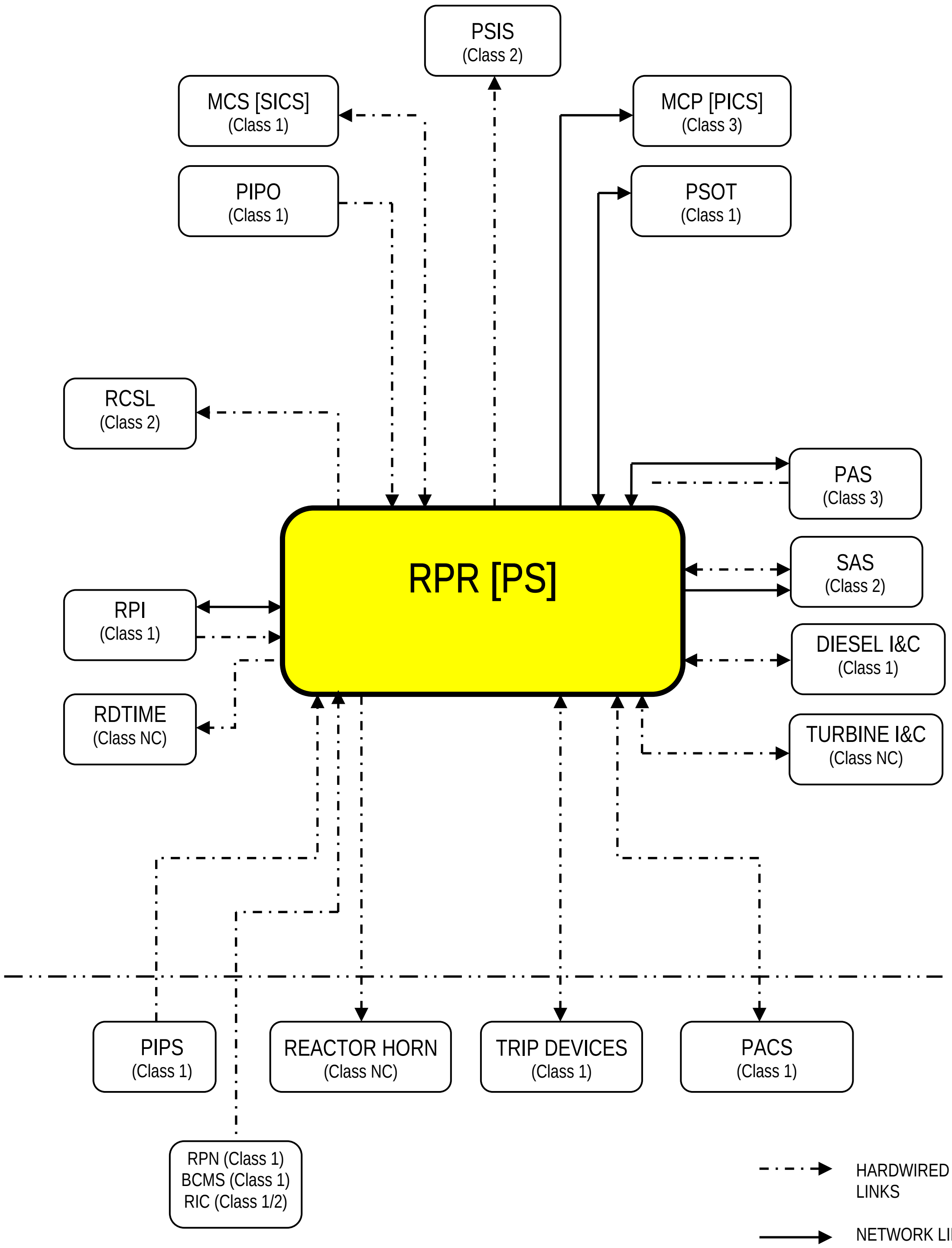
SECTION 7.3.1 - TABLE 7

Control functions of the auxiliary safeguard systems performed by the RPR [PS]

PROTECTION FUNCTION	PCC/RRC
DIESEL ACTUATION	
Diesel load shedding sequence	PCC-2/3

SECTION 7.3.1 - FIGURE 1

Interfaces and relations between the RPR [PS] and the other systems of levels 0, 1 and 2

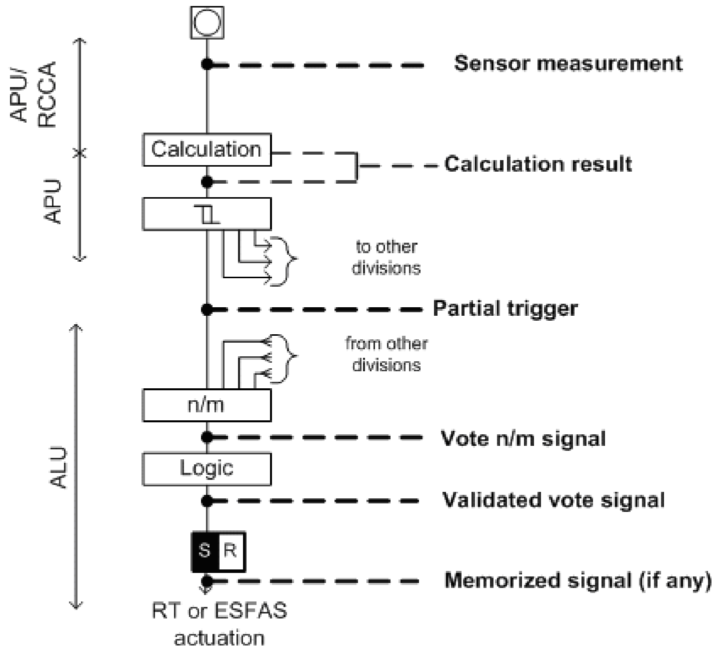


This figure only addresses the RPR [PS]. The interconnections between other I&C systems do not appear.

