UK EPR	Title: PCSR – Sub-chapter 7.4 – Class 2 instrumentation and control systems **UKEPR-0002-074 Issue 04**
Total number of pages: 38	Page No.: I / V
Chapter Pilot: B. WORINGER *Name/Initials* B. Woringer *Date* 30-10-2012	
Approved for EDF by: A. MARECHAL *Name/Initials* A.JC.Marechal *Date* 31-10-2012	Approved for AREVA by: G. CRAIG *Name/Initials* G Craig *Date* 31-10-2012

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA information	14-01-2008
01	Integration of technical and co-applicant review comments	29-04-2008
02	PCSR June 2009 update: - Clarification of text - References added - SAS RRC-B added (new section 4) - SA I&C added (new section 5) - Text regarding periodic testing of the RCSL updated (sections 3.0.4.2 and 3.8.2). - Section 7.4.3 – Figure 2 updated	30-06-2009
03	Consolidated Step 4 PCSR update: - Minor editorial changes - Clarification of text - Update and addition of references - Safety Automation System (SAS) (new section 1) added; previously in Sub-chapter 7.4 - Non Class 2 systems (PICS, PAS, SAS RCC-B and SA I&C) removed to Sub-chapter 7.5 - Update of Safety Function Categorisation and SCC Classification to clearly summarise Category A, B, C and Class 1, 2, 3 for I&C scope - Architecture: RCSL is now Class 2; text updated accordingly - Electrical and functional isolation for interfaces to systems of different safety class - Text updated to address diversity between lines of defence in depth - NCSS added (section 3)	29-03-2011

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 (§1.0, §1.0.1, §1.3.2, §2.0, §2.0.1, §3, §3.0.1) - Update of text regarding SAS implementing category A function (§1.0, §1.0.2, §1.1, §1.4.1) - Update of text regarding SAS interfaces with other I&C systems (§1.4.3) - Clarification of classification of test equipment added (§1.8, §2.8, §3.8) - Clarification on RCSL links to SAS (§2.4.1, Section 7.4.2 - Figure 1) - Updates to NCSS section to account for current functions performed and architecture (§3)	31-10-2012

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 7.4 – CLASS 2 INSTRUMENTATION AND CONTROL SYSTEMS

1. SAFETY AUTOMATION SYSTEM (SAS)

Note: Refer to the quality plans, system specification reports and overall architecture drawings for more detailed information on the Safety Automation System (SAS) [Ref-1] to [Ref-14].

1.0. SAFETY REQUIREMENTS

The SAS is subject to the safety requirements applicable to Class 2 systems, due to its management of the Category B I&C Functions. As a diverse line of protection, SAS also contributes to 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].

The SAS enables the processing of automatic and manual actions, together with the associated monitoring, necessary for the performance of the safety functions detailed as follows:

1.0.1. Safety functions

As part of the management of I&C processing, the SAS is required to contribute to the three basic safety functions:

- control of fuel reactivity;
- fuel heat removal;
- confinement of radioactive material.

1.0.2. Design requirements

The SAS Class 2 I&C Safety Features are involved in the fulfilment of Category B I&C Functions, and Category A I&C Functions whilst operating as a line of protection diverse from the RPR [PS]. It must therefore meet the requirements detailed below. These requirements must be met for all the functions managed by the SAS (including those Priority and Actuator Control (PACS) functions processed by SAS equipment, refer to Sub-chapter 7.2).

1.0.2.1. Requirements resulting from the functional classification

1.0.2.1.1. Functional classification of the system

The SAS must be safety classified according to the principles specified in Sub-chapter 3.2.

1.0.2.1.2. Single failure criterion

The single failure criterion must be applied to the SAS at the functional level (see Sub-chapter 3.2) by integrating a sufficient degree of redundancy, structure and adequate equipment provision.

The system must be designed with sufficient redundancy to continue to process Category B I&C Functions even in the event of equipment being unavailable due to testing, and other equipment being assumed unavailable due to application of the single failure criterion (at the functional level for Class 2 I&C Safety Features).

Independence and physical separation: In order to meet this requirement, the SAS will require physical and electrical independence of the equipment in the four I&C divisions upon which it depends.

1.0.2.1.3. Emergency power supplies

The electrical power supply for the SAS equipment must be backed-up by the emergency diesel generators. Moreover, the power supply must be “uninterruptible”, guaranteeing the power supply even during switching between normal power and diesel power (i.e. it must ensure that the SAS I&C Functions can continue without interruption).

The SAS must be powered from the same division as that of the processes it actuates, each division being electrically and physically independent of the three others in a way that eliminates the possibility that a single hazard or failure can affect more than one division.

1.0.2.1.4. Qualification under operating conditions

The SAS equipment must remain operational in post-accident conditions, and must therefore meet the qualification requirements defined in Sub-chapter 3.6.

Moreover, this equipment must be operational in both normal and extreme environmental conditions applicable to the automation rooms in which it is located. These conditions are defined in section 1 of Sub-chapter 9.4.

1.0.2.1.5. 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.

Some I&C Functions implemented in SAS may be performed using I&C equipment of a higher class than is required by the safety classification principles defined in Sub-chapter 3.2. In some cases, this can simplify the design.

1.0.2.1.6. Seismic classification

The SAS equipment meets the seismic requirements defined in Sub-chapter 3.2.

1.0.2.1.7. Periodic testing

The I&C Functions managed by the SAS must be tested periodically (as defined in section 1 of Sub-chapter 3.2).

The SAS must be designed to allow periodic tests.

1.0.2.1.8. Additional requirements

Not applicable.

1.0.2.2. Hazards

The SAS must be protected against common cause failures which can be generated by internal or external hazards according to the requirements defined in Sub-chapter 3.1 (external and internal hazards). This leads to a requirement for independence (physical and electrical) of each of the four divisions housing the SAS equipment.

1.0.3. Tests

After installation, the SAS must be subject to pre-operational testing to verify that it conforms to the system performance required by the design.

The requirements for periodic testing are set out in section 1.0.2.1.7 of this sub-chapter.

1.1. ROLE

The role of the SAS is to manage Class 2 I&C Safety Features involved in post-accident management and to provide a diverse digital system from the Protection System (RPR [PS]) (see section 1.2).

Whilst operating as a diverse line of protection from the RPR [PS], the SAS is capable of carrying out Category A I&C Functions, that do not require Class 1 properties. (Refer to section 1.3.2 of Sub-chapter 7.2 for a justification of this statement.)

It should be noted that the RCC-B SAS is a separate system (refer to section 1 of Sub-chapter 7.5 for details) and is independent of the SAS and other SPPA-T2000 based systems [Ref-1].

1.2. FUNCTIONS PERFORMED

The SAS carries out the following instrumentation and control functions:

- **Data processing:** acquisition and conditioning
- **Processing of application calculations:** closed loop controls, generation of individual and grouped commands (simultaneous or sequential), controls prioritisation, generation of various information intended for other I&C units, etc.
- **Processing of monitoring signals:** Processing of status and fault check-backs, generation of alarms and indications.

