UK EPR	Title: PCSR – Sub-Chapter 7.2 – General architecture of the Instrumentation and Control systems
	UKEPR-0002-072 Issue 04

Total number of pages: 76	Page No.: I / IV
Chapter Pilot: B. WORINGER *Name/Initials* B. Woringer *Date* *05-11-2012*	
Approved for EDF by: A. MARECHAL *Name/Initials* A.J.C. Marechal *Date* *05-11-2012*	Approved for AREVA by: G. CRAIG *Name/Initials* G Craig *Date* *05-11-2012*

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA review	14-04-08
01	Integration of technical, co-applicant and INSA review comments	27-04-08
02	PCSR June 2009 update: - Clarification of text - Introductory paragraphs covering RRC-B SAS, SAS BUS, SA C&I (section 1.3) - References added	26-06-09
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 - Architecture: Class 1 manual control and indication systems in the MCR and RSS - NCSS added - Text updated to address diversity between lines of defence in depth	27.03.11
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	05.11.2012

Continued on next page

REVISION HISTORY (Cont'd)

Issue	Description	Date
04 cont'd	Consolidated PCSR update: - Clarification of text (§1.2.1, §1.3.1, §1.3.2, §1.3.3, §1.3.3.1, §1.3.3.2, §1.3.3.3, §1.3.4, §1.3.5, §1.5, §1.5.1, §1.5.2, §1.5.3, §1.5.5, §1.5.6, §2.3, §3.1, §3.4.1, §3.6.1, Table 1, Figures 1 to 8) - Addition of RodPilot® (§1.1, §1.3.1) - Integration of the PSOT as a specific HMI for the PS, based on the QDS platform (§1.1, §1.3, §1.5, Table 1) - Addition of classification requirements for periodic test and maintenance equipment (§1.2.1) - Addition of justification of SAS and NCSS classification (§1.3.1) - Addition of justification of SAS / PICS independence (§1.3.3.1) - Addition of justification of Plant Bus and Terminal Bus response times (§1.3.4) - Section discussing diversity and independence rewritten (§1.3.6) - New section on reliability added (§1.3.7) - PACS section updated to current status (§1.4) - Table added showing classification and reliability of each system (Table 2)	

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 7.2 - GENERAL ARCHITECTURE OF THE INSTRUMENTATION AND CONTROL SYSTEMS

1. OVERALL INSTRUMENTATION AND CONTROL ARCHITECTURE

1.1. OVERVIEW

The overall architecture of the Instrumentation and Control (I&C) system is given in Sub-chapter 7.2 - Figure 1. The functional architecture is structured in different levels:

Level 0: Process interfaces

Consisting of:

- Instrumentation including the sensors and transducers up to the automation system, and any components needed for pre-processing the signal before the automation system, including the Process Instrumentation Pre-Processing System (PIPS).
- Switchgear units and actuators including RodPilot® and Management of Priority and Actuation Control (PACS).

Level 1: Automation systems

Including:

- Class 1 protection systems (Reactor Protection System (RPR [PS])).
- Class 2 systems (Safety Automation System (SAS), Reactor Control, Surveillance and Limitation System (RCSL) and Non-Computerised Safety System (NCSS)).
- Class 3 systems (Process Automation System (PAS), RRC-B Safety Automation System (RRC-B SAS) and Severe Accident I&C system (SA I&C).
- Data acquisition, automation processes, monitoring and control implemented in specific Class 3 or NC I&C systems (turbine, alternator, etc.). These systems are outside the scope of Chapter 7.

Level 2: Monitoring and control of the unit

Including: data processing relating to the Human-Machine Interface (HMI) for the monitoring and control of processes implemented in:

- Process Information and Control System (MCP [PICS]) (Class 3).
- Safety Information and Control System (MCS [SICS]) (Class 1).

There are also the following additional interfaces:

- The Inter WorkStation Console (PIPO) (Class 1).
- The Protection System Operator Terminal (PSOT) (Class 1) which is the HMI unit of the RPR [PS].
- The Inter-Panel Signalisation Panel (PSIS) (Class 2).
- The Severe Accident (SA) Panel (Class 3) which is a dedicated area within the MCS [SICS] panel.

Further details of the interfaces and the above systems are given in section 1.3.3 of this sub-chapter.

Level 3: Non real-time applications

Level 3 applications are non real-time applications, for example the Data Acquisition System. These are outside the scope of Chapter 7.

1.2. DESIGN BASIS

1.2.1. Safety requirements

The I&C classification principles are given in Sub-chapter 3.2.

The classification of process instrumentation depends on the specific functions to be carried out.

Safety functions are allocated to systems and the systems are classified based on the category of the allocated functions. Sub-chapter 7.2 - Table 1 gives an overview of the allocation of the different types of I&C Functions to these I&C systems. A more detailed allocation is given in [Ref-1].

The I&C functional criteria are defined in Sub-chapter 7.1.

The safety requirements related to I&C systems are given in Sub-chapters 7.3, 7.4 and 7.5.

To reduce the risk of common cause failure, there is required to be:

- diversity and independence between the RPR [PS] and the SAS and the NCSS;
- independence and diversity between the MCP [PICS] / PSOT and the MCS [SICS].

Sub-chapter 7.2 - Table 2 gives a classification and a reliability claim for each I&C system.

Periodic test and maintenance functions on I&C systems shall be categorised one category below the function impacted by the maintenance or the periodic test. 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.

1.2.2. Availability requirements

The availability targets for typical I&C functions are defined in Sub-chapter 15.1 (I&C failure model).

Availability requirements affect I&C systems rather than the I&C architecture. The availability requirements are specified in Sub-chapters 7.3, 7.4 and 7.5.

1.2.3. Performance requirements

The global response time targets for I&C in a stable situation are:

- Any process data should be displayed on the operator interface in less than 1.5 seconds.
- Manual commands should be transmitted to the actuator in less than 1.5 seconds.

The response time targets for automatic actions are given by system in Sub-chapters 7.3, 7.4 and 7.5.

1.3. DESCRIPTION OF INSTRUMENTATION AND CONTROL SYSTEM ARCHITECTURE

1.3.1. Level 0

Sensors (analogue and digital), transducers and data acquisition devices

The sensors (analogue and digital), transducers and data acquisition devices are components of the following instrumentation:

- Conventional process instrumentation (see section 1 of Sub-chapter 7.6).
- Accident and severe accident instrumentation (see section 2 of Sub-chapter 7.6).
- Process Instrumentation Pre-processing System (PIPS) (see section 3 of Sub-chapter 7.6)
- In-core instrumentation (see section 4 of Sub-chapter 7.6).
- Ex-core instrumentation (see section 5 of Sub-chapter 7.6).
- Rod position instrumentation (see section 6 of Sub-chapter 7.6).
- Reactor pressure vessel level instrumentation (see section 7 of Sub-chapter 7.6).
- Loose parts monitoring and vibration monitoring (see section 8 of Sub-chapter 7.6).
- Radiation monitoring (see section 9 of Sub-chapter 7.6).
- Boron concentration instrumentation (see section 10 of Sub-chapter 7.6).

The instrumentation includes measurement channels of various classes / levels of safety importance; the classification of a particular measurement channel depends on the highest level of classification of the I&C Function for which the measurement is used.

If a given measurement signal is processed in different level 1 systems, acquisition of the measurement occurs in the highest class system. The signal is then generally transferred to other systems via the plant network.

Exceptions exist for measurement signals which:

- relate to high-performance I&C functions for which delay due to serial transmission is not acceptable: these signals are therefore hardwired; or
- are required in the RPR [PS] and other automation systems (PAS, SAS, NCSS, etc.).

The measurement signals are then distributed hardwired to the other systems, using isolating modules if necessary. These isolating modules are mounted within the instrumentation system signal conditioning of the system that has the highest classification.

The redundant sensors and transducers used for a Category A or B I&C Function and their cabling are physically separated and allocated to different divisions.

Electrical switchgear

The electrical switchgear design requirements are defined on the basis of the principles provided in Sub-chapter 3.2.

The redundant actuators and electrical switchgear used for a Category A and B I&C Function are arranged in separate divisions.

Priority and Actuation Control (PACS)

The PACS is provided to manage the control of actuators that are subject to commands from multiple sources and to facilitate the monitoring of the actuators under all plant operating conditions.

In terms of safety, the PACS must support the automation functions associated with the control and monitoring of the actuator to ensure operation of the I&C Function with the highest priority. The PACS functionality is implemented in either the PAS or SAS automation systems and in the actuator switchgear.

The PACS functions are as follows:

- Management of control priority, which includes two sub-functions: one prioritises multiple commands received or generated by the PAS or SAS, and the other prioritises the commands received from different I&C systems by the electrical switchgear unit powering the actuator.
- Control of the switching device.
- Monitoring of the actuator.
- Essential protection of the components.

Refer to section 1.4 of this sub-chapter for more detailed information on PACS.

Process Instrumentation Pre-Processing System (PIPS)

The function of the PIPS is to provide signal processing (signal conditioning and/or signal multiplication) as required for the analogue and binary signals delivered by sensors. It provides isolation between the downstream systems for sensors shared by more than one such system. The input signals processed by PIPS consist of all sensors that do not require specialised conditioning and are used by the following I&C systems:

- RPR [PS].
- RCSL.
- SA I&C.
- PAS (only sensors shared with the TELEPERM XS systems).
- SAS (only sensors shared with the TELEPERM XS systems).
- NCSS (only sensors shared with the TELEPERM XS systems).
- RRC-B SAS (only sensors shared with the TELEPERM XS systems).
- Diesel I&C (only sensors shared with the TELEPERM XS systems).

The PIPS does not provide signal conditioning and/or signal multiplication and distribution for sensors that use specialised measurement and conditioning equipment. Such specialised equipment is used for the following systems:

- In-core instrumentation.
- Ex-core instrumentation.
- Rod position measurement.
- Boron concentration measurement.
- Inductive position sensors (only signal multiplication and distribution provided).

Refer to section 3 of Sub-chapter 7.6 for more detailed information on PIPS.

RodPilot®

RodPilot® is the digital control rod drive system which actuates the control rods. The RCSL sends a 4 bit coded hardwired signal to RodPilot® for the actuation of one rod.

Each RodPilot® cabinet manages four rods, except the cabinet managing the central control rod, which only handles this rod. The RodPilot® modules manage the currents in the rod coils, contain the switchgear for the high voltage supply to the rods and perform monitoring tasks.

RodPilot® also acquires reactor trip demands from the four divisions of the RPR [PS] via hardwired connections, the trip is performed on 2 out of 4 voting.

RodPilot® is Class 2.

1.3.2. Level 1

Overview

The automation functions are implemented in the following level 1 systems:

- PAS.
- RCSL.
- RPR [PS].
- SAS.
- NCSS.
- RRC-B SAS.
- SA I&C.

Sub-chapter 7.2 - Table 1 gives an overview of the allocation of the different types of I&C Functions to these I&C systems.

Process Automation System (PAS)

The main role of the PAS is the monitoring and control of the plant in all normal operating conditions. In addition, the PAS performs sufficient monitoring and control of sub-functions related to risk reduction.

The PAS performs the Category C non-seismically qualified and non-categorised I&C Functions of the nuclear island and of the conventional island (except for non-categorised I&C Functions assigned to other specific systems outside the scope of Chapter 7, such as the turbine/alternator I&C).