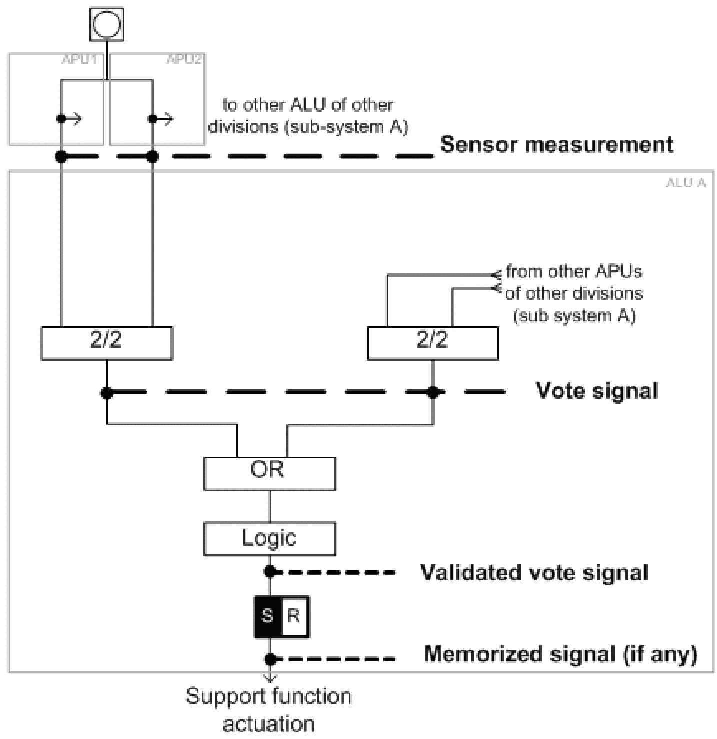
SECTION 7.3.1 - FIGURE 2 (1/2)

General functional structure (one division) of the RPR [PS]

General functional structure for reactor trip (RT) or ESFAS actuation



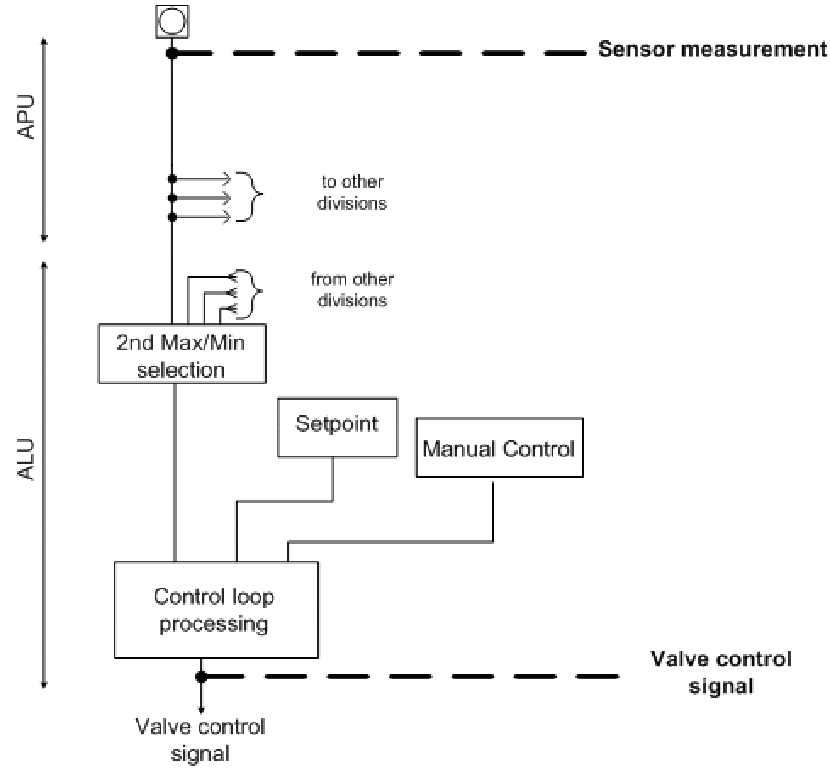
General functional structure for support function actuation



SECTION 7.3.1 - FIGURE 2 (2/2)

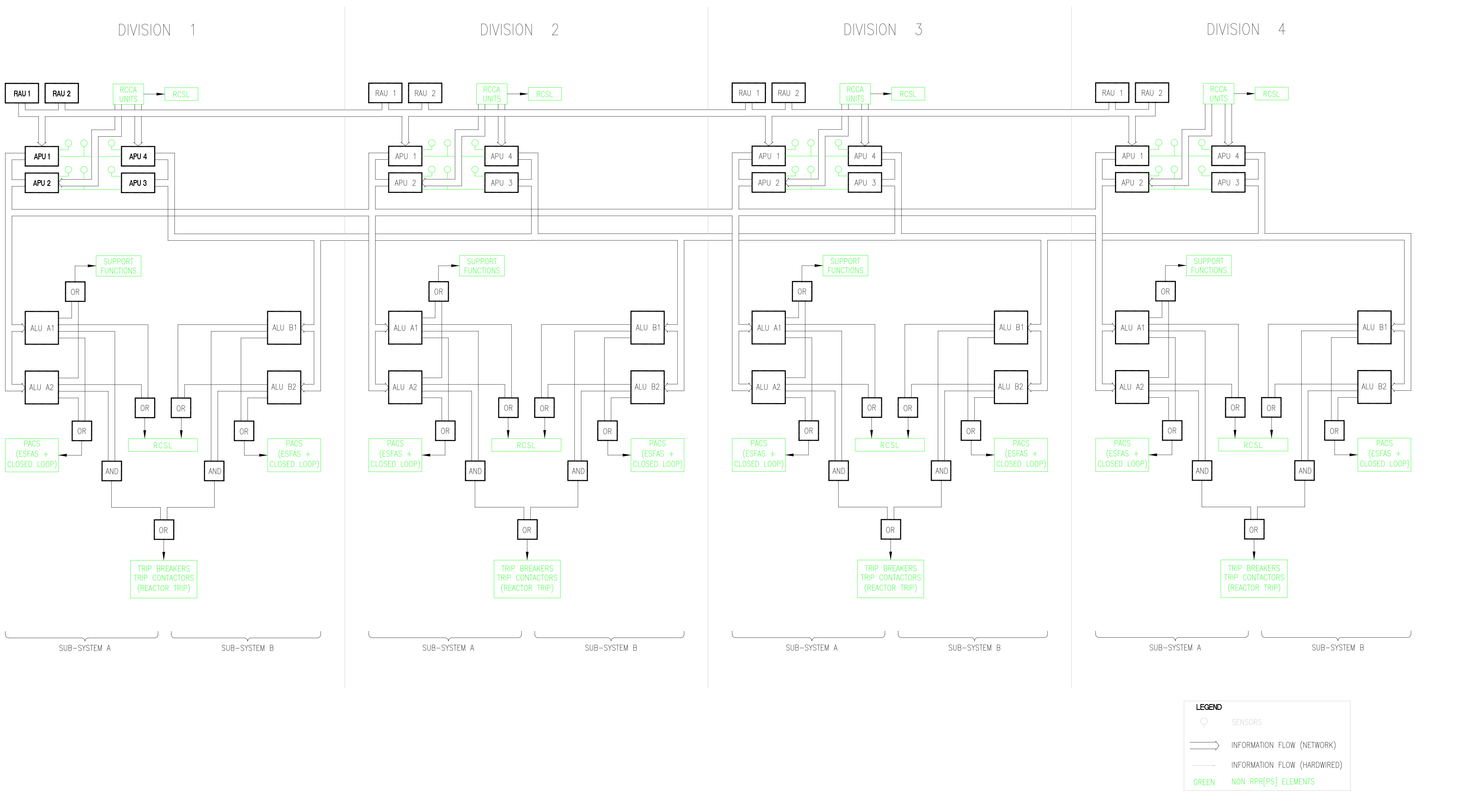
General functional structure (one division) of the RPR [PS]