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

In addition, the SAS monitors the MCP [PICS] life-sign. The corresponding MCP [PICS] status signal is displayed on the Inter-Panel Signalisation Panel (PSIS). The MCP [PICS] status is used by the operator to know when to transfer control to the MCS [SICS], in the event of unavailability of the MCP [PICS].

1.3. DESIGN BASIS

1.3.1. Availability requirements

The main availability requirements for the SAS are linked to the reliability and the maintainability of the system i.e.

- to limit the loss of SAS due to failure of one of its components (mainly by component redundancy),
- to facilitate the maintenance and repair of the SAS to minimise downtime.

1.3.2. Performance requirements

The SAS must fulfil the performance requirements of the I&C Functions in terms of response time and accuracy as derived from the functional requirements.

- Response time requirements:
  - maximum time from the variation of an input (logic or analogue) to its transmission to an output interface;
  - maximum time from the receipt of a manual command to its transmission to an output interface.

These global criteria are applied to the SAS as follows:

- for a MCP [PICS] manual command, refer to section 2 of Sub-chapter 7.5;
- for an automatic command:
  - acquisition of a logic input, calculation of a logic command, and transmission to an output interface;
  - acquisition of an analogue input, calculation of a logic or analogue command, and transmission to an output interface.

The SAS must contribute to fulfilling the global criteria described above and in section 2 of Sub-chapter 7.5.

In particular, the two acquisition, processing and transmission actions performed by the SAS must be compatible with the required total response time (including MCS [SICS] or MCP [PICS], SAS and level 0).

- Sizing requirements:
    - o static sizing includes the number of actuators, sensors and functions that the SAS supports;
    - o dynamic sizing includes sampling and processing times, taking into account the way in which the functions are processed (periodically or event-triggered).

1.3.3. Environmental requirements

The environmental conditions that the SAS must tolerate are dictated by the temperature and relative humidity of the rooms housing this equipment. The environmental characteristics are defined in Sub-chapter 9.4, for normal and extreme conditions.

1.3.4. Human-machine interface requirements

The SAS must interface with an engineering HMI to enable safe, effective and error-free commissioning, maintenance, periodic testing and configuration of the SAS.

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

1.4. ARCHITECTURE

1.4.1. Structure and composition

The structure and composition of the SAS are dictated by the functional requirements. This set of requirements affects the allocation of I&C processing tasks to the various components within the SAS.

These functional requirements relate to the following:

- The safety classification of the processed I&C Functions (typically Category B for SAS), although, in certain situations the SAS could be required to process certain Category A, Category C and non-classified I&C Functions;
- The electrical division (together with the processing cabinet, and associated actuators and sensors);
- The classification of processing to be performed (affecting the choice of input/output card types for example);
- The processing performance requirements (response times, propagation times, accuracy);
- The processing groupings/exclusions which require certain processes to be grouped (due to the requirement to simultaneously shut down all these processes in the event of malfunction of part of the I&C system that manages it), or conversely, that certain processing groups need to be managed by different SAS equipment units (due to the requirement to maintain a group of processes despite the loss of others due to a malfunction).

Moreover, the SAS structure takes into account the segmentation of the process being controlled, dictated by the number, geographic location and type of actuator and sensor interfaces to be managed.

For a given safety function, different combinations are possible, for example:

- 4 x 100%: 1 mechanical train out of 4, with its associated I&C, is necessary to fulfil the safety function;
- 4 x 50%: 2 mechanical trains out of 4, with their associated I&C, are necessary to fulfil the safety function;
- 2 x 100%: 1 mechanical train out of 2, with its associated I&C, is necessary to fulfil the safety function.

In order to prevent a SAS internal failure affecting more than one mechanical train, each mechanical train is controlled by a SAS sub-group in the same division as the mechanical train.

This section outlines the functional requirements of the SAS and considers the section of the process to be controlled for a given safety function. Diagnostic self tests are performed throughout the SAS. These include tests performed within modules, between modules and between system components [Ref-1].

1.4.2. Installation

The SAS equipment is distributed within the four divisions. The equipment is installed in the I&C cabinet rooms of divisions 1 to 4 in the safeguard buildings and in the I&C cabinet rooms in the diesel buildings.

With regard to the position of the SAS cabinets, the following are taken into consideration:

- consistency with the location and division of the actuators and the sensors to be managed;
- available space;
- consistency with the electrical supplies of the four divisions.

1.4.3. Interfaces with other I&C systems

The SAS exchanges information with the following:

- the HMI, MCS [SICS] in the MCR and MCP [PICS] in both the MCR and RSS: for plant operation by the operator;
- the Process Automation System (PAS) and RPR [PS]: for the plant automation management;
- the Non-Computerised Computer System (NCSS) to provide the life-sign of the SPPA-T2000 systems;
- the instrumentation process for measurement and data acquisition;

- the switchgear units (electrical boards) and the control devices (electro-positioners, etc) for actuator control;
- the "external" systems (I&C cabinets for the diesels, etc): for the unit automation management.

A dedicated Class 2 SAS bus network is used for the transmission of signals up to Class 2, between SAS equipment.

The SAS will provide alarms if it detects that the MCP [PICS] is not operational [Ref-1].

The input and output modules of the SAS are designed to ensure the required electrical isolation [Ref-2].

Refer to section 1.4.3 of Sub-chapter 7.3 for details of how the SAS interfaces with the RPR [PS].

1.5. OPERATING CONFIGURATIONS

The configuration of the SAS (from hardware and functional points of view) is independent of the plant situation. Processing allocation depends only on functional criteria and on the allocation principles of the I&C system. The configuration of SAS is, from this point of view, constant.

The SAS configuration only depends on the following principle: in the event of malfunction of an active CPU, the system switches to a redundant standby unit. This principle applies to all the redundant SAS boards (CPU boards and communication management boards).

As mentioned above, the SAS configuration includes a SAS bus Class 2 network interface, unlike the RRC-B SAS.

1.6. TECHNOLOGY

The equipment used to implement the SAS is the digital I&C system based on the SPPA-T2000 platform [Ref-1].

1.7. POWER SUPPLY

Within each division, the I&C cabinets of the SAS are supplied by a dual power supply, via independent AC/DC converters and DC/DC converters. One power supply is provided by a 400V AC supply and the other by a 220V DC supply with appropriate converters.

Each mechanical train is controlled by a SAS sub-group located and powered by the same division as the mechanical train.

The voltage required by the SAS cabinets will be regulated internally in dedicated power supply cabinets. These power supply cabinets are situated in the same rooms as the SAS cabinets.

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

1.8. PROVISIONS FOR PERIODIC TESTING

The safety function test will allow the verification of the whole control channel, from the sensor (automatic control), or from the MCS [SICS] / MCP [PICS] (manual control), via SAS, up to the change of state of the actuator.

However, if the reconfiguration of the relevant actuator cannot be carried out (for example, during the plant operation), provisions are taken for blocking the control signals during the test, so that the actuator control line can be tested without physically controlling it.

In addition, the SAS executes self-tests during start up and cyclic program processing and at the time of synchronization by comparison between redundant sub-units [Ref-1].

Any equipment used to test the SAS will be at least Class 3. 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.