PAS functions are monitored by the operators through the MCP [PICS]. If the MCP [PICS] becomes unavailable in PCC-1 conditions (normal operation), some PAS functions required to maintain the plant in stable operating conditions can be monitored via the MCS [SICS] (see sections 1.3.3 and 1.5 of this sub-chapter).

The PAS is a Class 3 digital system.

Reactor Control, Surveillance and Limitation System (RCSL)

The RCSL processes Category B, Category C and non-categorised I&C Functions related to core control and monitoring.

These include:

- the core control functions; and

- the automatic Limiting Conditions of Operation (LCO) functions and limitation functions for core parameters and for the reactor coolant circuit requiring control rod actuation (some of these functions may be implemented in the PAS if this is more suitable).

The actuator control functions for the control rods are implemented in the RCSL; the control functions for the other actuators controlled by RCSL are implemented in other level 1 systems, and the RCSL communicates with them via the plant network.

The RCSL is a Class 2 digital system.

Reactor Protection System (RPR [PS])

The RPR [PS] monitors the safety parameters in all Plant Condition Categories (PCC), and for all initiating events, enables:

- the automatic Category A protection and safety I&C Functions;
- the automatic Category A control I&C Functions of the safety support systems; and
- the manual Category A I&C Functions.

The RPR [PS] also provides information on safety parameters for the MCS [SICS] (Class 1), the MCP [PICS] (Class 3) and the PSOT (Class 1) HMI unit of the RPR [PS]. Refer to Sub-chapter 7.3 for details of the PSOT.

The parameters, the initiating signals and the RPR [PS] commands are displayed to the operator by the MCP [PICS], MCS [SICS] and by the PSOT. Safety Interlocks are implemented in the RPR [PS] to prevent manual actions including reset of automatic functions from the MCS [SICS] and PSOT if the process conditions do not permit it.

The RPR [PS] is a Class 1 digital system.

Safety Automation System (SAS)

The main functions performed by the SAS are:

- post-accident management I&C Functions (manual and automatic) necessary to bring the plant from the controlled state to the safe shutdown state after an initiating event (Category B);
- I&C Functions related to Class 2 support systems which do not change their status during an event (autonomous safety support systems such as ventilation);
- Category A & B I&C Functions preventing significant radioactive release including those that are the diverse line of protection in the main line of defence;
- Category B I&C Functions with an SC1 seismic requirement; and
- Category C I&C Functions with an SC1 seismic requirement.

Further details dealing with allocation of RRC-A I&C functions are also provided in section 1.5.5 of this sub-chapter.

The elements of the SAS performing the I&C Functions related to the autonomous support systems are organised in autonomous sub-systems incorporating the necessary protection against external effects (for example, functional isolation, local controls, etc.).

When a category A function is performed by two or more independent systems, the systems should be Class 1 systems. If it is desired to use systems of a lower class, at least one of the systems shall meet the requirements of a Class 1 system and a safety justification shall be provided for systems not meeting Class 1 system requirements to enable the acceptability of this to be assessed (IEC 61226:2009 Clause 7.3.2.1).

Safety Class 2 is justified for the SAS as the functions implemented by SAS:

- make a significant contribution to fulfilling a Category A safety function, or
- form a diverse line of protection for fulfilling a safety function when at least one other safety Class 1 system also fulfils the function or
- form a principal means of ensuring a Category B safety function.

The RPR [PS] is the Class 1 system that is the principal means of fulfilling Category A safety functions. The SAS is a Class 2 system that makes significant contributions to fulfilling Category A safety functions. A Class 2 system can contribute to a Category A function provided that the system fulfils the safety function in combination with at least one diverse Class 1 system [Ref-1] [Ref-2].

The status and operating parameters (initiation and actuation signals, feedback signals) of the SAS are displayed to the operator by the MCP [PICS] and MCS [SICS]. Category B Safety Interlocks are implemented in the SAS to prevent manual actions and the resetting of functions from the MCP [PICS] if the process conditions do not permit it.

The SAS is a Class 2 digital system.

Non-Computerised Safety System (NCSS)

The NCSS provides protection and control in case of total loss of computerised I&C functions (i.e. those performed by systems based on the SPPA-T2000 and TXS platforms).

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 systems reliabilities are such that the design complies with Targets 8 and 9 of the HSE SAPs [Ref-3].

The NCSS processes Category A, Category B and Category C functions required to reach and maintain a non-hazardous stable state.

Safety Class 2 is justified for the NCSS as the functions implemented by the NCSS:

- make a significant contribution to fulfilling a Category A safety function;
- form a back-up line of protection for fulfilling a safety function when at least one other safety Class 1 system also fulfils the function.

The NCSS is a Class 2 system.

RRC-B Safety Automation System (RRC-B SAS)

The RRC-B SAS is dedicated to severe accident Risk Reduction Category B (RRC-B) functions (with the exception of the Loss of Off-site Power (LOOP) severe accident scenario, which is managed by the Severe Accident I&C system (SA I&C), see below) and performs the Category C seismically qualified I&C Functions that contribute to the following safety functions:

- Primary circuit depressurisation;
- Hydrogen control (mitigation);
- Containment depressurisation and heat removal; and
- Radiological source term monitoring.

The RRC-B SAS is a Class 3 digital system.

Severe Accident I&C system (SA I&C)

SA I&C provides the necessary commands and information in the event of a severe accident coupled with, or due to, a Loss of Off-site Power (LOOP), loss of Emergency Diesel Generators (EDG) and Ultimate Diesel Generators (UDG).

The SA I&C performs three main I&C Functions:

- Acquires and processes signals;
- Displays data (on the SA Panel on MCS [SICS]); and
- Acquires manual commands from the SA Panel on MCS [SICS].

The SA I&C will have a 12 hour battery back-up.

The sensors used for SA I&C Functions are routed through different PIPS cubicles from those only used in other systems. They must meet some additional specific qualification requirements over and above the general safety requirements linked to classification. Refer to section 2 of Sub-chapter 7.6. PIPS cubicles used to support SA I&C will have a 12 hour battery back-up.

The SA I&C is a Class 3 digital system.

1.3.3. Level 2

The I&C level 2 systems are principally located in the Main Control Room (MCR) and Remote Shutdown Station (RSS). These systems can be broken down into two distinct groupings; computerised and conventional systems.

There are two level 2 computerised systems; the MCP [PICS] and the PSOT (the HMI unit of the RPR [PS]) and one level 2 conventional system: the MCS [SICS]. There are also conventional HMI of the SA Panel, the PIPO and the PSIS.

Data processing at level 2 is mainly used to support the HMI for unit monitoring and control.

Plant operations generally take place on MCP [PICS], direct control of RPR [PS] takes place on PSOT and a diverse and non-computerised MCS [SICS] is used when MCP [PICS] or PSOT is unavailable.

Sub-chapter 7.2 - Table 1 provides an overview of the allocation of types of process I&C Functions to I&C systems.

Sub-chapter 7.2 - Figure 2 provides an overview of the structure of the level 2 systems, the communication network and interfaces.

1.3.3.1. Computerised systems

Process Information and Control System (MCP [PICS])

MCP [PICS] is used by the operators to monitor and control the plant in all plant conditions (PCC and RRC).

The MCP [PICS] has access to information from all level 1 systems and presents this information to the operating personnel on the following HMI equipment:

- monitoring and control workstations (in operating mode) in the MCR used to operate and monitor the plant;
- supervisory workstations (display only) in the MCR;
- Plant Overview Panel (POP) (display only) permitting a shared overview in the MCR of the state of the plant and its parameters;
- workstations for monitoring and control in the RSS;
- display only workstations in the Technical Support Centre (TSC); and
- printers.

The MCP [PICS] generates alarms in the event of process or system anomalies and provides the operators with guidance for implementing appropriate measures.

Most of the plant actuators can be controlled by MCP [PICS] via level 1 systems.

Commands are executed by the operators from the screens and transmitted to the level 1 systems, which act both on safety and non safety actuators.

The MCP [PICS] does not send any operator commands to the RPR [PS]. These are implemented by means of the PSOT, the HMI unit of the RPR [PS].

Should an initiating event occur, the operators monitor the automatically initiated protection or risk reduction functions on the MCP [PICS] screens, and if needed initiate the following from the MCP [PICS] screens:

- reset of automatically initiated Category B I&C Functions in the SAS;
- I&C Functions for post accident management in level 1 systems;

- risk reducing I&C Functions for RRC-A conditions and diverse line of protection in the SAS;
- risk reducing I&C Functions for RRC-A conditions in the PAS; and
- I&C Functions implemented by the RRC-B SAS for RRC-B conditions.

The MCP [PICS] supports Category A, Category B and C I&C Functions. The Class 3 PICS provides commands to the SAS. The Class 2 SAS can operate independently of the PICS and the Plant Bus via two redundant and independent “SAS bus” network links that are used for the transmission of signals up to Class 2, between SAS equipment. The redundant SAS bus is both physically separate and architecturally diverse from the Plant Bus. The SAS protects itself from erroneous data and commands from Class 3 systems in the following ways:

- The functional specifications together with the priorities of commands within the standard diagrams managing the actuators ensure that Category A and B functions are treated as priority over lower classified functions;
- The SPPA-T2000 is a proven Digital Control System without any spurious command reported to Siemens;
- The SAS automatically performs regular and extensive ‘life-sign’ checks of the main MCP [PICS] hardware and software components required for the monitoring of alarms and status, and for the generation of commands, i.e. the Plant Bus, Processing Units, Terminal Bus, Operating Terminals and Thin Client graphics drivers (this life-sign indication is displayed on the PSIS);
- The overall I&C architecture and ongoing safety studies based particularly on the functional redundancies of the Category A and B functions guarantee the successful management of the worst case scenario of plausible, erroneous commands sent by the MCP [PICS] affecting a maximum of one division [Ref-1].

If a fault is detected, the operator will have the option to switch control of the plant to MCS [SICS]. Refer to section 1.5.1 of this sub-chapter.

If the MCP [PICS] does fail, then the MCS [SICS] is used as the back-up operating system for all plant conditions. MCS [SICS] is a Class 1 system. The MCS [SICS] displays are permanently in operation and provide an independent and complementary back-up line to the operating team and for the Safety Engineer’s (or equivalent role) surveillance. The MCS [SICS] is diverse from the MCP [PICS]. It is capable of a safe, but more limited, set of normal operating and accident condition controls [Ref-2] and [Ref-3].

Although MCP [PICS] is a Class 3 system, the equipment and architecture of the computerised HMI workstations in the MCR and the RSS meet the requirements for Class 2 systems; the workstations for control and monitoring functions in the MCR and the RSS have to meet the single failure criterion and have SC1 seismic requirements. Other functions such as printing, archiving, etc. are implemented in SC2 equipment (to ensure that no hazard is presented to SC1 equipment).

The MCP [PICS] is functionally independent of the MCS [SICS] [Ref-4].

Protection System Operator Terminal (PSOT)

The PSOT is the HMI unit of the RPR [PS] and provides a dedicated Class 1 interface, used to display data from and send commands to the RPR [PS] whilst the plant is being operated from MCP [PICS]. The commands available via the PSOT are also available via the conventional controls of MCS [SICS] when operating from that location.

The PSOT is located at the operator's normal workplace adjacent to the MCP [PICS] workstations within the MCR and the RSS [Ref-3].