General functional structure for closed loop function



SECTION 7.3.1 - FIGURE 3

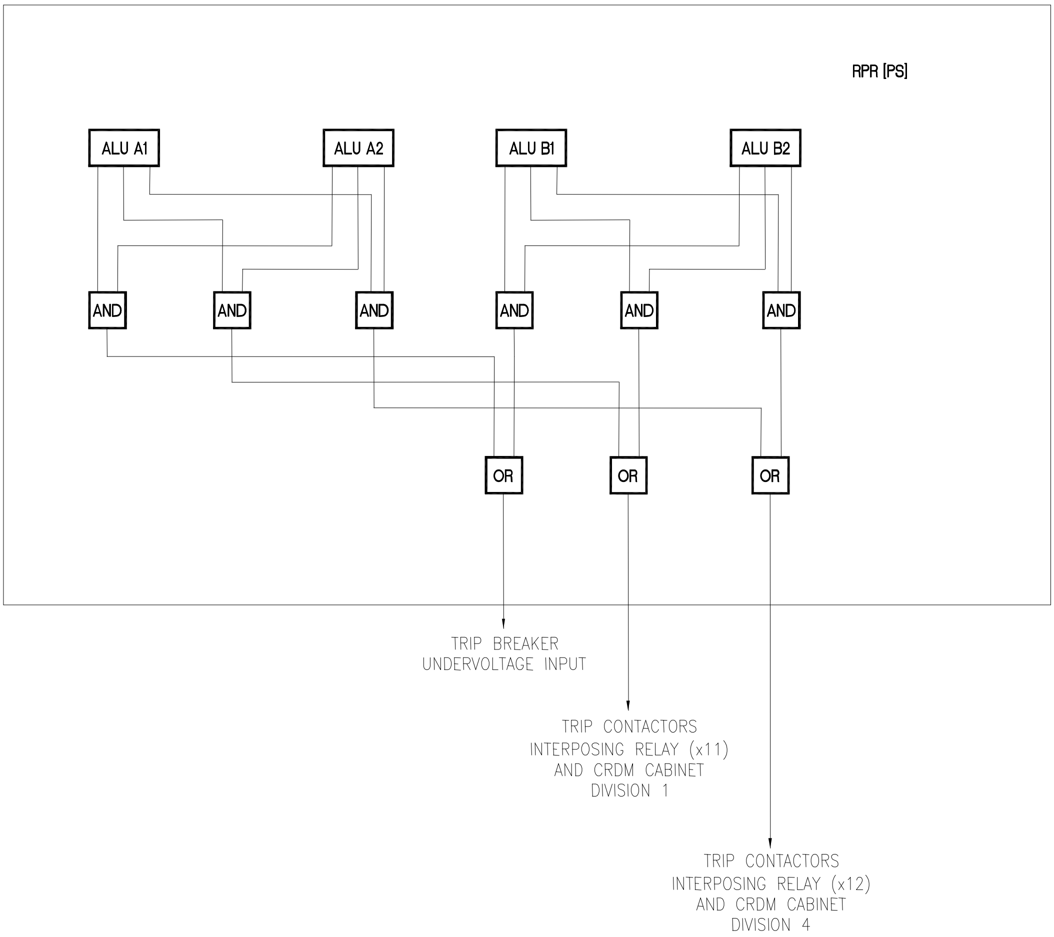
Equipment architecture of the part of the RPR [PS] system performing category A functions.



SECTION 7.3.1 - FIGURE 4 (1/2)

Equipment interfaces of the RPR [PS]