2. REACTOR CONTROL, SURVEILLANCE AND LIMITATION SYSTEM (RCSL)

Note: Refer to the quality plans, system specification reports and overall architecture drawings for more detailed information on the Reactor Control, Surveillance and Limitation System (RCSL) [Ref-1] to [Ref-10].

2.0. SAFETY REQUIREMENTS

The RCSL is subject to the safety requirements applicable to Class 2 systems, due to its management of I&C Functions up to Category B.

The requirements are detailed in several documents, which provide all the required information contained within an IEC 61513 compliant system requirements specification as demonstrated for the RPR [PS] in section 1.0 of Sub-chapter 7.3.

2.0.1. Safety functions

As part of the management of I&C processing, the RCSL is required to contribute to the following main safety functions:

- control of fuel reactivity;
- fuel heat removal.

2.0.1.1. Functional criteria

The RCSL provides automatic control, Limiting Conditions of Operation (LCO) and limitation functions, for core parameters.

It monitors the core physical parameters and when needed initiates various LCO or limitation functions, such as partial reactor trip.

2.0.2. Design requirements

2.0.2.1. Requirements resulting from the functional classification

2.0.2.1.1. Functional classification of the system

The RCSL must be safety classified according to the principles specified in Sub-chapter 3.2.

2.0.2.1.2. Single failure criterion

RCSL is a Class 2 system used for normal operation. Therefore there is no single failure requirement applicable to the RCSL.

2.0.2.1.3. Emergency power supplies

The electrical power supply for the RCSL equipment must be backed-up by the emergency diesel generators. Moreover, the power supply must be “uninterruptable”, guaranteeing the power supply even during switching between normal power and diesel power (i.e. it must ensure that the RCSL I&C Functions can continue without interruption).

The RCSL must be powered from the same division as that of the processes it actuates. Each division is electrically and physically independent of the others in a way that eliminates the possibility that a single hazard or failure can affect more than one division.

2.0.2.1.4. Qualification under operating conditions

The equipment must be operational in normal environmental conditions applicable to the rooms in which it is located. These conditions are defined in section 1 of Sub-chapter 9.4.

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

2.0.2.1.5. Electrical and I&C classifications

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

Some I&C Safety Features implemented in the RCSL may be performed using I&C equipment of a higher class than is required (Class 2 instead of Class 3 for example). In some cases, this can simplify the design.

2.0.2.1.6. Seismic classification

The RCSL is designed with seismic requirements consistent with the principles given in Sub-chapter 3.2.

2.0.2.1.7. Periodic testing

The I&C Functions managed by the RCSL must be tested periodically (as defined in section 1 of Sub-chapter 3.2). The RCSL must be designed to allow periodic tests.

Since the control rods are moved periodically during normal operation, periodic tests are performed via the regular surveillances of these rod measurements. It is expected that periodic tests will be performed on all other parts of the RCSL (e.g. on the instrumentation used in RCSL functions) and on the shutdown rods.

2.0.2.1.8. Additional requirements

None.

2.0.2.2. Hazards

The RCSL is required to be protected against common cause failures which may be generated by internal or external hazards according to the requirements defined in Sub-chapter 3.1 (external and internal hazards). This leads to a requirement for independence (physical and electrical) between each of the redundant parts of the RCSL equipment.

2.0.3. Tests

Pre-operational tests must prove the adequacy of the design and the performance of the RCSL.

2.1. ROLE

The RCSL is required to contribute to the normal operation of the plant (PCC-1) and controls and monitors core parameters.

2.2. FUNCTIONS PERFORMED

As defined in section 1 of Sub-chapter 7.2, the RCSL performs Category B and Category C I&C Functions to control and to monitor operations related to the core. These include:

- Core control functions;
- Core related LCO functions;
- Core related limitation functions;
- Operator Aid 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 RCSL.

A list of the typical application functions performed by the RCSL is given in Section 7.4.2 - Table 1.

The RCSL also performs some primary and secondary limitation and LCO functions.

2.3. DESIGN BASIS

2.3.1. Availability requirements

The RCSL is only required to operate in normal operating conditions.

2.3.2. Performance requirements

Performance requirements in terms of response time and accuracy are derived from the functional requirements.

2.3.3. Environmental requirements

2.3.3.1. Normal conditions

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

2.3.3.2. Accident conditions

The RCSL is not required to remain operational in post-accident conditions.

2.3.4. Human-machine interface requirements

The RCSL must interface with an engineering HMI to enable safe, effective and error-free commissioning, maintenance, periodic testing and configuration of the RCSL.

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

2.4. ARCHITECTURE

Note that the allocation of controls to RCSL is to be decided and could impact the architecture described in this section.

2.4.1. Structure and composition

As shown in Section 7.4.2 – Figure 1, The RCSL is composed of four parts:

- An Acquisition Unit (AU). This acquires the signal from the sensors. There is one AU per division. The acquisition of redundant sensors is distributed between the four AUs;
- Control Unit (CU). This processes the I&C Functions of the RCSL. There are two CUs: one in division 1 and one in division 4;
- Drive Units (DUs). These condition the signals sent to the RodPilot® which manages the rod positions, or other I&C systems, on request of the computations of the CU. There are four DUs, two in division 1 and two in division 4. Half of the rods are driven by the DU in division 1, the other half by the DU in division 4;
- Interface with PAS and level 2. This is composed of:
    - Two Message and Service Interface (MSI) units dedicated to the monitoring of the RCSL and the management of interfaces (with PAS, level 2 and service unit);
    - Two gateways ensuring the interface with PAS and MCP [PICS];
    - Dedicated hardwired links to MCS [SICS];

- One Service Unit (SU) dedicated to ensure the maintenance, periodic testing facilities and diagnosis function of the RCSL.

A summary description of the RCSL is provided in Section 7.4.2 – Table 2.

A typical allocation of an RCSL I&C Function is provided in Section 7.4.2 – Figure 2.

The design of the RCSL is based on two channels of redundancy.

Redundancy of the processing units:

The two Control Units (CUs) process the same I&C Functions. In the pair, one CU is the master and the other is in stand-by mode.

Redundancy of the drive units:

The two DUs of the same division are redundant and generate the same outputs.

Redundancy of the interface with the PAS and level 2:

The two MSI and Gateways, one located in each division, provide redundancy.

2.4.2. Installation

The RCSL acquisition level (AUs) is arranged within the I&C cabinet rooms of safeguard buildings 1 to 4.

The RCSL actuation level (DUs) is arranged within safeguard buildings 1 and 4. In order to reduce the amount of cabling, it will be installed if possible with the corresponding power electronic modules cabinet within the switchgear room.

The RCSL processing level (CUs) is also arranged within the I&C cabinet rooms of safeguard buildings 1 and 4.

The Service Unit is installed in the I&C Service Centre.

2.4.3. Interfaces with other I&C systems

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

2.4.3.1. Inputs

The RCSL receives inputs:

- from the Process Automation System (PAS):
  - process parameters;
- from the Protection System (RPR [PS]):
  - process parameters;

- signals for periodic tests;

- from the Control Rod Drive Mechanisms (CRDM):
  - state/status of the Control Rod Drive Mechanisms;
- from the Rod Position Instrumentation:
  - analogue rod position indications;
- from the Process Information and Control System (MCP [PICS]):
  - manual commands;
  - change of control rod sequence;
  - set-points.