1.3.3.2. Conventional systems

There is one level 2 system (MCS [SICS]) which uses conventional technology. In addition, there are a number of level 2 interfaces which are not part of the MCS [SICS] but use similar conventional technology:

- The SA Panel which provides the monitoring and control interface to the SA I&C.
- PIPO which provides hardwired controls including reactor and turbine trip.
- PSIS which provides status indications for the I&C systems including MCP [PICS], SAS/PAS and RPR [PS].

The MCS [SICS] and these interfaces are described below.

Safety Information and Control System (MCS [SICS])

The MCS [SICS] provides the HMI facilities for the safety demonstration for all categories of control and monitoring I&C Functions needed to bring the plant to a safe shutdown state in the event of unavailability of the MCP [PICS] or the PSOT.

The MCS [SICS] enables:

- the plant to be monitored and controlled for a limited time of up to 8 hours in steady state power operation in PCC-1 or to be brought to and maintained in the shutdown state; and
- in the event of PCC-2 (design basis transient) to PCC-4 (design basis accident) events coincident with unavailability of the MCP [PICS]:
  - the safety functions of the plant to be monitored, especially the Category A automatic protection and post accident I&C Functions;
  - the manual functions necessary to bring the plant from the controlled to the safe shutdown state to be initiated;
  - the support systems of the safety systems needed for post accident control to be monitored and controlled; and
  - fire fighting control functions on the nuclear island to be initiated.

The MCS [SICS] is not normally used by the operators when the MCP [PICS] and PSOT are available. The exceptions to this are:

- during some periodic tests; and
- for additional monitoring of the main safety process parameters and the status of the safety systems in incident or accident conditions.

While operating from the MCP [PICS], alarms are indicated on both the MCP [PICS] and MCS [SICS], but the MCS [SICS] alarms are auto-acknowledged [Ref-1].

While operating from the MCP [PICS], the MCS [SICS] controls are not active. This reduces the risk of spurious actuation as a result of an internal hazard or internal faults within the MCS [SICS].

The MCS [SICS] controls are enabled when required by changeover controls on the MCS [SICS] panel. The enabling of the MCR MCS [SICS] controls is managed by three two-position (MCP [PICS] / MCS [SICS]) switches, each of which includes independent contacts for each of the four divisions [Ref-2] [Ref-3].

When operating from MCS [SICS]:

- manual commands are sent from the MCS [SICS] to the level 1 systems which block all commands coming from the MCP [PICS] and PSOT, this being to prevent a spurious actuation being generated by MCP [PICS] or PSOT malfunction or during maintenance activity on the MCP [PICS] or PSOT; and
- the alarm functions on the MCS [SICS] (acoustic alarms, acknowledge and reset) that were not active whilst the MCP [PICS] and PSOT were operational are activated.

The manual functions and information display associated with the NCSS will be provided on the MCS [SICS] when the MCS [SICS] is enabled and the Normal / NCSS selector switch is set to NCSS [Ref-4]. There is one Normal / NCSS selector switch for each of the four divisions.

However the NCSS controls for permissive validation and the status of the NCSS automatic functions are always active whatever the operating mode of the MCS[SICS].

The MCS [SICS] is functionally independent of the MCP [PICS] and PSOT, and is located in the MCR.

Severe accident panel

The SA Panel is the HMI associated with the SA I&C located in a dedicated area of the MCS [SICS] panel. The controls of the SA Panel are not normally active but are enabled by the operator when required using dedicated switches situated on the panel. The MCS [SICS] is not required to be enabled for the SA Panel to be enabled. The SA Panel has SC1 seismic requirements as it is located on the MCS [SICS] panel.

The Inter Workstation Console (PIPO)

PIPO is a conventional manual control interface which is located on the Inter Workstation Console. PIPO provides a small number of manual commands including reactor and turbine trip. These manual commands are used during the evacuation of the MCR to the RSS. The console has SC1 seismic requirements. PIPO is a Class 1 interface.

Inter-Panel Signalisation Panel (PSIS)

The PSIS is a conventional display located between the four POP screens and provides binary indications for Category B functions such as the MCP [PICS] life-sign, SAS/PAS status and RPR [PS] status. The equipment has SC1 seismic requirements.

1.3.3.3. Locations

The main level 2 HMIs are located in the locations indicated below. However, I&C safety systems are not available to facility operators at locations other than the MCR and RSS.

Main Control Room (MCR)

The operating and safety functions of the plant are initiated and/or monitored from the MCR in all operating conditions unless the MCR is rendered unavailable by an internal hazard. Refer to section 1.5.3 of this sub-chapter for details of the MCR evacuation procedure.

The MCR is equipped with:

- MCP [PICS] workstations.
- MCP [PICS] plant overview panel.
- PSOT Protection System HMI.
- PIPO.
- PSIS.
- MCS [SICS].
- SA Panel.

Remote Shutdown Station (RSS)

If the MCR is unavailable, the operators monitor and control the plant from the RSS. The reactor is tripped from the MCR prior to evacuation.

The RSS is equipped with:

- MCP [PICS] workstations.
- PSOT Protection System HMI.
- control facilities to block commands from both the computerised and conventional HMI equipment in the MCR; technical and administrative measures prevent spurious or unauthorised activation of these functions. The RSS control facilities are connected to conventional logic panels that are in separate fire zones to the MCR and RSS. These panels disable MCS [SICS] inputs by removing the power supply to the changeover controls and provide an input to the RPR [PS] to disable the PSOT workstations in the MCR. MCP [PICS] workstations are disabled by cutting the power supply to the MCR network switches from the computer room, which is in a different fire zone to the MCR and RSS [Ref-1] [Ref-2] [Ref-3].

All I&C equipment and support systems needed for operation from the RSS are separated from the MCR area and are located in different fire sectors.

Technical Support Centre (TSC)

The TSC is a room used by the emergency support team in the event of an accident. These additional staff analyse the condition of the plant and support post-accident management.

The TSC is equipped with MCP [PICS] workstations with access to all the information but without the control functions.

Decentralised HMIs

Some limited monitoring and control facilities are installed locally, near to the equipment monitored and/or controlled (e.g. effluent treatment building and nuclear auxiliary building). The decentralised HMI uses MCP [PICS] technology.

1.3.4. Communication between the instrumentation and control systems

Interfaces between I&C systems and their support systems shall be designed such that interface failure will not endanger the systems own or any other system's safety function.

Communication between levels 1 and 2

The data exchanges between the level 1 I&C systems and the MCP [PICS] take place over the plant network.

It should be noted that the NCSS sends signals to the MCP [PICS] via a link to the Plant Bus.

To the extent possible, the internal exchanges within a system (including data exchange between divisions) are performed by the system itself without calling up external resources.

The plant network crosses the divisions and extends through:

- the nuclear island safeguard and electrical buildings;
- the effluent treatment building;
- the diesel buildings; and
- the electrical building on the conventional island.

The plant network is Class 3 with a SC1 seismic requirement and, for availability reasons, is designed to withstand a single failure as well as internal hazards within a division [Ref-1] (see also section 2 of Sub-chapter 7.5).

Independently from the plant network, two redundant and independent "SAS bus" network links are used for the transmission of signals up to Class 2, between SAS equipment. These network links form the SAS bus network that is Class 2 and is designed to withstand a single failure as well as internal hazards within a division.

Data exchange between the MCS [SICS] and the RPR [PS], SAS, RRC-B SAS, NCSS and PAS is via hardwired links.

An analysis of the FA3 studies and tests for the Plant Bus and Terminal Bus shows that the design derived time responses are considerably more pessimistic than those determined by the testing performed. It presents arguments for the acceptability of the results that have been obtained and argues that the equipment to be used for the UK EPR can be expected to produce more acceptable results. It is noted that the numerical criteria for the time responses are not safety related limits, but are average response time targets [Ref-2].

Communication between levels 0 and 1

For Category A and B I&C Functions, the data exchanges between level 0 equipment and level 1 equipment are always performed by hardwired connections.

For Category C and non-categorised I&C Functions, the data exchanges between level 0 equipment and level 1 equipment are performed either via network or hardwired connections.

1.3.5. Technology

The platform used to implement the RPR [PS], RCSL and SA I&C is the I&C digital system TELEPERM XS (TXS) [Ref-1] [Ref-2] [Ref-3].

The platform used to implement the PAS, SAS, RRC-B SAS and MCP [PICS] is the I&C digital system SPPA-T2000 [Ref-4].

The platform used to implement the Non-Computerised Safety System (NCSS) is UNICORN [Ref-5].

Refer to Sub-chapter 7.7 for details on production excellence and independent confidence building activities used to support the selection and substantiation of the system platforms.

The MCS [SICS] and NCSS are both based on conventional technology. However, the use of digital equipment within these systems is not precluded (recorders for example).

The three platforms mentioned above (TELEPERM XS, SPPA-T2000 and UNICORN) must be diverse from each other. This is detailed in section 1.3.6 of this sub-chapter.

The Human Machine Interfaces MCS [SICS], MCP [PICS] and PSOT, the HMI unit of the RPR [PS], must be independent from each other. This is detailed in section 1.3.6 of this sub-chapter.

1.3.6. Independence and Diversity

To meet the high reliability claims made on I&C functions, and to reduce the possibility of a Common Cause Failure (CCF) of redundant equipment, the use of independent and diverse systems and components in the I&C architecture is necessary.

1.3.6.1. Independence and diversity in level 0

As part of the overall requirements for the provision of reliable redundant safety functions, independence and diversity is considered for level 0 equipment. Appropriate diversity and independence of sensors, related signal conditioning equipment and of Priority and Actuation Control (PACS) modules is required to ensure that the full benefit of the diversity and independence arrangements at level 1 can be credited. Independence and diversity for level 0 equipment is primarily assessed on a Postulated Initiating Event basis.

Sensors and conditioning modules

Diversity criteria have been developed and documented to inform the processes of selection and/or development of diverse sensors and conditioning modules where deemed necessary [Ref-1]. The level of diversity required is dependent upon the reliability claim made upon the sensor and/or conditioning module. An assessment against the criteria will be carried out for the selected components.

For frequent faults where both the RPR [PS] and SAS (and sometimes the NCSS) provide a line of protection, the approach is for the RPR [PS] to have a dedicated group of sensors and the SAS and NCSS to share a second group. The diversity between these two groups of sensors will be assured for each Postulated Initiating Event (PIE) [Ref-2] [Ref-3], and suitably substantiated [Ref-4].

Priority and Actuation Control (PACS)

Diversity requirements have been defined to support the specification or selection of two types of PACS modules, designated PACS A and PACS B, such that overall reliability claims can be justified when these diverse modules are appropriately allocated [Ref-5].

The level of diversity required is dependent upon the reliability claim made upon the PACS module [Ref-6]. Because the PACS modules are implemented using simple conventional components whose failure modes are well understood, just two cases are defined with a boundary between the two cases at the CCF claim limit for such simple devices:

- Case 1: common reliability bounded by: pfd > 10^{-5}
- Case 2: common reliability bounded by: 10^{-5} > pfd > 10^{-9}

Hence for Case 1, there are minimal requirements for diversity between PACS modules claimed in combination, consisting of the normal good practice of peer review of specification documents and appropriate separation between redundant PACS modules.

For Case 2, where the reliability claim is 10^{-5} > pfd > 10^{-9}, more stringent diversity criteria will be applied related to design, equipment and human diversity considerations as well as appropriate separation.

Diversity between PACS modules is to be provided within the first line of protection with the application of a generic rule that PACS A modules are to be utilised in divisions 1 and 2 and PACS B modules are to be utilised in divisions 3 and 4. This generic rule is adequate in the vast majority of cases with only a small number of exceptions requiring a modified allocation rule to provide the required level of diversity [Ref-7].