Output for Reactor trip signal

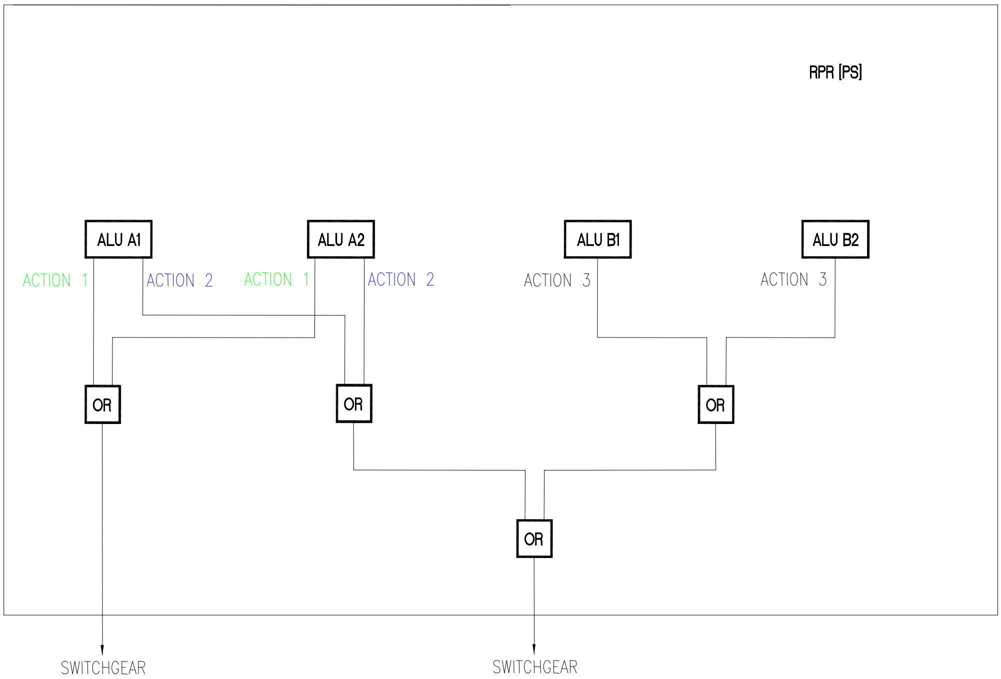


Note: Decoupling should be provided for interconnections with other divisions

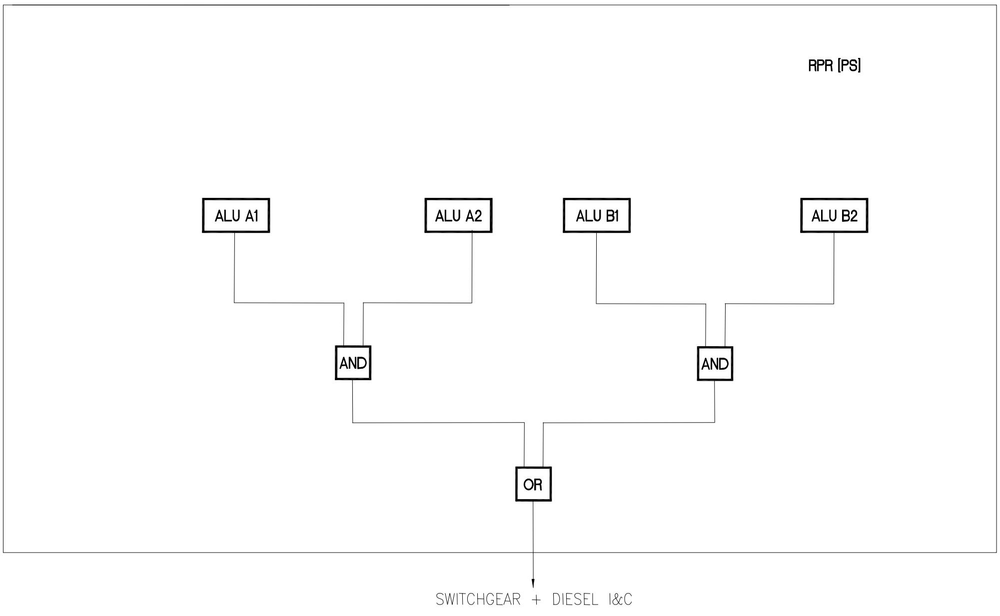
SECTION 7.3.1 - FIGURE 4 (2/2)

Equipment interfaces of the RPR [PS]