Refer to Sub-chapter 7.3 section 1.4.3 for details of how the RCSL interfaces with the RPR [PS].

2.4.3.2. Outputs

The RCSL provides outputs to:

- the Process Automation System (PAS) with:
  - commands and set-points;
- the Control Rod Drive Mechanisms (CRDM) with:
  - the signals that control the currents in the coils;
- the Process Information and Control System (MCP [PICS]) with:
  - process parameters;
  - pre-processed alarms;
  - state/status of the Control Rod Drive Mechanisms;
  - state/status of the automatic controls;
  - status of RCSL (self-surveillance);
- the Safety Information and Control System (MCS [SICS]) with:
  - rod drop check backs;
  - TXS and cabinets alarms.

Refer to section 1.4.3 of Sub-chapter 7.3 for details of how the RCSL interfaces with the RPR [PS].

2.5. OPERATING CONFIGURATIONS

The RCSL comprises a set of computerised TXS units. The operating modes of the computerised TXS units are described in section 1 of Sub-chapter 7.3.

2.6. TECHNOLOGY

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

It is described in section 1.4 of Sub-chapter 7.3 and section 1 of Sub-chapter 7.7.

2.7. POWER SUPPLY

The RCSL I&C cabinets receive a separate double in-feed at 24V DC via independent AC/DC converters and DC/DC converters. The DC voltage is derived from an uninterruptible I&C power supply converter cabinet, connected to the 400V AC busbar or to 220V DC batteries busbar.

In the event of maintenance of the power supply of the division, one of the incoming feeders can be connected to the uninterrupted power supply of another division (1+2, 3+4). In order to cope with the loss of the on-site and off-site power supply, the uninterrupted power is supplied by 2 hour batteries.

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

2.8. PROVISIONS FOR PERIODIC TESTING

The self-test features of the TXS hardware and the use of the RCSL Service Unit for periodic testing fulfil the periodic testing requirements.

The periodic tests are performed in an overlapping manner, i.e. the instrumentation, the processing equipment and the actuator control are tested separately. This overlapping separate testing is performed in order to avoid multiple actuations of actuators, to maintain full plant availability and to test under operational conditions.

For maintenance purposes (software downloading, parameter modification, component replacement), the maintenance team must be able to work on the RCSL without impairing the operability of the system. In order to perform maintenance, internal tests or diagnosis it must be possible to switch off the unit for maintenance by means of the RCSL Service Unit and hardware release keys.

Any equipment used to test the RCSL will be at least Class 3. 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 7.4.2 - TABLE 1

Typical application functions performed by the RCSL

TYPICAL APPLICATION FUNCTIONS	TYPE OF APPLICATION FUNCTIONS		
	Control functions	LCO surveillance functions	Limitation functions
Closed loop control	X		
Open loop control	X	X	X
Combinatory control	X		
Alarm elaboration	X	X	X
CRDM control	X	X	X
Priority management	*Not specific to a type of application function*		

SECTION 7.4.2 - TABLE 2

Description of the RCSL

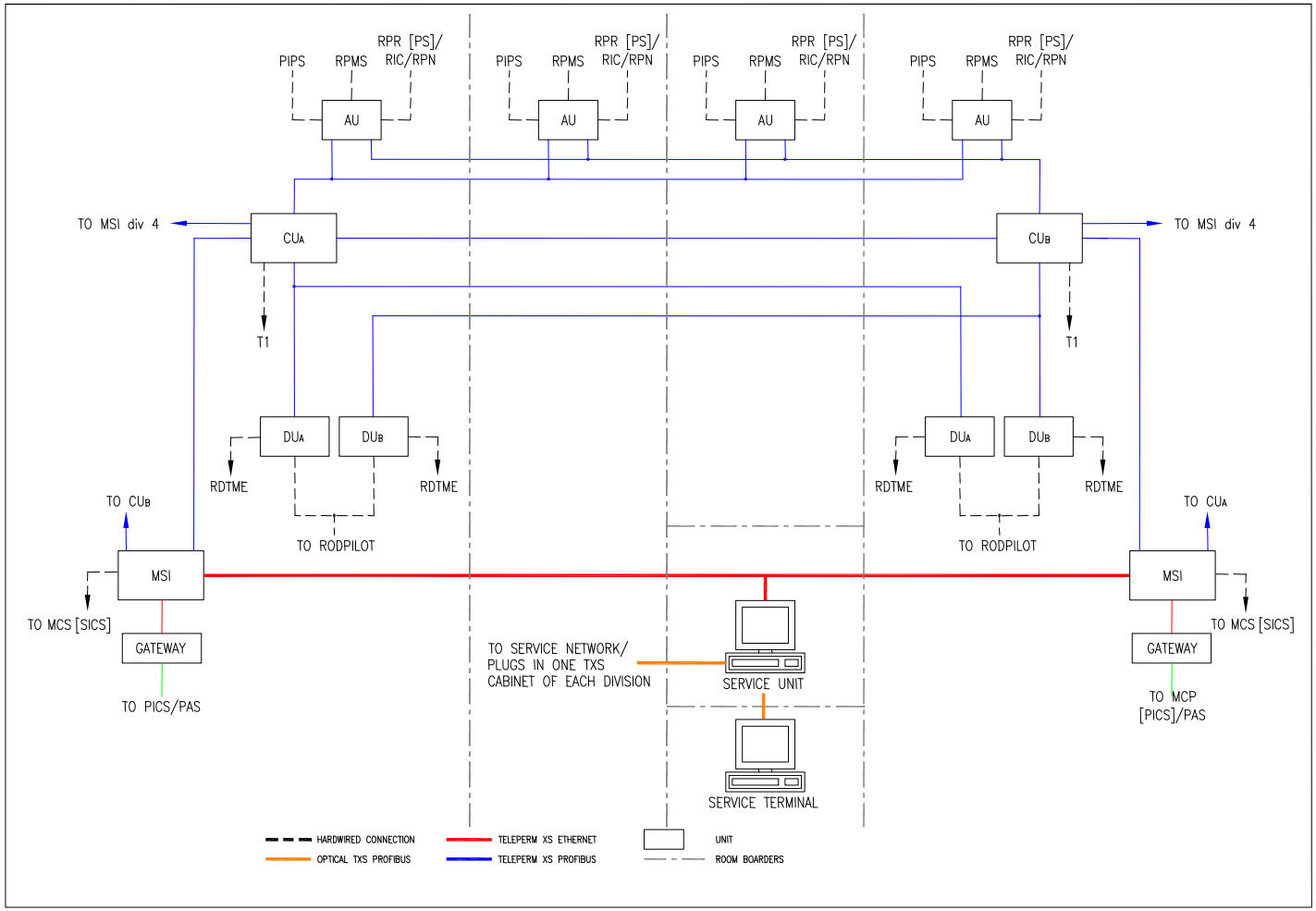
Unit	Redundancy and safety classification	Location (division)	Description
Acquisition Unit (AU)	The AUs perform the acquisition of input signals from redundant sensors. Class 2	1, 2, 3, and 4	Performs: - Acquisition of input signals from other I&C systems, from process systems and Rod Cluster Control Assembly (RCCA) analogue positions - Performance of pre-processing of control, LCO or limitation functions - Alarms