1.3.6.2. Independence and diversity in level 1

Defence in Depth

One of the fundamental safety principles used for UK EPR is the concept of Defence in Depth (DiD) as introduced in Sub-chapter 3.1. The I&C architecture provides prevention and protection to support the first four DiD levels by the provision of a preventive I&C line of defence, a main I&C line of defence and a risk reduction I&C line of defence. The following systems provide protection at each of the DiD levels [Ref-1]:

- DiD Levels 1 and 2: Prevention and control of abnormal operation. These DiD levels are supported by the preventive I&C line of defence which is made up of the PAS and RCSL.

- DiD Level 3: Control of faults within the design basis. This DiD level is supported by the main I&C line of defence, which is made up of a first I&C line of protection and a diverse I&C line of protection. The RPR [PS] and SAS are assigned to the main I&C line of defence.

- DiD Level 4: Control of severe plant conditions in which the design basis may be exceeded. This DiD level is supported by the risk reduction I&C line of defence, which is made up of a back-up I&C line of protection and a severe accident I&C line of protection. The NCSS provides the back-up I&C line of protection, and the RRC-B SAS and SA I&C the severe accident I&C line of protection.

- DiD Level 5: Mitigation of radiological consequences of radioactive release: No plant I&C systems support this level.

There are no specific requirements for independence and diversity of systems within the preventive I&C line of defence or within the severe accident I&C line of defence.

There is a requirement for independence and diversity between the two systems which make up the main I&C line of defence, and between the systems in the main I&C line of defence and the backup I&C line of protection [Ref-2].

Independence

The main protection systems are the RPR [PS] and SAS of the main I&C line of defence, and the NCSS of the backup I&C line of protection. Independence is provided between these systems, and between redundant equipment in each system to exclude the possibility of a common cause failure. This independence has been assessed as adequate for the following factors [Ref-3]:

- Diversity

- Physical separation

- Power supply equipment

- Electrical isolation between systems

- Communication links between systems

- HVAC system

- EMI/RFI considerations

- Hazard protection

- Maintenance and repair arrangements

A set of diversity criteria have been derived providing requirements for diversity between the RPR [PS], SAS and NCSS at a system level, as well as between the TELEPERM XS, SPPA-T2000 and UNICORN platforms which these systems are based upon [Ref-4] [Ref-5]. This includes requirements for hardware diversity, I&C system design diversity and I&C platform design diversity (including tool set diversity).

Diversity between RPR [PS], SAS and NCSS

The diversity between the RPR [PS], SAS and NCSS systems has been assessed using an approach based upon IEC 61513, IEC 62340 and NUREG 6303. The I&C system designs have been assessed against a set of derived diversity criteria in terms of:

- Design diversity
- Functional diversity
- Human diversity
- Software diversity
- Separation criteria

The provisions for I&C system designs are considered appropriate in terms of meeting the diversity criteria [Ref-6].

Diversity between TELEPERM XS, SPPA-T2000 and UNICORN

Certain diversity requirements are considered to apply at the level of the technological platform rather than the implemented system. The three platforms have differing architectures with the TELEPERM XS and SPPA-T2000 platforms, which are computerised, and the UNICORN platform, which uses non-computerised technology.

The key differences between the TELEPERM XS and SPPA-T2000 platforms are listed below:

- Product responsibility (Siemens PG L for SPPA-T2000 and AREVA NP Gmbh RS/PTL-G – ex. Siemens PG N for TXS).
- Engineering tools (TEC4 Function, OM Editor etc. for SPPA-T2000 and SPACE for TXS).
- Database system for engineering tools (Ingres for SPPA-T2000 and Oracle for TXS)
- Operating System (S7-OS, AP-SSW for SPPA-T2000 and MICROS real time operating system for TXS).
- Communication between automation processors (SIMATIC NET for SPPA-T2000 and TXS-Profibus for TXS).
- Central Processing Unit (Simatic S7 CPU 400H, based on ASIC implementation for SPPA-T2000 and SVE2: AMD K6-2E for TXS).

- Centralised I/O (FUM Modules developed by Siemens IA&DT in Fűrth for SPPA T2000 and Specific TXS Modules developed by Siemens EDM in Erlangen for TXS).

The UNICORN platform is based upon non-computerised technology. The safety functions are implemented on modules based on Magnetic Dynamic Logic (MDL) technology with simple components such as discrete elements (transistors, transformers...), TTL logic gates or operational amplifiers, which are inherently diverse from the two software based systems [Ref-7].

The three platforms will be assessed against the diversity criteria to demonstrate that they are suitably diverse.

1.3.6.3. Independence and diversity in level 2

The only diversity required for level 2 systems is between the main operational HMI system and the safety HMI system to ensure that a CCF cannot lead to total loss of all operator display and control facilities [Ref-1].

The main operational HMI consists of the MCP [PICS] and the PSOT, both of which are computer based display and control terminals relying on data networks to send and receive information.

- The MCP [PICS] is based upon the SPPA-T2000 Operating and Monitoring System, OM690, which is the screen-based graphical user interface of the SPPA-T2000 platform. It provides the plant operator with user-friendly and ergonomic information displays and manual control facilities. OM690 is based on redundant workstations running UNIX. The main components of the OM690 system architecture are the Processing Unit, Server Unit and Operator Terminals. These components are based on SUN workstations running the T2000 application software.

- The PSOT is based on the Qualified Display System (QDS) platform, part of the TXS platform, which is a computer-based system with a graphical user interface to display information and provide manual control facilities associated with the RPR [PS]. The QDS platform uses PC/AT hardware architecture with system software. Each PSOT connects directly to a RPR [PS] Data Interface via a point-to-point digital data link.

The safety HMI is the MCS [SICS], which consists of discrete indicators and switches mounted in a mosaic panel. These devices are mostly conventional switches, LEDs and galvanometer indicators (exceptions being the digital chart recorders and 7-segment displays which are complex or SMART devices). The discrete devices connect directly to the level 1 automation systems via conventional hardwired analogue and binary links.

Hence in terms of technology, architecture and signal transmission the main operational HMI system and the safety HMI system are suitably diverse [Ref-2].

1.3.6.4. Functional diversity

The fault schedule in Sub-chapter 14.7 and functional diversity analyses of Sub-chapter 16.5 illustrate that the I&C Function that contributes to each Category A safety function is performed by the RPR [PS] and by the SAS, where required as a diverse line to the main line of protection. The NCSS also contributes to Category A safety functions in the event of total loss of computerised systems.

The RCSL and RPR [PS] are both implemented on the TXS platform, and both systems act upon the control rods. The RCSL acts upon the control rods in normal operation and is designed to support the limitation functions in order to avoid demands for protection action. The RPR [PS] trips the reactor if protection limits are reached. If a common cause failure of the RCSL and RPR [PS] were to occur, it could lead to an Anticipated Transient Without Scram (ATWS), as both systems could fail to send the signal to insert control rods when necessary. In this case, the SAS, which is implemented on the SPPA-T2000 platform, would recover the situation and enable the controlled state to be reached.

The reactor trip equipment and the boration systems (the Safety Injection System (RIS [SIS]) and the Extra Boration System (RBS [EBS])) are initiated by multiple I&C signals. The implementation of these I&C functions and signals in the I&C systems depends on which line of defence the function and signal belong to. The reactor trip equipment and the boration systems are both actuated by the same I&C system (RPR [PS] / TXS platform) as they belong to the main line of defence. However, because the reactor trip, RIS [SIS] initiation and RBS [EBS] initiation are also required in the diverse line of protection within the main line of defence, which protects against RRC-A multiple failure events, they can also be actuated by the diverse SAS (SPPA-T2000). Therefore, in the event of unavailability of the RPR [PS], the Reactor Trip, RIS [SIS] and RBS [EBS] functions would still be available.

The main NCSS automatic functions are reactor and turbine trip, main feedwater isolation and Emergency Feed Water System (ASG [EFWS]) actuation. These actions leave the plant in a stable steady-state condition. Other automatic functions such as reactor cooling pump trip, Component Cooling Water System (RRI [CCWS]) isolation, or chemical and volume control system (CVCS) isolation take care of specific dominant events and sequences [Ref-1].

1.3.6.5. Lifetime management of independence and diversity

Methodologies, procedures and organisations will be put in place to manage the diversity between the TELEPERM XS, SPPA-T2000 and UNICORN I&C platforms and to ensure that it is maintained in the long term [Ref-1].

Supplier lifetime diversity management

The long term policy for management of diversity between the TELEPERM XS and the UNICORN platforms is to control the development of, and modifications to, these platforms to ensure that evolutions do not jeopardise their mutual diversity position. The processes for ensuring diversity of the platforms are event driven when a modification to either platform is proposed:

- Before performing a modification to either the TELEPERM XS or UNICORN platform, a diversity analysis is performed to ensure that the proposed modification will not pose a threat to the diversity position between the three platforms;
- No modification can be launched on either of these platforms if it weakens the diversity position;
- The documentation for justification of diversity between I&C platforms is updated when the modification is performed.

For the SPPA-T2000 platform, the long term diversity management policy is based on monitoring and analysing modifications proposed or made to the SPPA-T2000 platform and reacting to maintain the overall diversity position between the three platforms. Similarly following any modifications to the SPPA-T2000 platform the documentation for justification of diversity between I&C platforms is updated.

Operator lifetime diversity management

Licence conditions will ensure that modifications to the design of plant during or after construction are appropriately controlled, these will include consideration of the I&C architecture diversity requirements.

The engineering organisation will maintain regular dialogue with suppliers on future obsolescence threats and possible management strategies to ensure that all potential changes to approved versions of equipment and possible threats to the diversity position are advised and understood well in advance.

1.3.7. Reliability

The reliability claims made upon the three main protection systems, RPR [PS], SAS and NCSS, are presented in Sub-chapter 7.2 - Table 2. Justification of these reliability claims is undertaken by consideration of systematic and hardware failures and compliance with appropriate guidance and standards.

1.3.7.1. RPR [PS] reliability

The RPR [PS] reliability claim is supported by:

- assessment against IEC standards appropriate to a class 1 system. These standards are outlined in Sub-chapter 7.7, section 4.1.1;
- undertaking a programme of Independent Confidence Building Measures (ICBMs) appropriate to the reliability claim. The ICBMs to be undertaken for the RPR [PS] are outlined in Sub-chapter 7.7, section 4.1.2;
- undertaking a reliability analysis consisting of FMEA of TELEPERM XS modules, FMEA of the RPR [PS], and a reliability and availability study [Ref-1].

The justification of the reliability is based first on a calculation of the reliability of the RPR [PS] architecture to perform I&C functions based on FMEA and fault tree methods. The consequences of potential failures of the TELEPERM XS modules on the processing of the RPR [PS] I&C functions are analysed. The failure rate of individual failures and of common failure in redundant parts are then combined, in order to calculate the reliability of the RPR [PS] to perform its I&C functions.

The confidence that the risk of systematic failure in the software part is sufficiently low with regards to the reliability target is provided by the application of production excellence and ICBMs as outlined in Sub-chapter 7.7, section 4.1.

1.3.7.2. SAS reliability

The SAS reliability claim is supported by:

- assessment against IEC standards appropriate to a class 2 system. These standards are outlined in Sub-chapter 7.7, section 4.2.1;
- undertaking a programme of ICBMs appropriate to the reliability claim. The ICBMs to be undertaken for SAS are outlined in Sub-chapter 7.7, section 4.2.2;

- undertaking a reliability analysis [Ref-1].