Output for ESFAS signal generation

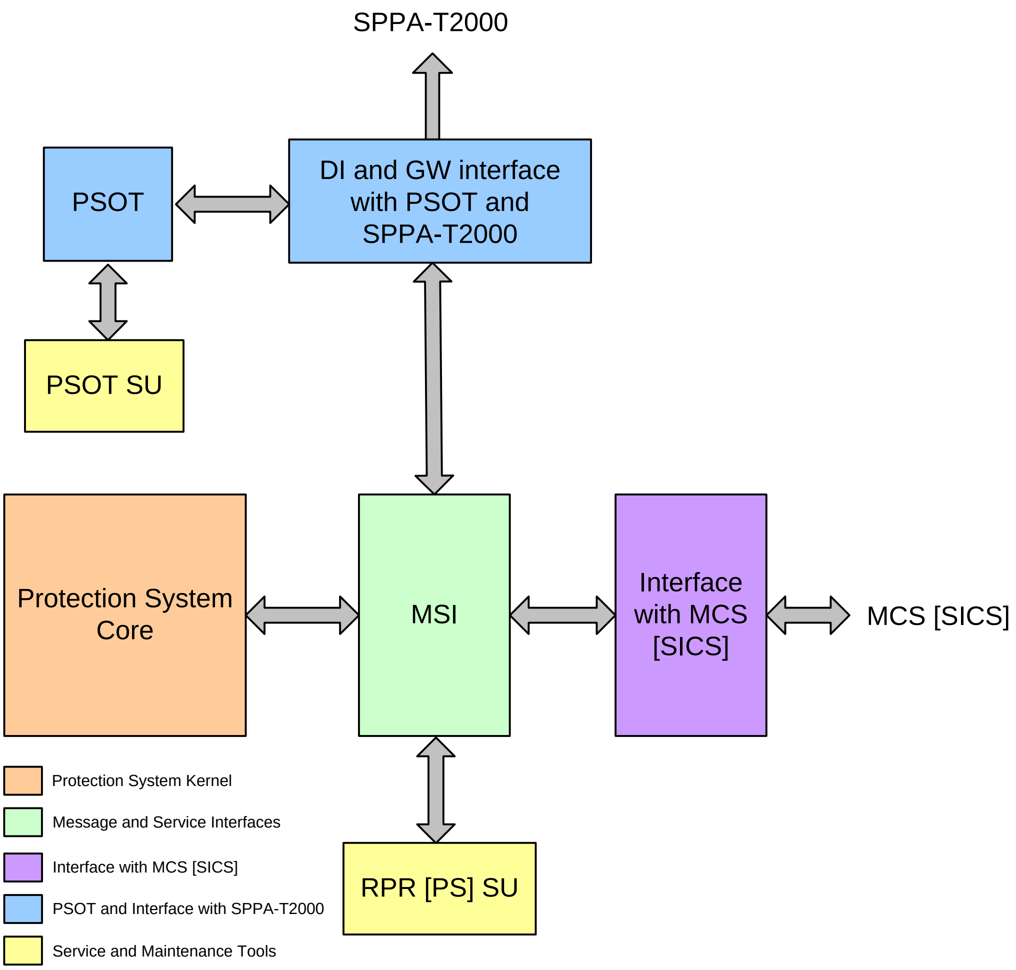


Output for Diesel or support signal generation



SECTION 7.3.1 - FIGURE 5

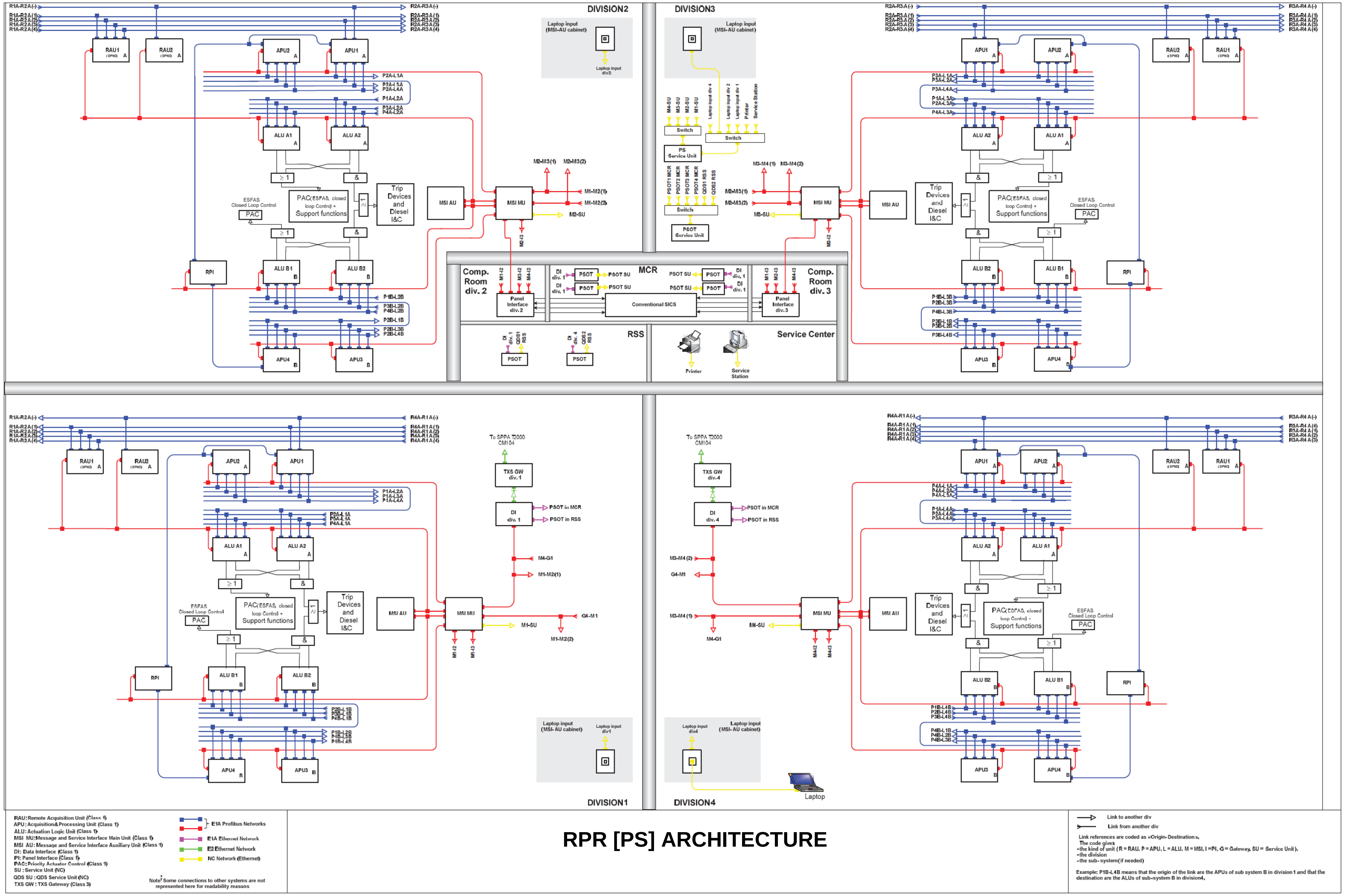
RPR [PS] architecture overview



Note: This diagram does not show all of the interfaces

SECTION 7.3.1 - FIGURE 6

Overall RPR [PS] architecture



2. SAFETY INFORMATION AND CONTROL SYSTEM (MCS [SICS])

Note: Refer to the quality plans, system specification reports and overall architecture drawings for more detailed information on the Safety Information and Control System (MCS [SICS]) [Ref-1] to [Ref-5].

2.0. SAFETY REQUIREMENTS

The MCS [SICS] is subject to safety requirements applicable to Class 1 I&C systems, as it interfaces to systems including the RPR [PS] and contributes to the management of I&C Functions up to Category A. As the MCS [SICS] provides discrete devices that connect to level 1 I&C systems, it supports the functional and divisional redundancy of the associated elementary systems but does not fulfil the single failure criterion at the MCS [SICS] component level. This is adequate to ensure the level of reliability claimed for this system.

2.0.1. Safety functions

The MCS [SICS] contributes to the I&C Functions supported by the I&C architecture (see Sub-chapter 7.1). MCS [SICS] controls and indications support input and output of level 1 I&C systems that perform I&C Functions for a number of elementary systems [Ref-1].

Regarding the safety analysis, the MCS [SICS] provides the operators with sufficient information and controls to reach and maintain the plant at safe shutdown following PCC-2 to PCC-4 type events. The MCS [SICS] is the operating interface used for the safety analysis. Therefore, the MCS [SICS] is Class 1.

2.0.2. Functional criteria

2.0.2.1. When MCP [PICS] is available

When the MCP [PICS] is available, the MCS [SICS] is used to undertake periodic tests related to the MCS [SICS] and in incident/accident operating situations to monitor the main safety parameters and the state of the back-up systems.

2.0.2.2. When MCP [PICS] is not available

When the MCP [PICS] system is not available, the MCS [SICS] has the following functions:

2.0.2.2.1. In case of normal operation with only the loss of the MCP [PICS]

The MCS [SICS] enables control in order to keep the unit in a stable state for a limited period of time, the recovery period (the maximum duration of which is 8 hours). If the period of unavailability of the MCP [PICS] is longer than the recovery period (8 hours), the MCS [SICS] makes it possible to bring the unit to a safe shutdown state and keep it there.

2.0.2.2.2. In case of loss of the MCP [PICS] in addition to a PCC-2 to PCC-4 event

The MCS [SICS] enables:

- monitoring of changes to the I&C Functions of the unit, in particular the automatic protection I&C Functions and post-accident I&C Functions (Class 1 and 2 I&C Safety Features),
- manual post-accident actions in order to achieve the controlled state (Class 1);
- the necessary manual post-accident actions in order to move the unit from the controlled state to the safe shutdown state and maintain this safe state in the long term (I&C Safety Features fulfilling Category B I&C Functions).
- monitoring and checking of the systems supporting the required back-up systems for post-accident operation from the MCS [SICS] [Ref-1].

2.0.3. Design requirements

2.0.3.1. Requirements resulting from the functional classifications

2.0.3.1.1. Functional classification of the system

The MCS [SICS] supports I&C Safety Features that have different architecture requirements due to their contribution to I&C Functions of different categories (A, B or C).

The MCS [SICS] is thus, according to Sub-chapter 3.2 and Sub-chapter 7.1, Class 1 and must therefore meet the safety requirements listed in the following paragraphs.

2.0.3.1.2. Single failure criterion

<u>MCS [SICS] Class 1 and Class 2 I&C Safety Features:</u>

The MCS [SICS] comprises a number of individual control and monitoring channels, each contributing to the delivery of functions associated with the supported plant systems. Where these plant systems are required to comply with the single failure criterion, they will include appropriate redundancy with the redundant parts allocated across the four segregated divisions. In such cases, the MCS [SICS] also includes the control and information necessary for the operation of the plant systems across the segregated divisions and, by this means, supports the plant system compliance with the single failure criterion. The justification of the compliance of these systems includes the MCS [SICS] control and information involved [Ref-1].

In addition, Class 1 controls of the MCS [SICS] utilise redundant electrical contacts.

<u>MCS [SICS] Class 3 I&C Safety Features:</u>

The single failure criterion is not applicable to the Class 3 I&C Safety Features of the MCS [SICS].

<u>MCS [SICS] NC I&C Safety Features:</u>

The single failure criterion is not applicable to the NC I&C Safety Features of the MCS [SICS].