Control Unit (CU)	Redundant: one master/hot stand-by pair.
	Class 2
		1 and 4	Performs:
			- Voting/selection of input data (if necessary).
			- Automation controls:
			  - Closed loop controls
			  - Open loop controls
			  - Combinational controls.
			- Priority management between the different commands dedicated to the rods.
			- Alarms

Drive Unit (DU)	Two-fold redundant Class 2	Two in division 1 and two in division 4 (division location according to the location of the RCCAs)	Performs: - Management of the cycles of coil current according to the order received from the CU. - Calculation of a report of good or wrong execution of insertion: withdrawal commands - The RodPilot® also acquires reactor trip demands from the four divisions of RPR [PS] via hardwired connections; the trip is performed if at least 2/4 of the input signals are on.
Message and Service Interface (MSI)	Two-fold redundant Class 2	1 and 4	Performs the interface between: - processing units (AUs, CUs and DUs) and PAS - processing unit and level 2 - processing unit and service unit
Gateway	Two-fold redundant Class 2	1 and 4	Performs the interface between: - RCSL and PAS - RCSL and MCP [PICS]
Service unit	Non redundant NC	1	Performs: - Testing and diagnosis functions.

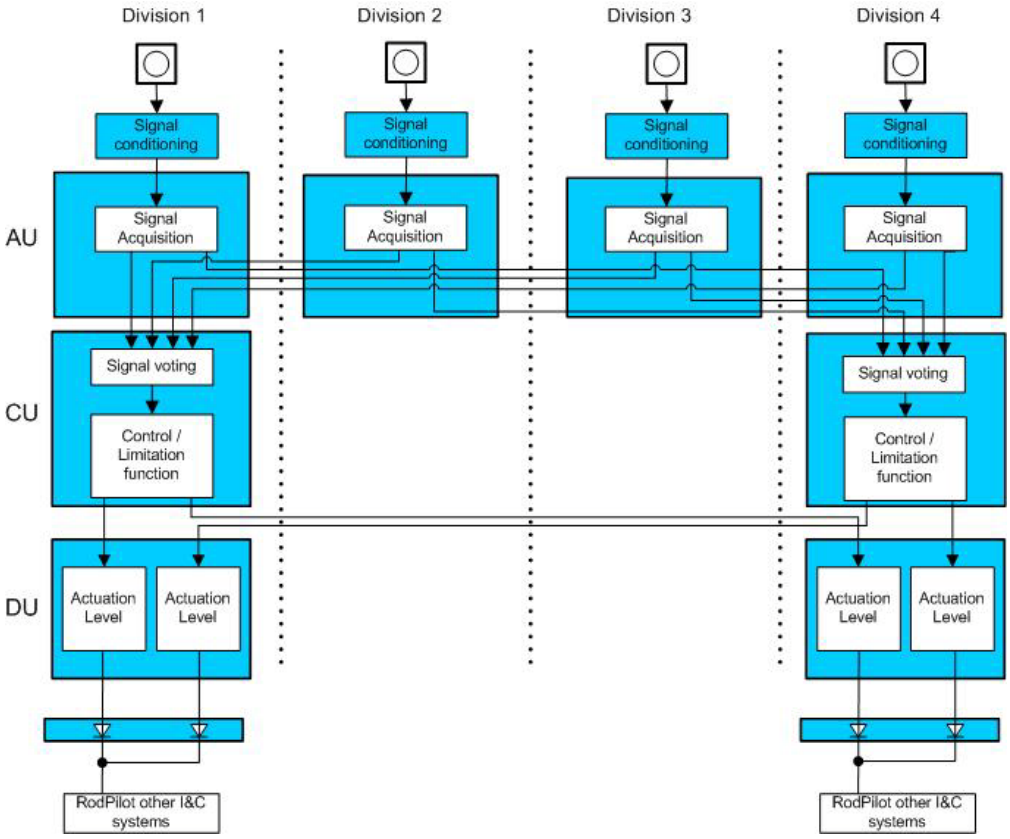
SECTION 7.4.2 - FIGURE 1

RCSL architecture



SECTION 7.4.2 - FIGURE 2

Typical allocation of RCSL I&C functions



3. NON-COMPUTERISED SAFETY SYSTEM (NCSS)

Note: Refer to the quality plans, system specification reports and overall architecture drawings for more detailed information on the Non-Computerised Safety System (NCSS) [Ref-1] to [Ref-12].

3.0. SAFETY REQUIREMENTS

3.0.1. Safety functions

As part of the management of I&C processing in the event of total loss of computerised I&C, the NCSS is required to contribute to the three main safety functions:

- control of fuel reactivity;
- fuel heat removal;
- confinement of radioactive material.

To meet the required overall reliability figures for I&C safety systems an additional, diversified and Non-Computerised Safety System (NCSS) has been introduced to ensure that the I&C system reliabilities are such that the design complies with Targets 8 and 9 of the HSE SAPs [Ref-1].

3.0.2. Design requirements

The NCSS must meet the requirements detailed below.

The diversity requirements for the NCSS have been assessed [Ref-1] [Ref-2].

3.0.2.1. Requirements resulting from the functional classification

3.0.2.1.1. Functional classification of the system

The NCSS must be safety classified, in accordance with the classification indicated in Sub-chapter 3.2.

3.0.2.1.2. Single failure criterion

The single failure criterion must be applied to the NCSS at the functional level (see Sub-chapter 3.2) by integrating a sufficient degree of redundancy, structure and adequate equipment provision. The NCSS must be designed to avoid spurious trip commands.

The system must be designed with sufficient redundancy to continue to process the I&C Safety Functions as detailed in section 3.0.1, even in the event of equipment being unavailable due to testing [Ref-1].

Independence and physical separation: The NCSS is subject to these requirements, which lead to the requirement for physical and electrical independence of the equipment in the four I&C divisions upon which it depends.

3.0.2.1.3. Emergency power supplies

The NCSS must be capable of operating in the event of a loss of offsite power. The power supply must be of the uninterruptible type (it must ensure that the NCSS safety functions can continue without interruption) [Ref-1].

The NCSS must be powered from the same division as that of the processes it actuates, each division being electrically and physically independent of the three others in a way that eliminates the possibility that a single hazard or failure can affect more than one division [Ref-2].

3.0.2.1.4. Qualification under operating conditions

The NCSS equipment must remain operational in post-accident conditions, and must therefore meet the qualification requirements defined in Sub-chapter 3.6.

Moreover, this equipment must be operational in both normal and extreme environmental conditions applicable to the rooms in which it is located. These conditions are defined in section 1 of Sub-chapter 9.4.

3.0.2.1.5. Electrical and I&C classifications

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

3.0.2.1.6. Seismic classification

The NCSS is designed with seismic requirements consistent with the principles given in Sub-chapter 3.2.

3.0.2.1.7. Periodic testing

The I&C Functions managed by the NCSS must be tested periodically (as defined in section 1 of Sub-chapter 3.2). The NCSS must be designed to allow periodic tests [Ref-1].