The reliability analysis is performed on the SPPA-T2000 platform and includes derivation of the mean time between failure, probability failure on demand average, probability failure per hour and spurious trip rate.

1.3.7.3. NCSS reliability

The reliability claim for the NCSS is supported by compliance with IEC standards, and undertaking a reliability study.

The development of the NCSS, along with the UNICORN platform, will be compliant with IEC standards applicable to a class 2 system with a reliability claim of 10^{-3} fpd/fpa [Ref-1].

The reliability study calculates a theoretical maximum probability of failure on demand, which is compared to the system reliability claim. The methodology for the reliability study is as follows [Ref-2]:

- identification of reliability requirements;
- definition of the undesirable events and their criteria;
- preliminary safety and availability analysis;
- modules reliability analysis;
- final safety reliability analysis.

This approach uses FMEA analysis and accounts for common cause failure for identical modules.

1.4. PRIORITY AND ACTUATION CONTROL (PACS)

The PACS functionality is provided to manage the control of actuators that are subject to commands from multiple sources and to facilitate the monitoring of the actuators under all plant operating conditions.

In terms of safety, the PACS must support the automation functions associated with the control and monitoring of the actuator to ensure operation of the safety function with highest priority. The PACS functionality is implemented in the PAS/SAS automation systems and in the actuator switchgear.

The PACS must support the classification and other requirements of the controlled actuators. Each PACS actuator must also be independent of the other PACS actuators; there is no exchange between them.

Links between the RPR [PS], PAS, SAS, NCSS and electrical switchgear units are hardwired.

Detailed information for the UK EPR will be provided in the system specification reports and overall architecture drawings, which will be based upon Flamanville 3 documentation [Ref-1] and [Ref-2].

1.4.1. Role

The role of the PACS is to manage control of the actuator, monitor its movement, and provide essential protection of the electrical components. It is responsible for the following:

- In terms of actuator control:
  - Selection of the highest priority command (in the case of simultaneous commands) from all the commands to which the actuator is subject.
  - Control of the switching device.
- In terms of actuator monitoring: Monitoring of the actuator position and any movement failures (excessive manoeuvre time or inconsistency between the expected and actual position of the actuator). Information for actuator surveillance is monitored via the PAS/SAS, presented to the operators through the computerised HMI. No equivalent additional actuator surveillance is carried out by the RPR [PS]
- In terms of essential protection of the components: Detection of malfunction that could damage the electrical components of the actuator or its electrical power supply and tripping of contactors as appropriate.

1.4.2. Functions performed

Sub-chapter 7.2 - Figure 8 shows an overview of the allocation of the PACS functions within the various I&C systems.

In keeping with the functions defined in section 1.3.1 of this sub-chapter, the PACS provides the following four functions:

- *Management of control priority:* Prioritisation of all commands (automatic and manual) governing the actuator, whatever their origin or function, and selection (in the case of simultaneous commands) of the command having the highest priority. The command selected is sent to the PACS function “control of switching device” (see below).

  The priority of commands is as follows (highest to lowest priority):
  - “Essential protection of components” command (protection against damage to the electrical components of the actuator or to its electrical connection).
  - Disconnection command (load shedding following a loss of electrical power).
  - Reactor protection command (Class 1).
  - Manual command via local HMI (i.e. portable HMI that can be plugged in to the electrical switchgear unit permitting a direct command to the switchgear, independent of the automation systems).
  - NCSS automatic commands
  - SAS/PAS component protection automatic commands (derived from process conditions: e.g. very high temperature of a heating coil).

- SAS/PAS operating command (coming from the process: e.g. start-up of a filling pump on low level from the SAS/PAS, with the SAS having priority over the PAS).
- SAS/PAS manual command derived from the MCS [SICS] or MCP [PICS].
- NCSS manual commands
  Note: These commands are only enabled if NCSS operation is selected from the MCS [SICS] and in this case, the SAS/PAS commands are disabled.

- *Control of the switching device:* Control of the device which activates movement of the actuator. This command is the output from the function "Management of control priority".
- *Monitoring of the actuator:* Monitoring of the position of the actuator, and of its movement failures. The latter function detects a movement malfunction in the actuator, e.g. an abnormally long movement time, or an inconsistency between the expected and actual position of the actuator.
- *Essential protection of the components:* Generation of a command resulting from malfunction of the moving part of the actuator (short-circuit or surge, isolation fault, etc.) in order to prevent risk of damage to the actuator or to its electrical power supply. This control is applicable to the PACS function "management of control priorities", where it is assigned the highest priority level.

The processing of the PACS functions is organised in the following way:

- The PAS/SAS generates Class 2, 3 or NC automatic commands and acquires the manual commands issued from the centralised HMI (MCP [PICS] or RSS and MCS [SICS]). In the event of simultaneous commands, it selects the highest priority command according to the hierarchy defined above (“management of control priority” function). The selected command is sent to the electrical switchgear unit. In addition, PAS/SAS provides monitoring of the actuator position and generation of movement fault signal ("actuator monitoring" function).
- The RPR [PS] generates Class 1 commands (safeguard actions and safeguard support) which are sent to the electrical switchgear unit.
- The NCSS generates Class 2 commands (safeguard actions and safeguard support) which are sent to the electrical switchgear unit.
- The electrical switchgear unit implements the essential protection of the components (“Essential protection of components” function), and receives command(s) issued from the RPR [PS], commands issued from the NCSS, commands selected by the PAS/SAS and commands issued from the local HMI. In the event of simultaneous commands, the highest priority command (according to the hierarchy defined above) is selected ("management of control priority" function) and sent to the switching device ("control of switching device" function).

N.B.: The “management of control priority” function is implemented partly by the PAS/SAS and partly by the electrical switchgear unit.

1.4.3. Design basis

1.4.3.1. Diversity Requirements

Analysis has been performed to identify the claims on components that may be used by more than one line of protection, taking account of the potential for common cause failure. A requirement for the provision of diverse PACS modules (the items contained within the actuator switchgear) has been identified and a specification of the diversity criteria for these modules has been developed [Ref-1].

A functional analysis has enabled the development of a plan for the implementation of PACS module diversity to ensure the reliability of safety functions claimed in the Main Line in the fault schedule [Ref-2].

1.4.3.2. Availability requirements

The main availability requirements for PACS are linked to the reliability and the maintainability of the equipment performing the functions, i.e.

- Limiting the loss of the PACS due to failure of one of its components
- Facilitating the maintenance and repair of the PACS to minimise downtime.

1.4.3.3. Performance requirements

The response time of the PACS following a command (including acquisition, processing and execution of the command) coming from the level 1 systems (RPR [PS], SAS, PAS and NCSS) must not exceed 100 ms.

1.4.3.4. Environmental requirements

The environmental conditions of the equipment managing the PACS functions depend on their location:

I&C cabinet rooms (PACS functions managed by PAS/SAS):

- The temperature and relative humidity characteristics of the air surrounding the PAS/SAS equipment (installed in the I&C cabinet rooms) are specified in section 1 of Sub-chapter 9.4, for both normal and extreme conditions.

Electrical switch rooms (PACS functions managed by the electrical switchgear unit):

- The temperature and relative humidity characteristics of the air surrounding the electrical switchgear units (installed in the electrical switch rooms) are specified in section 1 of Sub-chapter 9.4, for both normal and extreme conditions.

1.4.4. Allocation of PACS functions

1.4.4.1. Structure and composition

The four PACS functions are processed partly by PAS automation (or the SAS, according to the required function), and partly by the electrical switchgear unit, (see section 1.4.2 of this sub-chapter).

The implementation of the PACS is decentralised. Each actuator has its own dedicated switchgear incorporating priority management functionality as required on a case-by-case basis. Relay based technology is used in the switchgear. No digital technology is used.

The command signals from the SPPA-T2000 systems (SAS, PAS, etc.) are hardwired to dedicated interposing relays in the actuator switchgear, as are the command signals from the RPR [PS] and the NCSS. The interposing relays ensure that the I&C systems outputs remain isolated from each other.

Where NCSS manual commands are implemented for an actuator, these commands are normally disabled. In the event that the operator selects NCSS mode at the MCS [SICS] panel (following detection of computerised I&C system failure), a selection relay within the PACS module enables the NCSS manual commands and disables commands from the SAS/PAS.

Information for actuator surveillance is presented to the operators, via a set of volt free relay contacts, through the computerised HMI. This information for all actuators is only collected by the SPPA-T2000 systems and transmitted to the HMI. These relay contacts, used for actuator surveillance, are isolated from any contacts used to implement the PACS priority and command circuits.

The structure and composition of the functions processed by the PAS are defined in section 3 of Sub-chapter 7.5.

The structure and composition of the functions processed by SAS are defined in section 1 of Sub-chapter 7.4.

1.4.4.2. Installation

The equipment processing the PACS functions will be installed:

- For PAS and SAS automation: in the I&C cabinet rooms of the division or sector containing the controlled actuator.
- For the electrical switchgear unit: in the electrical switch rooms of the electrical division or sector containing the controlled actuator.

1.4.4.3. Interfaces with I&C systems

The PACS functions are implemented within the PAS/SAS and within the electrical switchgear unit, which exchange information as follows:

PAS/SAS PACS functions communicate with:

- the centralised HMIs (MCP [PICS] in both the MCR and RSS, MCS [SICS]);

- the PAS or SAS functions including generation of automatic operating commands, and generation of fault information.
- the PACS modules in the electrical switchgear.

The electrical switchgear unit communicates with:

- the local HMI (HMI which can be connected to the electrical switchgear unit);
- the NCSS;
- the RPR [PS] (for the management of safety commands);
- the switching devices(s) (managing the actuator electrical power supply);
- the process sensors.

Electrical switchgear units are used for driving the actuators (low and high voltage): these switchgear units are managed by conventional I&C technology (with digital electrical protection for the high-voltage actuator switchgear units).

1.4.5. Power supply

The power supplies for the different equipment that implements the PACS processing functions are as follows:

- PAS automation (or SAS, according to the functional requirements): Supplied via a duplicated diesel-backed power supply (see section 3.7 of Sub-chapter 7.5 for details of the PAS power supplies and section 1.7 of Sub-chapter 7.4 for details of the SAS power supplies). The PAS (or SAS) automation implementing the management of the PACS functions of a given actuator is supplied by the same division or section as that of the actuator.
- Electrical switchgear units are supplied with:
    - Power voltage, by a supply, which, depending on the functional requirements, is diesel-backed or not.
    - Control voltage, which supplies the internal instrumentation and control of the switchgear unit, by a supply derived from two redundant 230V AC sources. The nature and level of the control voltage of the switchboard will be part of the detailed design.

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

To allow full interchange ability of switchgear, all medium voltage and low voltage switchgear will be qualified to the same standards [Ref-1]. Note: during any interchange, the PACS diversity requirements will be respected.

1.4.6. Provisions for periodic testing

PACS (as an element of the actuator control channel) is subject to periodic testing to verify the integrity of the control channel.

This test applies to the overall function, and includes:

- the test initiator (HMI manual command or local mechanical action on a sensor, as appropriate);
- the PACS, comprising the automation (PAS or SAS, depending on the functions required) and the electrical switchgear unit including the switching device(s); and
- the actuator, whose movement is verified in the test.