2.0.3.1.3. Emergency power supplies

The electrical power supply to the MCS [SICS] equipment must be safeguarded by the Emergency Diesel Generators. Moreover, this power supply must be uninterruptible, guaranteeing a power supply even during switching between normal power and diesel power. In this way, the I&C Functions performed by the MCS [SICS] can be assured without interruption of service.

The MCS [SICS] equipment must be powered by the same electrical division as the I&C division that it monitors and controls. Each division is electrically and physically independent from the others in a way that eliminates the possibility that a single hazard or failure can affect more than one division.

2.0.3.1.4. Qualification under operating conditions

The equipment supporting the MCS [SICS] I&C Functions must be qualified for their safety class, according to Sub-chapter 3.6, and for the normal and extreme environmental conditions under which it would be operating when fulfilling these I&C Functions, in accordance with section 1 of Sub-chapter 9.4.

2.0.3.1.5. Electrical and I&C classifications

The electrical and I&C classification of the system is consistent with the classification principles given in Sub-chapter 3.2.

MCS [SICS] equipment is considered as a Class 1 system.

2.0.3.1.6. Seismic classification

MCS [SICS] meets the seismic requirements defined in Sub-chapter 3.2.

2.0.3.1.7. Periodic testing

All I&C Functions must be subject to periodic testing. The MCS [SICS] must be designed so that specific periodic tests can be performed.

2.0.3.2. Hazards

The MCS [SICS] must be protected against failures that could result from relevant internal or external hazards, in accordance with the requirements defined in Sub-chapter 3.1. The MCS [SICS] is located within the Main Control Room (MCR) and will therefore have limited protection against some hazards (for example fire). However, its power supply will have greater protection as it is supplied from four divisions (see section 2.7 of this sub-chapter).

2.0.4. Tests

2.0.4.1. Pre-operational tests

After installation, the MCS [SICS] must be subject to pre-operational testing to verify that it complies with the defined design requirements.

2.0.4.2. Monitoring in operation

Not applicable.

2.0.4.3. Periodic tests

The MCS [SICS] must be designed to allow periodic testing to be performed.

2.0.5. Additional requirements

There are no particular constraints beyond those mentioned in Section 7.3.1 – Table 1.

2.1. ROLE

The MCS [SICS] is a safety-classified I&C system that provides information and controls necessary to reach and maintain safe shutdown for post-accident operation in the event of unavailability of the MCP [PICS]. The monitoring and control systems supported by the MCS [SICS] are not the operating interface preferred by the operating team for monitoring and operating the plant.

Furthermore, the MCS [SICS] is the operating system claimed in the safety analysis of PCC-2 to PCC-4 design conditions.

The main role of the MCS [SICS] is therefore to provide the operators with sufficient controls and information to address the following situations:

- in the event of a short period of unavailability of the MCP [PICS] in normal operation (PCC-1): to monitor and control the plant in a steady power state;
- in the event of a longer period of unavailability of the MCP [PICS] in normal operation (PCC-1): to shutdown and keep the plant in a safe shutdown state and be able to stop the Conventional Island (turbine trip);
- in the event of unavailability of the MCP [PICS] during PCC-2 to PCC-4 design conditions: to monitor the plant and initiate appropriate post-accident I&C Functions to reach and maintain safe shutdown conditions.

In the event of fire, if the operating team uses the MCS [SICS], then the fire-fighting I&C Functions can also be initiated from the MCS [SICS].

When the MCP [PICS] is available in the MCR, the MCS [SICS] is also active in the following circumstances:

- Periodic testing associated with the MCS [SICS];
- In accident situations, monitoring of the main safety parameters and of the state of the safety systems (information search on a facility diverse from that of the MCP [PICS]).

2.2. FUNCTIONS PERFORMED

The MCS [SICS] performs the following control and monitoring functions:

- display of process information;
- control functions;
- alarm display and processing;
- analogue data recording;
- interface functions (filtering, data transmission);
- test functions.

2.3. DESIGN BASIS

2.3.1. Redundancy

The MCS [SICS] is a group of indicators and controls. Although individual I&C Functions may have a requirement for redundancy, there is no requirement for additional redundancy of the physical indicators and controls associated with each redundant item of equipment supported [Ref-1].

2.3.2. Separation

As discussed in sections 2.0.3.1.5 and 2.4.3, the MCS [SICS] will have interfaces to different classes of systems. In order to ensure that lower classes of system cannot interfere with higher classes, each class of controls and indicators within the MCS [SICS] will be electrically and functionally separated by being connected directly to the associated Level 1 I&C systems. The requirements for electrical isolation are defined in [Ref-1]. The justification of the compliance of these systems with the requirements for isolation and non-interference includes the MCS [SICS] control and indicators involved.

2.3.3. Detection of degraded states

The MCS [SICS] panel will include a lamp test facility to aid in the detection of any failed lamp indicators. The MCS [SICS] controls and indicators are considered in the FMEAs of the systems to which they are connected. Reliability is discussed in Sub-chapter 7.2 section 1.3.7, where these FMEAs are referenced.

2.3.4. Implementation of diverse process variables

There is no processing undertaken within the MCS [SICS] system. The MCS [SICS] may provide diverse information to the operator, who then will process the information.

2.3.5. Special provisions

The particular design provisions that must be taken into account for the MCS [SICS] are as follows:

- The MCS [SICS] must be functionally independent of the MCP [PICS] so that failure of the MCP [PICS] cannot, under any circumstance, have consequences on the MCS [SICS].
- When the MCS [SICS] is in service (see State 2 in section 2.5 of this sub-chapter), the MCP [PICS] controls must be deactivated.
- No internal hazard in the MCR resulting in the loss of MCS [SICS] may also result in the loss of the Remote Shutdown Station (RSS) workstations.
- The MCS [SICS] must meet the human-machine interface requirements described in Sub-chapter 18.1 and section 2.3.9 of this sub-chapter.

2.3.6. Availability requirements

The MCS [SICS] is a diverse back-up to the MCP [PICS].

2.3.7. Performance requirements

The MCS [SICS] is subject to the following performance criteria:

- response time requirements: as for the MCP [PICS] (see Sub-chapter 7.5), the MCS [SICS] must meet response time requirements. The use of hardwired links for the transmission of data, without data processing, guarantees that the response time is equal to or less than for the MCP [PICS].
- sizing requirements: the MCS [SICS] must support all the conventional control and monitoring devices necessary for the operator to perform the tasks described in section 2.1 of this sub-chapter, without requiring any resources from the MCP [PICS]. Notably, operation from the MCS [SICS] must be possible without the plant overview panel.

2.3.8. Environmental requirements

As the MCS [SICS] panels are installed in the MCR, the environmental requirements that it has to withstand are those of the MCR.