3.0.2.1.8. Additional requirements

It must be impossible for a fault in the computerised I&C systems to prevent the operation of the NCSS when required. This is in order to comply with the required reliability target for I&C. For these reasons, the NCSS must be diverse from the computerised I&C in as much as it must be implemented in a technology that does not rely on computers to operate [Ref-1].

Note: Although the NCSS will be built from components which are diverse from those of the computerised I&C, the purpose of the NCSS is not to provide diversity per se. Rather, it is diverse for the purpose of attaining a sufficiently high reliability when considered in combination with the computerised I&C.

3.0.2.2. Hazards

The NCSS must be protected against common cause failures which can be generated by internal or external hazards according to the requirements defined in Sub-chapter 3.1 (external and internal hazards). This leads to a requirement for independence (physical and electrical) of each of the four divisions housing the NCSS equipment [Ref-1].

3.0.3. Tests

After installation, the NCSS must be subject to pre-operational testing to verify that it conforms to the system performance required by the design.

The requirements for periodic testing are set out in section 3.0.2.1.7 of this sub-chapter.

3.1. ROLE

The NCSS is a non-computerised I&C system that is designed to bring the plant to a non-hazardous stable state following the Total Loss of Computerised I&C [Ref-1].

3.2. FUNCTIONS PERFORMED

The NCSS performs necessary automatic Reactor Trip (RT) and some Engineered Safety Features Actuation System (ESFAS) initiations and also provides manual commands enabling the operators to bring the plant to a non-hazardous stable state and maintain it in that state until the computerised I&C can be recovered [Ref-1] [Ref-2] [Ref-3].

The NCSS also provides indications to the MCR (MCP [PICS] or MCS [SICS]) (see section 3.4.1 for clarification) [Ref-4].

Category A (as a back-up line for Reactor Trip functions) and Category B and C I&C Functions are processed by hardwired circuits and logic to satisfy diversity requirements; Category C functions to communicate status information to the MCP [PICS] via the plant bus are implemented by a computerised gateway that has hardwired connections from the NCSS processing modules. Processing modules consist of non-computerised I&C equipment.

3.3. DESIGN BASIS

3.3.1. Availability requirements

The NCSS must be available to operate in the event of a Total Loss of Computerised I&C [Ref-1].

3.3.2. Performance requirements

The response times of the NCSS will be defined later, but they will not be more stringent than those for the RPR [PS] [Ref-1].

3.3.3. Environmental requirements

The environmental conditions that the NCSS must tolerate are dictated by the temperature and relative humidity of the rooms housing this equipment. The environmental characteristics are defined in Sub-chapter 9.4, for normal and extreme conditions.

3.3.4. Human-machine interface requirements

The manual functions, permissive management and information display details associated with the NCSS will be provided on the MCS [SICS] [Ref-1].

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

3.4. ARCHITECTURE

3.4.1. Structure and composition

The NCSS is fourfold redundant for automatic functions; each redundancy is allocated to a different electrical division. Each redundancy contains elements to perform automatic and manual actions.

NCSS cabinets use non-computerised components to process automatic functions. These cabinets exchange information with the 3 other divisions through decoupling devices. The exchanges between divisions are hardwired.

The NCSS receives information coming from the sensors through the Process Instrumentation Pre-processing System (PIPS) or Ex-core conditioning. The automatic actions initiated by the NCSS are Reactor Trip (acting on the Main Trip Breakers), ESFAS actuations (acting on electric switchgear), and Turbine Trip.

The NCSS outputs to the trip breakers and switchgear are designed to be energised to actuate. Internal signals between NCSS divisions and modules up to the voting logic are de-energised to actuate so that they are failsafe and are generated in duplicate logic trains to minimise the spurious actuation rate. A clock signal is used to ensure that failures can be detected in normal operation.

The NCSS provides indications to the MCR (MCP [PICS] and MCS [SICS]) and receives individual commands from MCS [SICS].

All manual commands are first routed through the MCS [SICS] Interface Cabinet which performs:

- the dispatching of MCS [SICS] manual commands to the PAS/SAS and NCSS,
- the validation of manual commands by the release button.

Some commands are used for functional processing in the NCSS cabinet (permissive validation or manual RT), whereas other commands are routed through the NCSS cabinet only to provide enough power for MCS [SICS] commands to switchgear units.

The transmission of information from the NCSS to the MCS [SICS] is hardwired and non-computerised, via the MCS [SICS] Interface Cabinet. This interface ensures that MCS [SICS] displays are driven correctly according to the Normal / NCSS selection switch and actuator check backs. The MCS [SICS] must also be enabled (see Sub-chapter 7.3 section 2.0.2).

The transmission of information from the NCSS to the MCP [PICS] for monitoring of the system during normal operation is performed via the plant bus [Ref-1].

Section 7.4.3 – Figure 1 shows the NCSS architecture principle across all four divisions.

3.4.2. Installation

The NCSS equipment is distributed within the four divisions. The equipment is installed in the safeguard buildings [Ref-1].

3.4.3. Interfaces with other I&C systems

With reference to Section 7.4.3 – Figure 1, the NCSS exchanges information with the following [Ref-1]:

PIPS - The PIPS gathers conditioning of the thermodynamic sensors for several I&C systems. It also manages the decoupling of output signals to transmit them to different safety class equipment.

The measurements provided by the sensors are acquired in the NCSS as inputs for automatic functions.

In-core/Ex-core conditioning - The NCSS acquires signals provided by the Neutron Flux Ex-core Measurement System conditioning modules.

Trip breakers - The NCSS sends an opening command to the trip breakers to perform the RT. It also receives check backs from the trip breakers for periodic tests purpose.

Switchgear - The NCSS outputs are directly connected to the switchgear units of the safety actuators.

The switchgear is in charge of the priority management of commands coming from various origins and from different safety classes for safety actuators. The NCSS sends actuation commands to switchgear for automatic and manual functions.

The NCSS could also receive the test check backs from switchgear for periodic test purposes (decision will be taken during the detailed design).

When required, the actuator check backs are acquired via the PIPS and then transferred to the NCSS and PAS/SAS in order to switch to the correct information to drive the MCS [SICS] displays.

Turbine I&C - The NCSS sends the turbine trip signal to the turbine I&C. It also receives check backs from the Turbine I&C for periodic test purposes.

SAS - The NCSS receives a life signal from SAS to display the status of the SPPA-T2000 systems on the Inter-Panel Signalisation Panel (PSIS). This status is used to allow switching of the NCSS mode.

MCP [PICS] - MCP [PICS] gathers all computerised controls and displays in the MCR. During normal operation without Total Loss of Computerised I&C, the NCSS provides MCP [PICS] with information (alarms, status, etc.) needed by the operators or for archiving via a uni-directional link to the plant bus.

MCS [SICS] - MCS [SICS] gathers all conventional controls and conventional displays located in the MCR. The NCSS provides MCS [SICS] directly with alarms and indication display. The MCS [SICS] provides the NCSS with the manual controls for the system management. All manual commands needed for the "NCSS situation" are routed through the NCSS cabinet for power interface purposes and then to the switchgear units.