N.B.: If a particular actuator cannot be activated (for example while the unit is operating), provisions must be made to ensure the test does not entail an actual actuator movement.

The basic principles for periodic testing are described below:

- To the maximum extent possible, periodic testing must be performed from the MCR if the tests involve an action on the process, or if the tests concern the HMI itself, without necessitating local intervention.
- When a safety system actuator receives commands from several systems (e.g. the RPR [PS] and SAS or PAS), the testing of this actuator must be performed as far as possible from only one of these systems. The testing of commands from other systems must be performed without actual movement of an actuator.
- Tests which involve actuator movement, and require the use of an HMI to send the commands and to verify the information received, require the participation of personnel. These tests should remain manual (no automatic activation, prior to the mechanical system tests).

1.5. OPERATING MODES

1.5.1. Normal operation

Sub-chapter 7.2 - Figure 3 provides an overview of the I&C systems used for the monitoring and control of the plant in normal operation.

The PAS and RCSL carry out all the automated functions in normal operation; the actuator commands go directly from the PAS to the switchgear and from the RCSL to the control rod drive mechanisms. The MCP [PICS] with its HMI equipment allows the operators to monitor and control the state of the plant and the I&C functions necessary during normal operation.

For monitoring the state of the RPR [PS], SAS, RRC-B SAS and SA I&C in normal operation, the MCP [PICS] receives information from these systems over the plant network.

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].

Unavailability of Computerised Interface

If the computerised interface is unavailable due to an internal fault, the operating team decides, based on the messages and alarms generated by the MCP [PICS] and PSOT self-surveillance functions and the Class 2 life-sign of the MCP [PICS] processing units (the information is displayed on the PSIS Category B monitoring I&C Function) [Ref-2] to [Ref-6], whether to transfer operation of the unit from the MCP [PICS] (i.e. the main operating area) to the MCS [SICS] (i.e. the back-up operating area) (Sub-chapter 7.2 – Figure 4). The MCS [SICS] is put into operation by implementing the functions described in section 1.3.3 of this sub-chapter.

It is intended that operation and monitoring of the plant in steady state power operation will be carried out via the MCS [SICS] for only a limited period. If the computerised interface is not made available within 8 hours, the operators bring the plant to a safe shutdown state and maintain it there using the MCS [SICS], RPR [PS], SAS and PAS.

1.5.2. Reference operating conditions

In accident conditions (PCC-2 to PCC-4) there are two distinct operating modes:

- operation with all I&C systems available; and
- operation with only Class 1 and 2 I&C systems available.

Accident mitigation with all I&C systems available

Sub-chapter 7.2 - Figure 5 gives an overview of the I&C systems which are used to monitor and control the plant, when all I&C systems are available.

The initiating events are detected by the RPR [PS]. The I&C protection functions necessary in the first 30 minutes are initiated automatically and implemented by the RPR [PS].

If manual actions are necessary to reach a controlled state or safe shutdown state, the operators are alerted by alarms generated by the RPR [PS] or SAS and displayed by the MCP [PICS].

With the help of operating displays and operating procedures, and based on the information delivered by all level 1 systems, the I&C functions in PAS, SAS and RPR [PS] are monitored and controlled on the MCP [PICS] screens and the PSOT to manage the post accident situation.

Operation with only Class 1 and 2 I&C systems available

The initiating events are detected by the RPR [PS]. The I&C protection functions necessary in the first 30 minutes are initiated automatically and implemented by the RPR [PS] (Sub-chapter 7.2 - Figure 4).

If manual actions are necessary to reach a controlled state or safe shutdown state, the operators are alerted by alarms generated by the RPR [PS] or SAS and displayed by the MCS [SICS].

The manual post-accident functions are initiated through the MCS [SICS]: the corresponding actions are performed by the RPR [PS] or SAS.

1.5.3. Internal hazards

Unavailability of the Main Control Room (MCR)

In the event of an internal hazard in the MCR, the plant remains in a PCC-1 condition. The operators will trip the reactor (using PIPO), inhibit all MCP [PICS] operations and within 30 minutes will have evacuated to the RSS. From there, the operators will block all commands coming from the MCR MCS [SICS] (Sub-chapter 7.2 – Figure 6).

On evacuating the MCR, the MCP [PICS] workstations in the MCR are disabled by preventing all communication between the clients (located in the MCR) that manage the operator HMI and the Operator Terminal (OT) servers (located in the computer rooms). This is achieved by de-powering the network switches that provide the connections between the clients and the OT servers. The circuit breakers for the network switch power supplies are located in the computer rooms. Appropriate measures will also be taken to disable the MCR PSOT equipment, precise details being determined during the PSOT detailed design process.

To transfer control to the RSS, after tripping the reactor at the MCR PIPO, the operators must turn the six rotary switches from MCR to RSS positions. These six switches are located in the RSS and implement the following functions [Ref-1]:

MCS [SICS] inhibition (3 switches): the disabling of the MCR MCS [SICS] controls is managed by three two-position (MCR / RSS) switches located in the RSS, each of which includes independent contacts for each of divisions 1, 2, 3 and 4. When transferring control to the RSS, the operators must turn these three rotary switches from MCR to RSS positions. Using a 2oo3 logic by division, the KSC system forces the disabling of MCS [SICS] controls by depolarising the validation push buttons to avoid the possibility of spurious commands being sent from the MCR. (The KSC design ensures that the validation command and the three rotary switches in the MCR cannot be powered via a spurious command and that commands from the RSS MCP [PICS] are enabled).

Severe Accident Panel inhibition (3 switches): the disabling of the MCR Severe Accident Panel (SAP) controls is managed separately from the above logic by two-position (MCR / RSS) switches located in the RSS, each of which includes independent contacts for each of divisions 1 and 4. When transferring control to the RSS, the operators must turn these three rotary switches from MCR SAP to RSS positions. Using a 2oo3 logic by division, the KSC system forces the disabling of the SAP controls if at least two switches are selected to RSS.

In the event that the MCP [PICS] is unavailable, then remote MCP [PICS] workstations are also unavailable; however, local portable HMI for the PACS will be available (see section 1.4.2).

In normal operation, the RSS MCP [PICS] workstations and the RSS PSOT are in standby mode so they can be rapidly brought into operation. The operators monitor and control the transition of the unit to a safe shutdown state using these workstations. The operating mode of the level 1 systems is similar to normal operation (see section 1.5.1 in this sub-chapter).

It must be possible for the operators to resume operation from the MCR when it is safe to return.

Internal hazards in level 2 systems

The redundancy and separation provided ensure that, even with a single failure, at least one division of the MCP [PICS] / PSOT or MCS [SICS] remains available.

The operating mode which ensues is similar to that described in section 1.5.2 of this sub-chapter.

Internal hazards in level 1 systems

The worst internal hazard impacting the level 1 systems in coincidence with a postulated single failure impacting the support systems results in the loss of two complete I&C divisions together with a PCC-2 due to malfunctions of I&C equipment. Depending on the failure combination, a complete loss of either MCP [PICS] or MCS [SICS] must be taken into account.

This situation can be managed with either the MCP [PICS] or the MCS [SICS] and the remaining Class 1 and 2 I&C equipment in two divisions of the level 1 systems. Consequently a safe shutdown state can be reached.

1.5.4. External hazards

The maximum impact of external hazards on I&C equipment is the loss of all equipment which is not seismically qualified: i.e. the loss of the PAS and part of the MCP [PICS].

This situation is the same as the loss of all operational I&C systems in accident conditions. The operating mode is as described in section 1.5.2 of this sub-chapter.

1.5.5. Risk reduction RRC-A conditions

The RRC-A functions are introduced to complement the deterministic design basis analysis (PCC) categories by considering a set of Design Extension Conditions (DECs) due to multiple failure events. The multiple failure sequence could result from the loss of a Category A safety function (either from the failure of an I&C system or from the failure of the plant system actuated) or from a combination of independent events affecting the core in the reactor building or the fuel elements in the fuel building. These functions are described in Sub-chapter 16.1.

Depending on the kind of failures which have led to RRC-A functions being initiated, the functional allocation rules for the I&C systems are as follows:

- If a RRC-A function addresses a fault sequence that results from a mechanical failure of the rods, this function is implemented in the RPR [PS];
- If a RRC-A function is credited as a diverse line of protection (i.e. failure of the RPR [PS]), or has a seismic qualification requirement, and addresses a fault sequence that is not initiated by the SPPA-T2000, this function is implemented in the SAS;
- If a RRC-A function that is not credited as a diverse line of protection and has no seismic qualification requirement and addresses a fault sequence that is not initiated by an SPPA-T2000 fault; this function may be allocated to the PAS;
- If a RRC-A function addresses a fault sequence that can be initiated by an SPPA-T2000 fault, this function would be allocated to the RCSL (or to the RPR [PS]).

The need for risk reduction measures and the tripping of automatic RRC-A or diverse functions is signalled to the operators by the MCP [PICS].

Station Black-Out (SBO)

The I&C operation mode considered below is the most stringent scenario consisting of a station black out (SBO) with one ultimate diesel generator lost.

LOOP is detected by the RPR [PS], which trips the reactor and sends a signal to start the emergency diesel generators (EDG).

If all emergency diesel generators fail to start, the power supply to I&C systems and components in all divisions is guaranteed by the batteries for 2 hours. In this phase, there is no ventilation in any division nor in the MCR and only a few actuators are supplied (those backed-up by batteries).

The start of one ultimate diesel generator (in division 1 or 4) is carried out manually from the MCP [PICS] via RRC I&C functions processed by the SAS. The design of the I&C systems prevents control signals with a higher priority (e.g. the RPR [PS] load shedding signal of the emergency diesel generator) from blocking the actuators needed in this situation.

As soon as the power supply to the batteries, lighting and ventilation in the MCR and I&C cabinet rooms in one division (1 or 4) is provided by the ultimate diesel generator, the power supply to all I&C equipment located in the non-ventilated divisions is shut off by local intervention before overheating, to prevent spurious actuations or erroneous signals that could block necessary RRC I&C functions.

The operators monitor and control the plant from the MCR via the supplied MCP [PICS] division, by using the information provided by the instrumentation in the remaining division processed in the remaining parts of RPR [PS], SAS or PAS. Actuators can be operated via the PAS as long as they are supplied with power.

1.5.6. Severe accidents (RRC-B)

In addition to the use of passive severe accident functions and local manual actions, the management of severe accidents is performed as described below.

RRC-B “LOOP” scenario

The RRC-B “LOOP” scenario is managed by dedicated SA I&C control cabinets in divisions 1 and 4. The following features apply to this equipment:

- all plant data necessary for the mitigation of the severe accident scenario (RRC-B “LOOP” sequence) – acquired by independent instrumentation;
- information display facilities necessary for the mitigation of the RRC-B sequence - provided by a dedicated severe accident panel; and
- means of controlling the various systems necessary in the “OSSA (Operating Strategies for Severe Accidents) mitigation path” for the scenario, including control of the 900t/h discharge valves - provided by the dedicated severe accident panel.

Sub-chapter 7.2 - Figure 7 gives the principles of the I&C architecture for severe accident management.

The power for I&C equipment necessary for the management of the RRC-B “LOOP” scenario is guaranteed by batteries for 12 hours.