The conditions are classified into two categories:

- the environmental conditions that the equipment must endure. This includes temperature and relative humidity,
- the contribution of the equipment to the environmental conditions. This includes noise level and dissipated heat.

2.3.9. Human-machine interface requirements

The arrangement of the MCS [SICS] into panels must meet ergonomic requirements (suitability for operator tasks), independence requirements (mainly physical separation) between I&C Safety Features connected to different divisions and with different levels of qualification.

The detailed list of different information and controls that must be provided by the MCS [SICS] is determined by analysing the activities that must be performed by the shift team. Information related to the I&C Functions implemented on the MCS [SICS] can be found in Sub-chapter 18.1.

The operational HMI for the MCS [SICS] is provided by the level 2 I&C systems (see section 1.1 of Sub-chapter 7.2).

2.4. ARCHITECTURE

2.4.1. Structure and composition

The MCS [SICS] consists of a set of mainly conventional controls and displays (push buttons, light indicators, analogue displays, recorders etc.) that are directly connected to the appropriate level in the I&C architecture (RPR [PS], NCSS, RCSL, SAS, RRC-B SAS or PAS) and arranged on the panels. Due to its nature, the MCS [SICS] has no data processing capability and receives information from level 1 systems.

2.4.2. Installation

The MCS [SICS] panels are installed in the MCR.

2.4.3. Interfaces with other I&C systems

The MCS [SICS] has two types of interfaces:

- interface with the operator in the MCR;
- interface with the automation level (RPR [PS], NCSS, RCSL, PAS, SAS and RRC-B SAS).

The MSC [SICS] will have two-way communications to systems of a lower classification. The controls and indications are implemented within conventional circuits and will be isolated from circuits of other systems [Ref-1]. There will therefore be no means by which the signals from a lower class system could influence those from a higher class system. As described in section 2.0.3.1.5, all MCS [SICS] equipment will be Class 1.

2.5. OPERATING CONFIGURATIONS

The MCP [PICS], in the MCR, is the preferred means of operating the plant. The operating team operates from the MCS [SICS] in the event of unavailability of the MCP [PICS] in the MCR.

It would require a fundamental change to the current operating philosophy, design changes across the RPR [PS], SAS and PAS, and changes to planned operating procedures and the periodic testing regime in order for both the MCS [SICS] and MCP [PICS] to be fully operational at all times, in parallel. Currently the operating philosophy is that there is a single point of control and that the information for that control point is available to all operators. As the MCS [SICS] controls and displays are behind the normal operating positions, they are out of the field of view of the operators. The MCS [SICS] auto-accepts all alarms when it is not in use, so a changeover would still be needed to bring it into use. The MCS [SICS] would need to be disabled for periodic testing and for operation from the RSS.

In the event of the loss of the MCR due to an internal hazard (such as fire), operation from MCS [SICS] and the MCP [PICS] in the MCR is no longer possible. In that situation, the operating team uses the MCP [PICS] and PSOT control facilities in the RSS. During this procedure, a manual reactor trip is required. This command is provided on the inter workstation console (PIPO).

The principles of transfer between the different control facilities are managed by the operating procedures.

Typically the MCS [SICS] modes of operation are as follows:

- State 1: passive state:
  - MCS [SICS] controls are deactivated;
  - Information is operational.
  - Alarms are initiated, automatically accepted and audible notification is muted.
- State 2: active state:
  - MCS [SICS] controls are activated;
  - Alarms are manually managed via MCS [SICS].
  - The MCP [PICS] and PSOT controls are deactivated.

2.6. TECHNOLOGY

The standard technical solution for the MCS [SICS] is based on the use of conventional technology, except for a few specific devices such as chart recorders and digital indicators. The choice of equipment conforming to the requirements stated in this sub-chapter will be defined following completion of detailed studies.

2.7. POWER SUPPLY

The MCS [SICS] is supplied by 230V AC sources from four divisions in such a way that the loss of an electrical division does not lead to the total loss of the MCS [SICS]. Each control facility is supplied by its own electrical division, which is backed-up by the Emergency Diesel Generator.

The controls and indications for the conventional island are supplied by equipment in the non-classified electrical building.

Isolation measures are provided to maintain the electrical separation of the MCS [SICS] equipment of the different divisions.

The description of the power supply distribution of the NI is given in Sub-chapter 8.3.

2.8. PROVISIONS FOR PERIODIC TESTING

The MCS [SICS] must be periodically tested and hence the MCS [SICS] configuration (in particular “State 2” described in section 2.5 of this sub-chapter) must therefore allow such testing.

Testing of each of the I&C Functions that are subject to periodic testing will allow verification of the complete control channel, from the sensor (automatic control), or from the MCS [SICS] (manual control), via the I&C processing equipment, up to the change of state of the actuator.

However, if the actuation of an actuator under test is not acceptable (e.g. during plant operation), then provisions are made to block the control signals during the test, so that the actuator control line can be tested without actually changing the actuator state.

SUB-CHAPTER 7.3 – REFERENCES

External references are identified within this sub-chapter by the text [Ref-1], [Ref-2], etc at the appropriate point within the sub-chapter. These references are listed here under the heading of the section or sub-section in which they are quoted.

1. PROTECTION SYSTEM (RPR [PS])

[Ref-1] PS (incl. RPI sw) / RCSL / SA I&C / PIPS TELEPERM XS I&C System Engineering Quality Plan. PEL-F DC 7 Revision A. AREVA. June 2012. (E)

[Ref-2] TXS I&C Systems Verification and Validation Plan. PELV-F DC 28 Revision A. AREVA. June 2012. (E)

[Ref-3] I&C TXS Cabinets Qualification Program. NLZ-F DC 3 Revision C. AREVA. July 2007. (E)

[Ref-4] PS dependability program. NLE-F DC 25 Revision B. AREVA October 2006. (E)

[Ref-5] Protection System – System Description. NLN-F DC 193 Revision C. AREVA. April 2012. (E)

[Ref-6] J. Latour. Protection System - Functional Diagrams. NLN-F DC 89 Revision A. AREVA. December 2009. (E)

NLN-F DC 89 Revision A is the English translation of NLE-F DC 44 Revision E.