PSIS - The PSIS receives the status of the SPPA-T2000 platform, elaborated in the NCSS.

3.5. OPERATING CONFIGURATIONS

The configuration of the NCSS (from hardware and functional points of view) is independent of the computerised I&C systems. The NCSS configuration only depends on the following principle: in the event of malfunction of the computerised I&C systems, the NCSS will operate to bring the plant to a non-hazardous stable state and maintain it in that state until the computerised I&C can be recovered.

3.6. TECHNOLOGY

The technology used for NCSS is a non-computerised technology; the platform is the AREVA TA UNICORN platform. The NCSS is implemented using non-computerised modules [Ref-1] [Ref-2].

3.7. POWER SUPPLY

Within each division, the I&C cabinets of the NCSS are supplied by a dual power supply, via independent AC/DC converters and DC/DC converters. One power supply is provided by a 400V AC supply and the other by a 220V DC supply with appropriate converters [Ref-1].

Within each NCSS I&C cabinet, the power supply distribution and monitoring is handled by dedicated modules. These power supply modules will use non-computerised technology and be designed by a different organisation to those that are designed for the RPR [PS] and SAS power supplies [Ref-1].

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

3.8. PROVISIONS FOR PERIODIC TESTING

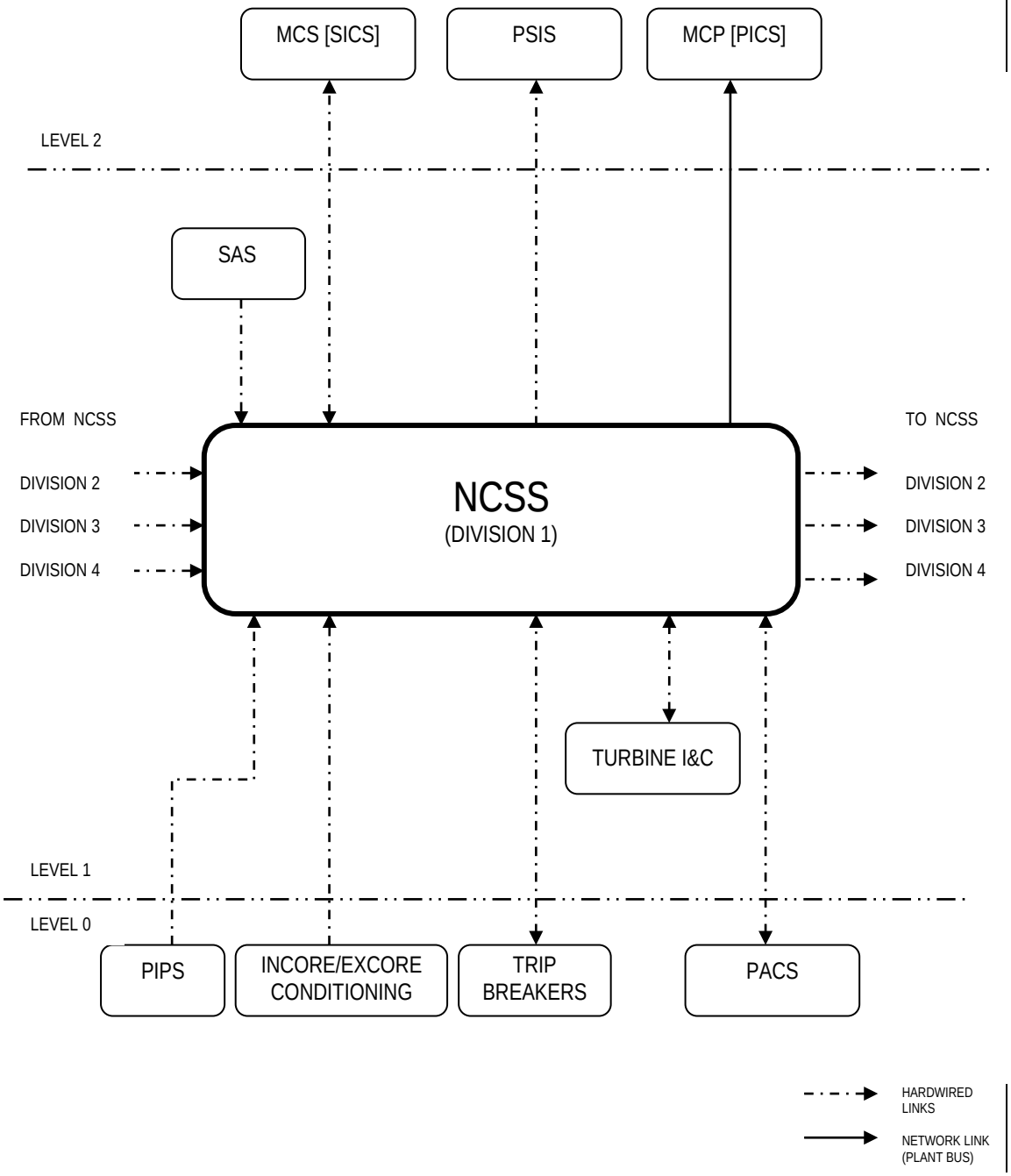
The safety function test will allow the verification of the whole control channel, from the sensor (automatic control), or from the MCS [SICS] (manual control), via NCSS, up to the change of state of the actuator.

However, if the reconfiguration of the relevant actuator cannot be carried out (for example, during the plant operation), provisions are taken for blocking the control signals during the test, so that the actuator control line can be tested without physically controlling it.

Any equipment used to test the NCSS will be at least Class 3. 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 7.4.3 - FIGURE 1

NCSS architecture across all four divisions



SUB-CHAPTER 7.4 – 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. SAFETY AUTOMATION SYSTEM (SAS)

[Ref-1] Project Development Plan relating to FA3 Standard I&C. NLF-F-DC11 Revision C. AREVA. June 2007 (E)

[Ref-2] Quality Plan for engineering of FA3 standard I&C based on SPPA-T2000. NLF-F DC 82 Revision C. AREVA. April 2008 (E)

[Ref-3] System Qualification Program. NLF-F DC 14 Revision D. AREVA. March 2009. (E)

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

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

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

[Ref-6] Application Software Test program. NLF-F-DC 89 Revision C. AREVA. December 2009. (E)

[Ref-7] Definition of the predictability model of SPPA-T2000/S7. SIE QU017 Revision 0.2. Siemens. May 2012. (E)

[Ref-8] DCE Project: Analysis of Common Cause Failures in the Instrumentation and Control System Based on the SPPA-T2000 Platform that Perform F1B (SAS) Safety Class Functions. H-P1A-2008-01857-FR Revision 3.0. EDF. August 2009. (E)

[Ref-9] KC Plant System. - Level 1 Instrumentation and Control Equipment Document P1 - DSE History. ECECC070931 Revision B1. EDF. September 2009. (E)

[Ref-10] KC System DES (Plant System File) - Part 2: KC. System operations. ECECC070539 Revision B1. EDF. September 2009. (E)

[Ref-11] KC Plant System File – Part 3: Designing KC system. ECECC070902 Revision B1. EDF. September 2009. (E)

[Ref-12] KC Plant System File – Part 4: KC system Mechanical Diagrams. ECECC070935 Revision B1. EDF. September 2009. (E)

[Ref-13] KC Plant System File - Part 5: KC System I&C. ECECC070903 Revision B1. EDF. September 2009. (E)

[Ref-14] Module dependability analysis for SPPA T2000 (S7) AS 620B / SPPA T2000 – OM components. Safety parameter determination approach. SIE QU019 Revision 0. Siemens. February 2012. (E)

1.0. SAFETY REQUIREMENTS

[Ref-1] UKEPR: SAS IEC 61513 System Requirements Specification (SRS) Equivalence. ECECC121435 Revision A. EDF. August 2012. (E)

1.1. ROLE

[Ref-1] Justification Report on the Independence of I&C Systems based on the SPPA T2000 Platform. ECECC080586 Revision B1. EDF. July 2009. (E)

ECECC080586 Revision B1 is the English translation of ECECC080586 Revision B.