RRC-B other scenarios

RRC-B other (i.e. non-LOOP) scenarios are managed by dedicated RRC-B SAS equipment in divisions 1 and 4. The following features apply to this equipment:

- all plant data necessary for the mitigation of the severe accident scenarios (RRC-B other sequences) – acquired by independent instrumentation;
- information display facilities necessary for the mitigation of the RRC-B sequences - available on the MCP [PICS]; and
- means of controlling the various systems necessary in the "OSSA (Operating Strategies for Severe Accidents) mitigation path" for the various RRC-B scenarios, including control of the 900t/h discharge valves and the severe accident EVU [CHRS] commands – provided from the MCP [PICS].

Sub-chapter 7.2 - Figure 7 gives the principles of the I&C architecture for severe accident management.

The I&C equipment necessary for the management of the RRC-B other scenarios is backed-up by the UDG.

1.5.7. Total loss of computerised I&C

A total loss of computerised I&C during normal operation and shutdown states could cause plant parameters to deviate in an inappropriate manner due to unavailability of controls. Moreover, a total loss of computerised I&C following an initiating event would be characterised by the unavailability of the protection system and of the commands and information needed for triggering manual actions.

The NCSS is designed to perform the necessary automatic Reactor Trip, some ESFAS initiations and also provide manual commands enabling the operators to stabilise the plant until computerised I&C can be recovered. Refer to section 3 of Sub-chapter 7.4 for more details.

2. EQUIPMENT ARRANGEMENT

2.1. ENVIRONMENTAL CONDITIONS

The I&C equipment is installed in different rooms (I&C equipment rooms in the electrical building, conventional island non-classified electrical building, effluent treatment building, I&C cabinet rooms, MCR, RSS, TSC, etc.).

The environmental conditions (temperature, humidity) in these rooms are defined in section 1 of Sub-chapter 9.4.

The main and emergency lighting as well as the lighting of evacuation routes is described in Sub-chapter 9.5.

The design principles ensuring effective protection of these rooms against electromagnetic interference EMI [Ref-1] and lightning are defined in section 2 of Sub-chapter 8.4.

The HMI rooms are provided with several lighting areas which can be manually controlled to provide sufficient light for the operators to perform their assigned tasks (Sub-chapter 18.1).

2.2. INSTRUMENTATION AND CONTROL SYSTEM POWER SUPPLY

The onsite emergency power supply, including the uninterruptible DC and AC power supply for I&C equipment, is described in Sub-chapter 8.3.

I&C cabinets' power supply

I&C cabinets are double fed by uninterruptible 220V DC and 400V AC power supplies provided by means of DC/DC and AC/DC converters respectively, which are fed from four battery-backed 400V AC busbars and by the 220V DC busbars directly connected to the batteries. They are installed in I&C cabinet rooms (divisions 1 to 4) and in the I&C rooms of the diesel buildings (divisions 1 to 4).

Generally a group of I&C cabinets will be supplied from one AC/DC and one DC/DC converter, supplied from redundant busbars. During maintenance of the division power supply, one of these converters can be supplied from either the same division or the neighbouring division (i.e. 1+2 and 3+4). Either of the two converters is able to power all the I&C cabinets. They are located in separate power supply cabinets each of which contains several converters. These cabinets are located close to the I&C cabinets they supply.

The secondary voltage used to supply input/output signals is 24 or 48V DC.

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

HMI power supply

The uninterrupted AC power supply for HMI is powered from the four 400V AC busbars. These busbars are supplied from the four battery-backed 400V AC busbars and, in the event of failure of the DC/AC converters, via electronic switch-over to the four 400V regulated voltage busbars.

The AC power supply is provided from all 4 divisions for HMI equipment located in the MCR (operator workstations and wall-mounted large screens), divisions 1, 3 and 4 for workstations located in the RSS, and Divisions 1 and 4 for the MCP [PICS] processing units located in I&C cabinet rooms.

2.3. EQUIPMENT ARRANGEMENT AND LAYOUT

Allocation of I&C systems to buildings

The I&C systems of the nuclear island are located mainly in the safeguard and electrical buildings (because these buildings have controlled environmental conditions), within four rooms situated in separate divisions and in rooms at the level of the MCR. Part of the I&C system, e.g. the I&C instrumentation for fuel handling gear, is installed in the reactor building, the fuel building, the nuclear auxiliary building and the effluent treatment building. The I&C equipment is designed to remain operational even after an aircraft crash. Thus, 2 out of the 4 divisions of the I&C systems that are Class 1 and 2 (including the MCR) are located in buildings protected by the aircraft shell.

Inside the buildings, the main hazards that could significantly damage one of the I&C divisions are fire, extreme temperatures or flooding. The combination of an internal hazard and a single failure, must not lead to the loss of Category A and B I&C Functions in more than 2 divisions (in particular for the HMI of the MCS [SICS]). This is achieved either by physical segregation of equipment into separate divisions, or by measures designed to prevent the propagation of hazards.

Thus, segregation into 4 divisions is required for the 4 redundant elements of the RPR [PS], whereas for the SAS this separation depends on the mechanical systems it controls which are allocated to the 4 divisions. The MCS [SICS] supply boards are installed in the MCR. The MCP [PICS] supplies all the operating facilities necessary for operation of the unit from the MCR and, if the MCR is unavailable, from the RSS. In order to ensure sufficient independence from the MCR, the MCP [PICS] processing units are located in the I&C equipment rooms of divisions 1 and 4 only. In the I&C equipment rooms, the I&C cabinets for the Class 1 and 2 I&C systems are grouped separately from the Class 3 I&C cabinets. All the systems for automatic control and for the HMI (levels 0, 1 and 2) of the nuclear island that are controlled from the MCR via the MCP [PICS] and MCS [SICS] are located in the I&C equipment rooms of divisions 1 to 4.

The PAS is located within the I&C equipment rooms of divisions 1 to 4.

The RCSL is located within the I&C equipment rooms of divisions 1 to 4.

The RPR [PS] is located within the I&C equipment rooms of divisions 1 to 4.

The SAS is located within the I&C equipment rooms of divisions 1 to 4

The NCSS is located within the I&C equipment rooms of divisions 1 to 4.

The RRC-B SAS equipment is located within the I&C equipment rooms of divisions 1 and 4 only.

The SA I&C equipment is located within the I&C equipment rooms of divisions 1 and 4 only.

Space is available in each I&C equipment room for possible modifications to power supply and air conditioning equipment. This will allow the preparation and implementation of future changes without affecting operation of the plant or its safety systems.

The MCP [PICS] processing units are installed in the I&C equipment rooms of divisions 1 and 4 only.

The I&C equipment directly linked to the HMI equipment or which is used frequently by operators, is installed mainly at the MCR level, either in the MCR itself or in the IT rooms. This mainly applies to the MCP [PICS] peripherals, but also applies to access control equipment, fire monitoring, video and telephone systems. The peripherals for the monitoring systems, i.e. loose parts detection, turbine/generator vibration monitoring, seismic monitoring, flux map calculator, and elements of the radioactivity monitoring systems, will be installed in the peripheral systems monitoring room.

The I&C equipment used for the Conventional Island or the Balance of Plant (BOP) are installed in the I&C equipment rooms on the conventional island or in the rooms dedicated to the BOP respectively.

The configuration management and diagnosis tools components of the I&C equipment are installed in the I&C maintenance room, situated in the safeguard building and electrical building at the MCR level.

Locally controlled I&C components and systems are installed near the associated mechanical equipment (e.g. emergency generator sets and diesel building ventilation). The monitoring of their main functions and faults is performed using the MCP [PICS].

The I&C equipment for the fuel handling systems (e.g. the refuelling machine and the swing bridge) is integrated into the mechanical systems or located nearby.

Main Control Room (MCR)

The MCR is located in a bunkered area (division 2), protected against radiation, external and internal missiles and earthquakes. All equipment installed in the MCR, whether or not it is required to operate in a seismic event, is designed not to interfere with the operators in performing their tasks, i.e. to maintain its stability (at least seismic class 2). Functional independence and physical separation are taken into account when equipment items of different safety classes are in close proximity within the MCR.

Four trains of ventilation and power supply, as well as lighting, are designed to maintain operational conditions in the MCR and the monitoring of the plant in all PCC and RRC conditions. The environmental conditions in the MCR are such as to allow the operators to work effectively and comfortably. The layout of the MCR level assures access by the operators into the MCR in all operating conditions of the unit. Evacuation of the MCR is possible by short routes to the lower level where the RSS is located.

The MCR space is sufficient to allow the shift operating team to perform all necessary actions. The layout of the different operational areas facilitates co-ordination and communication between the members of the operating team.

The layout of the MCR level takes into account a limited need for access to the MCR by other staff members of the unit while preserving the necessary space for I&C staff to communicate with the fire patrol, maintenance teams and other staff in other rooms (e.g. the Head of Operations' office, the I&C maintenance room, the padlocking room and the peripheral systems monitoring room).

The computerised operator workstations, the POP, the MCS [SICS], the severe accident panel, the communication facilities, the PSOT HMI unit and the centralised fire alarm system are installed in the MCR.

MCR related rooms

The Technical Support Centre (TSC) is located outside the MCR and has independent access.

There are also washrooms and a kitchen near the MCR.

Operating instructions must be provided to support the operators during activities that could impact on safety. This documentation is available in the offices, in the MCR, in the RSS and in the TSC.

Means of local control is installed if one of the following conditions is met:

- due to its safety function, the equipment must be controlled independently of the MCR and the RSS;
- operations personnel require a direct link between themselves and the process, for example, visual or audible contact; or
- the system operates independently and after commissioning does not need further manual action (at least does not need daily manual action) to perform its function.

Remote Shutdown Station (RSS)

Internal hazards leading to the unavailability of the MCR require the use of the RSS to bring the unit to safe shutdown and maintain it there. The design concept is that such internal hazards e.g. fire in the MCR, will not occur at the same time as other independent failures, accidents or hazards, with the sole exception of possible loss of the external power supply.

In order to achieve independence between the RSS and the MCR, the RSS is installed in a different fire sector (division 3) with a separate access. The corresponding processing units are situated in separate I&C equipment rooms (division 1 and 4) in order to prevent the propagation of internal hazards. The links, for example ventilation ducts between the fire sectors, are designed not to propagate the fire [Ref-1] [Ref-2].

Back-up computerised workstations and communications equipment (phones) are installed in the RSS.

I&C interconnections between the various I&C rooms

I&C interconnections between the various I&C rooms and within an I&C room are isolated electrically in accordance with the following principles:

The different classes of I&C equipment represent low voltage islands in each division; they are isolated electrically from equipment in other buildings and other rooms, also from equipment of different classes in the same room.

For signal and communications connections between I&C equipment, that is achieved by:

- The use of opto-isolators, isolation modules or fibre-optic cables in the case of individual signal connections;
- the use of fibre-optic cables in the case of bus connections.

For power supplies, this is achieved by:

- Provision of separate secure supplies in each of the four divisions
- Dedication of individually protected power feeds to equipment of a single class in a single room

120-minute fire resistant barriers conforming to ETC-F (section 5 of Sub-chapter 3.8) will be installed between the I&C equipment rooms of the various fire sectors and between the service shafts and the cable runs of the various divisions.

I&C cabinets

The arrangement of the I&C equipment rooms and of the safeguard building rooms allows sufficient space for all the I&C cabinets to be installed on the nuclear island.

Inside these rooms, the I&C cabinets for the same I&C system are located side by side to form a suite of cabinets. Requirements are met for independence of the various lines of defence and for access control to the different classified equipment.