[Ref-7] Protection System – Concept for I&C failure handling. NLE-F DC 33 Revision C. AREVA. June 2007. (E)

[Ref-8] Protection System – Concept for periodic test. NLE-F DC 34 Revision E. AREVA. March 2010. (E)

[Ref-9] Protection System – Concept for Signal Annunciation. NLE-F DC 35 Revision F. AREVA. July 2009. (E)

[Ref-10] Protection System – Principle for manual commands. NLE-F DC 42 Revision B. AREVA. March 2008. (E)

[Ref-11] P. Martinet. Reactor Trip Concept. NLE-F DC 124 Revision B. AREVA. June 2008. (E)

[Ref-12] System Design Manual - Reactor Protection System (RPR), Part 2 – System operation. NLE-F DC 59 Revision C. AREVA. June 2007. (E)

[Ref-13] System Design Manual - Reactor Protection System (RPR), Part 3 – System sizing. NLE-F DC 58 Revision C. AREVA. April 2007. (E)

[Ref-14] System Design Manual - Reactor Protection System (RPR), Part 4 – Flow Diagrams. NLE-F DC 77 Revision B. AREVA. March 2007. (E)

[Ref-15] System Design Manual - Reactor Protection System (RPR), Part 5 – Instrumentation and Control. NLE-F DC 66 Revision E. AREVA. July 2008. (E)

[Ref-16] TELEPERM XS Engineering Procedure Calculation of Response Time and Accuracy of TELEPERM XS channels. NLE-F DM 10014 Revision C. AREVA. September 2010. (E)

[Ref-17] TELEPERM XS Engineering Procedure - Methodology for RAMS Studies. NLE-F DM 10032 Revision A. AREVA. June 2010. (E)

[Ref-18] UK EPR GDA - Basis of substantiation for the Reliability Claims for Sensors and Conditioning Modules. PELA-F DC 7 Revision B. AREVA. October 2012. (E)

1.0. SAFETY REQUIREMENTS

[Ref-1] Massini. IEC61513 ed. 2001 §6.1.1 Mapping to FA3 PS documentation. AREVA. June 2012. (E)

1.0.3. Design requirements

1.0.3.3. Hazards

[Ref-1] Analysis of the digital CCF within systems supporting F1A safety-class functions (PS) in the instrumentation & control architecture of the FA3 EPR. ENSECC080054 Revision A1. EDF. August 2009. (E)

1.3. DESIGN BASIS

1.3.2. Separation

1.3.2.1. Segregation of redundant equipment of the RPR [PS]

[Ref-1] Independence of the Class 1 Protection System (PS), the Safety Automation System (SAS) and the Non-Computerised Safety System (NCSS). ECECC111963 Revision C. EDF. August 2012. (E)

1.3.2.4. Independence between diverse functions

[Ref-1] Overall Approach to Diversity of UK EPR I&C Systems. ECECC121713 Revision A. EDF. August 2012. (E)

1.3.3. Detection of degraded states

[Ref-1] Justification of PS Reliability. PELL-F DC 233 Revision B. AREVA. June 2012. (E)

[Ref-2] TXS Self-monitoring and fail safe behaviour. NLTC-G/2008/en/0079 Revision B. AREVA. November 2008. (E)

1.3.8. Human machine interface requirements

[Ref-1] Protection System – System Description. NLN-F DC 193 Revision C. AREVA. April 2012. (E)

1.4. ARCHITECTURE

1.4.1. Structure and composition

1.4.1.3. Composition

1.4.1.3.1. Class 1 part of the RPR [PS]

[Ref-1] Protection System Operator Terminal Basis of Safety Case. ECECC120489 Revision A. EDF. May 2012. (E)

[Ref-2] Protection System Operator Terminal (PSOT) – Functional Scope. ECECC120711 Revision A. EDF. July 2012. (E)

1.4.1.4. Diversity and common cause failures

[Ref-1] Diversity Criteria between Protection System and Safety Automation System. PTL-F DC 3 Revision B. AREVA. August 2012. (E)

[Ref-2] Methodology and Organization for Diversity Management between I&C Platforms and I&C Systems. PTL-F DM 1 Revision B. AREVA. June 2012. (E)

1.4.3. Interfaces with other I&C systems

[Ref-1] TELEPERM XS based systems. Concept for Electrical Separation. NLE-F DC 249 Revision E. AREVA. January 2011. (E)

1.4.3.1. Inputs

[Ref-1] Protection System – System Description. NLN-F DC 193 Revision C. AREVA. April 2012. (E)

[Ref-2] Analysis of the non disturbance of the Protection System by lower classified signals coming for systems in interface. PELL-F DC 252 Revision A. AREVA. April 2012. (E)

1.7. PROVISIONS FOR MAINTENANCE AND I&C TESTS

1.7.1. Maintenance

[Ref-1] Protection System – System Description. NLN-F DC 193 Revision C. AREVA. April 2012. (E)

2. SAFETY INFORMATION AND CONTROL SYSTEM (MCS [SICS])

[Ref-1] System Specification for KSC Plant System: Safety Information and Control System and layout of Main Control Room, Remote Shutdown Station and Emergency Technical Centre. ECECC060019 Revision A1. EDF. July 2010(E)

[Ref-2] Sizing of SICS, ECEF021069 Revision E1. EDF. December 2010. (E)

[Ref-3] C. Botta. System Design Manual - Main Control Room (KSC [MCR]), Part 5: Control and Instrumentation System (KSC [MCR]) EPR FA3 (Stage 2). ECECC070760 Revision B1. EDF. November 2009. (E)

[Ref-4] System specification file (DSS). SY710 Version 6.0. Siemens. March 2009. (E)

[Ref-5] J. Latour. Overall Architecture Drawing. NLN-F DC 91 Revision A. AREVA. December 2009. (E)

NLN-F DC 91 Revision A is the English translation of NLF-F DC 10 Revision E.

2.0. SAFETY REQUIREMENTS

2.0.1. Safety functions

[Ref-1] Sizing of SICS. ECEF021069 Revision E1. EDF. December 2010. (E)

2.0.2. Functional criteria

2.0.2.2. When MCP [PICS] is not available

2.0.2.2.2. In case of loss of the MCP [PICS] in addition to a PCC-2 to PCC-4 event

[Ref-1] Sizing of SICS, ECEF021069 Revision E1. EDF. December 2010. (E)

2.0.3. Design requirements

2.0.3.1. Requirements resulting from the functional classifications

2.0.3.1.2. Single failure criterion

[Ref-1] Sizing of SICS. ECEF021069 Revision E1. EDF. December 2010. (E)

2.3. DESIGN BASIS

2.3.1. Redundancy

[Ref-1] Sizing of SICS. ECEF021069 Revision E1. EDF. December 2010. (E)

2.3.2. Separation

[Ref-1] Generic rules for the Electrical Isolation of EPR UK Instrumentation and Control Systems (Internal Connections and Interfaces).
ECECC111058 Revision B. EDF. June 2012. (E)

2.4. ARCHITECTURE

2.4.3. Interfaces with other I&C systems

[Ref-1] Generic rules for the Electrical Isolation of EPR UK Instrumentation and Control Systems (Internal Connections and Interfaces).
ECECC111058 Revision B. EDF. June 2012. (E)