1.4. ARCHITECTURE

1.4.1. Structure and composition

[Ref-1] Self Test Coverage Analysis. QU003 Revision 0.1. Siemens. February 2012. (E)

1.4.3. Interfaces with other I&C systems

[Ref-1] Self Test Coverage Analysis. QU003 Revision 0.1. Siemens. February 2012. (E)

[Ref-2] Generic Rules for the Electrical Isolation of EPR UK Instrumentation and Control Systems (Internal Connections and Interfaces). ECECC111058 Revision B. EDF. June 2012. (E)

1.6. TECHNOLOGY

[Ref-1] Basis of Safety Case of SPPA-T2000. PEL-F DC 13 Revision A. AREVA. June 2012. (E)

1.8. PROVISIONS FOR PERIODIC TESTING

[Ref-1] Self Test Coverage Analysis. QU003 Revision 0.1. Siemens. February 2012. (E)

2. REACTOR CONTROL, SURVEILLANCE AND LIMITATION SYSTEM (RCSL)

[Ref-1] TELEPERM XS – System Overview. ANP:G-49 V1.0. AREVA. 2006. (E)

[Ref-2] 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-3] TXS I&C Systems Verification and Validation Plan. PELV-F DC 28 Revision A. AREVA. June 2012. (E)

[Ref-4] I&C TXS Cabinets Qualification Program. NLZ-F DC 3 Revision C. AREVA. July 2007 (E)

[Ref-5] RCSL - Detailed Specification. NLP-G\2006\en\1007 Revision H. AREVA. June 2009. (E)

[Ref-6] RCSL – Concept for Periodic Tests. NLE-F DC 179 Revision B. AREVA. May 2009. (E)

[Ref-7] RCSL – Concept for Signal Annunciation. NLE-F DC 166 Revision B. AREVA. August 2009. (E)

[Ref-8] RCSL - Functional Diagrams. NLN-F DC 90 Revision A PREL. AREVA. December 2009. (E)

NLN-F DC 90 Revision A PREL is the English translation of NLE-F DC 167 Revision D.

[Ref-9] 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-10] TELEPERM XS Engineering Procedure - Methodology for RAMS Studies. NLE-F DM 10032 Revision A. AREVA. June 2010. (E)

2.4. ARCHITECTURE

2.4.3. 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)

3. NON-COMPUTERISED SAFETY SYSTEM (NCSS)

[Ref-1] Principles to be used for the implementation of the NCSS for Emergency Operating Procedures. ECEF100659 Revision A. EDF. March 2010. (E)

[Ref-2] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

[Ref-3] EPR UK Functional Requirements on Non-Computerised Safety I&C Functions. NEPR-F DC 551 Revision C. AREVA. July 2012. (E)

[Ref-4] Safety Requirements for Non Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

[Ref-5] Non Computerised Safety System – Diversity Criteria. PELL-F DC 11 Revision C. AREVA. August 2012. (E)

[Ref-6] NCSS System Verification and Validation Plan. TA-2065953 Revision C. AREVA. July 2012. (E)

[Ref-7] NCSS Quality Plan. TA-2061589 Revision C. AREVA. July 2012. (E)

[Ref-8] UNICORN Project - Platform Quality Plan. TA-2057230 Revision D. AREVA. June 2012. (E)

[Ref-9] UNICORN Project - Platform Qualification Plan. TA-2073805 Revision D. AREVA. July 2012. (E)

[Ref-10] UNICORN Project - Justification of Platform Reliability & Response Time on a Typical Automatic Function. TA-2082935 Revision B. AREVA. July 2012. (E)

[Ref-11] UNICORN Project - Platform Specification. TA-2060143 Revision C. AREVA. May 2012. (E)

[Ref-12] Non Computerised Safety System – Basis of Safety Case. PTL-F DC 5 Revision A. AREVA. August 2012. (E)

3.0. SAFETY REQUIREMENTS

3.0.1. Safety Functions

[Ref-1] Safety Requirements for Non Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

3.0.2. Design requirements

[Ref-1] Non Computerised Safety System – Diversity Criteria. PELL-F DC 11 Revision C. AREVA. August 2012. (E)

[Ref-2] Requirements for non-computerized I&C platform. PTI DC 2. Revision E. AREVA. April 2012. (E)

3.0.2.1. Requirements resulting from the functional classification

3.0.2.1.2. Single failure criterion

[Ref-1] Safety Requirements for Non Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

3.0.2.1.3. Emergency power supplies

[Ref-1] Safety Requirements for Non Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

[Ref-2] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

3.0.2.1.7. Periodic Testing

[Ref-1] Safety Requirements for Non Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

3.0.2.1.8. Additional Requirements

[Ref-1] Non Computerised Safety System – Diversity Criteria. PELL-F DC 11 Revision C. AREVA. August 2012. (E)

3.0.2.2. Hazards

[Ref-1] Safety Requirements for Non Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

3.1. ROLE

[Ref-1] Safety Requirements for Non Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

3.2. FUNCTIONS PERFORMED

[Ref-1] Safety Requirements for Non Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

[Ref-2] EPR UK Functional Requirements on Non-Computerised Safety I&C Functions. NEPR-F DC 551 Revision C. AREVA. July 2012. (E)

[Ref-3] EPR UK – Functional Justification of the Non Computerised Safety System Design. PEPR-F DC 105 Revision A. AREVA. July 2012. (E)

[Ref-4] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

3.3. DESIGN BASIS

3.3.1. Availability requirements

[Ref-1] Safety Requirements for Non Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

3.3.2. Performance requirements

[Ref-1] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

3.3.4. Human-machine interface requirements

[Ref-1] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

3.4. ARCHITECTURE

3.4.1. Structure and composition

[Ref-1] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

3.4.2. Installation

[Ref-1] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

3.4.3. Interfaces with other I&C systems

[Ref-1] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

3.6. TECHNOLOGY

[Ref-1] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

[Ref-2] UNICORN Project - Platform Specification. TA-2060143 Revision C. AREVA. May 2012. (E)

3.7. POWER SUPPLY

[Ref-1] Non Computerised Safety System - Diversity Criteria. PELL-F DC 11 Revision C. AREVA. August 2012. (E)