The following EMI requirements are taken into account in the installation of the various electronic components in the cabinets:

- enclosed and shielded casing comprising the cabinet itself (notably the doors);
- sufficient separation between the I&C cables and the low voltage power supply cables;
- cable shield bonded directly at the cable entry into the cabinet on an instrument earth bar; and
- additional shielding devices for particular electromagnetic interference sources.

All the cabinets, control desks and panels are linked by their chassis reinforcement to the steel structure of the building in conformance with requirements set down in section 2 of Sub-chapter 8.4.

The Class 1 and 2 I&C equipment cabinets are seismically-qualified against the relevant ground spectrum. The Class 3 and NC I&C equipment cabinets will not affect the Class 1 and 2 cabinets in a seismic event (i.e. no missile effect). The I&C equipment meets the design requirements appropriate to its seismic classification.

I&C cabling

The I&C cabling uses several independent network connections in addition to conventional cabling, notably to interconnect the various I&C systems. They can be described as follows:

1) Level 2 – MCP [PICS] level 2 network connection to operator workstation screens.

2) Main communication network (plant network) - network connections between the four safeguard and electrical building divisions, the diesel building, the conventional island, the nuclear auxiliary building and the effluent treatment building.

3) Connections between one safeguard and electrical building division and another division (for example, point to point connections of class 1 I&C equipment including between the operating system boards and the conventional MCS [SICS] panel).

4) Network connections within a safeguard and electrical building division.

5) Possible connection of level 0 on specific networks (maintenance network for example) for operating functions outside real time for using "intelligent" technologies for sensors and actuators.

All cables between cabinets inside I&C equipment rooms pass through the cable deck under the rooms. The cables between the I&C rooms of different divisions, or from the I&C room to the process, are drawn into the trunking for the various divisions. The I&C interconnections between divisions use fibre-optic networking with no metal parts, except for the NCSS. If copper cables are used, isolation devices must ensure that an internal hazard arising from a single failure cannot lead to the loss of Category A and B I&C Functions in more than two divisions.

The I&C control and measurement cables as well as the network cables (fibre-optic or co-axial) are separated from the low and medium-voltage cables, in accordance with the recommendations of section 1 of Sub-chapter 8.4. Separate routing in the trunking or metal service shafts on the independent cable routes is required only for the cables for the detection of neutron flux and radiation.

Class 1 and 2 signals assigned to the different divisions do not use the same cabling, the same sub-distribution network or the same penetrations and are protected against the propagation of an internal hazard between divisions. They do not use the same junction boxes or the same cables as Class 3/NC signals or they are clearly separated from the latter, at least in the main channels.

The cabling to the MCR is mainly the junction cabling to the MCS [SICS] conventional panel which is linked through the electronic equipment rooms via the trunking/cable trays dedicated to each division. The cabling from the MCP [PICS] processing units (situated in divisions 1 and 4) to the MCR and the RSS is separately laid to each division via independent cable trunking so as to provide protection against possible internal hazards.

Shielded earthed conventional I&C cables are used between level 1 and level 0. The concept of earthing which is based on an earth loop around each building and a mesh network connected to the I&C equipment between the buildings includes protection against lightning conforming to the requirements set down in section 2 of Sub-chapter 8.4.

Fibre-optic cables are used for transmission in the applications where insensitivity to electrical or electromagnetic interference, galvanic isolation between systems or divisions, or bus length up to 2,000 m, is required. Because several networks are used, the applications can be connected by gateways, routers and switches.

Separation means are used for the fibre-optic interconnecting local networks across a division with high data concentration (for example the plant network or the level 2 network). The local networks are tolerant to a single failure (by using a redundant local network or bus ring) so as to achieve a high level of reliability for data transmission and will be laid in different cable ducts so as to provide protection against possible internal hazards.

3. QUALIFICATION PRINCIPLES FOR THE VARIOUS INSTRUMENTATION AND CONTROL COMPONENTS AND SYSTEMS

3.1. INTRODUCTION

Definition of assessment

Judgement based on evidence of the suitability of I&C items for the performance of a specific function or type of function.

Definition of evaluation

Attribution of a qualitative or quantitative value to the characteristics of a system.

Definition of qualification

The I&C qualification is the process by which an I&C item is shown to be capable of responding continuously to design requirements for safety performance, in the environmental conditions existing at the moment that it is needed. Refer to Sub-chapter 7.7 for details of the standards to be used for the qualification process.

An I&C item is defined as a single I&C component or an I&C system.

I&C qualification covers both I&C hardware and software. The term I&C Item encompasses:

- the I&C components that can be configured in an I&C system conforming to the I&C system specifications; and
- the I&C systems supporting the I&C functions specified in the I&C functional specifications;
- smart instruments used to provide or condition inputs to the I&C systems. Refer to Sub-chapter 7.7 for the qualification process for smart instruments.

According to the above definition:

- qualification concerns only the I&C items involved in the support of Category A, B and C I&C Functions. The qualification requires different levels of depth of evaluation of the I&C item depending on the classification of the I&C system or equipment; and
- qualification must be maintained during the entire lifetime of the I&C item.

The life cycle:

- starts with the specification and the selection of I&C items;
- continues with the operation, maintenance and possibly modification and replacement of the I&C item; and

- ends when the safety function that the I&C item supports is no longer required.

Qualification requires:

- as input data, the assessment and evaluation of the suitability of the selected I&C item. This is based on a comparison of the required characteristics of the I&C item with the technical specifications for the I&C item;
- the evaluation and assessment of the compliance of the I&C item with its specification; and
- a final assessment to ensure that the elementary systems are able to meet their specified safety functional requirements.

3.2. QUALIFICATION AND I&C LIFE CYCLE

A feasibility study of the qualification of the I&C item defines the main concepts and steps of the qualification process and demonstrates that:

- the qualification is feasible in the context of the requirements of the equipment class of the I&C item;
- the requirements are verifiable by a process limited to a cost-effectiveness report by a person or machine;
- all new developments will meet the safety requirements from the outset; and
- the qualification can be maintained as long as the safety function in which the I&C item participates is required.

A qualification plan defines the main steps of the qualification of the I&C item based on the feasibility of its qualification.

Following the I&C item life cycle stage:

- a compliance assessment ensures that the I&C item meets its specification. It completes the design stage and allows the inclusion of the I&C item in the design;
- a final assessment ensures that after it is installed and commissioned, the I&C item will support the safety function as required; and
- during operations and replacement, the I&C item will be maintained in a qualified state for continuing operation (Sub-chapter 7.2 - Figure 9).

3.2.1. Qualification of an I&C item during the specification, design and implementation phases

The specification of an I&C item is evaluated and assessed to ensure that it meets its technical specification.

The evaluation and assessment demonstrate that the I&C item meets its technical specification.

At the specification and selection stage of an I&C item, the designer selects either an already available I&C item or develops a new I&C item suitable for fulfilling its safety functions.

The I&C item can be a single I&C component or a product line of equipment. The I&C components can be configured to perform various types of I&C function (typical application functions).

Input data for suitability assessment

Before acceptance of the specification of the I&C item, the suitability study evaluates and assesses the compliance of the I&C item specification with the technical specification.

If pre-developed items are selected, the evaluation documentation on the conformity of the pre-developed items must be taken into account to facilitate the qualification process.

Assessment and evaluation of conformity

On the basis of the suitability assessment, a qualification plan is developed and implemented in order to evaluate and assess the compliance of the I&C item with the qualification specification.

The qualification plans should be agreed between assessor and designer so as to limit analysis and tests to those sufficient to demonstrate compliance with the relevant acceptance criteria.

The qualification plan defines the safety relevant aspects of the qualification for the I&C systems and components, for which compliance shall be evaluated and assessed.

These are:

- the specified requirements on components and configurations of the I&C item (e.g.: functionality, performance, reliability, fault tolerance...);
- the environmental conditions (i.e. temperature, electromagnetic fields, etc.) under which compliance shall be demonstrated;
- the requirements on the I&C system software (for computer based items); and
- the specified plant-specific functional requirements (e.g. the application functions of the plant, specific service functions...).

The qualification plan:

- identifies the qualification documentation already available; and
- identifies the I&C item specifications and documentation that are the basis for qualification.

The qualification plan establishes:

- the principles for evaluating the properties of components and configurations of the I&C item (e.g. the use of type tests, analysis...);
- the approach for evaluating the properties of the I&C system software; and
- the approach for evaluating the properties of the plant-specific functions (e.g. the application software).

The qualification plan:

- specifies the acceptance criteria for the tests and test sequences;
- specifies the acceptance criteria for analysis;
- indicates whether acceptance shall be based on quantitative figures or on qualitative judgement; and
- specifies the documentation to be produced for each property to be qualified.

The compliance assessment is based on the evaluation of the results.

The qualification plan includes the qualification of the I&C equipment (see section 3.5 below) and the specific I&C qualification (see section 3.6 below).

3.2.2. Final assessment

Installation checks and commissioning tests demonstrate that the I&C item functions correctly within the overall I&C system and with the equipment it controls so as to meet its safety functional requirements.

The final assessment gives assurance that all I&C items are capable of continuously meeting the design basis performance requirements needed for the safety function under the environmental conditions when the safety function is required.

3.2.3. Maintaining the qualification

The qualification must be maintained over the operating lifetime of the I&C system in the following cases:

- modification of the physical configuration of the I&C system;
- replacement of equipment or software of the I&C system;
- modification or extension to the application software;
- modification of any tools that are used for the qualification evaluations; and
- modification of interfaces.

3.3. QUALIFICATION PROCESS

The UK EPR I&C consists as far as possible of I&C systems using already available configurable equipment product lines.

The qualification process of such I&C systems evaluates and assesses:

- the general (non plant-specific) properties of the I&C system, noting that the majority of general properties of the I&C system are covered by the evaluations and assessments already available for the equipment product line (see section 3.3.1 below); and

- the plant-specific properties of the I&C system.

If an equipment product line is used for which the properties for equal or more severe service have already been assessed; only the plant-specific evaluations and assessments are necessary.

The qualification process is summarised in Sub-chapter 7.2 - Figure 10.

3.3.1. Non plant-specific evaluation and assessment

Non plant-specific evaluations and assessments address the use of I&C components and the basic configuration(s) of the equipment product line.

The basic configurations are I&C systems built up with I&C components of an equipment product line that operate together in defined architectures. These architectures are representative of permitted configurations that can be achieved with the equipment product line.

The evaluation and assessment of:

- the properties of the components and the basic configurations of the equipment product line;
- the properties of the system software of the equipment product line (i.e. evaluation of the confidence that the system will perform as specified); and
- the properties of the development tools of the equipment product line.

give assurance that the components of the equipment product line:

- perform their functions as specified in the component specifications; and
- operate together in all the allowed configurations as specified in the equipment product line specification.

3.3.2. Plant-specific qualification

The plant-specific evaluation and assessment give assurance that the properties of the equipment product line make it possible to build up the I&C systems to meet their specifications, i.e. the already available assessments of the general properties of the equipment product line give assurance that:

- the intended configurations of the I&C systems are permitted configurations for the equipment product line; and
- the components of the equipment product line function together in the intended configurations as specified.

3.3.3. Product line documentation

The documentation specifies the properties of all I&C components and the permitted configurations of the equipment family.

The documentation should provide a means for determining:

- the safety, integrity and performance that can be achieved for the plant application functions in the anticipated configuration(s);
- the functional behaviour and performance in defined normal and abnormal conditions; and
- the influence of the functions and components not submitted to qualification.

The I&C components and permitted configurations that have already been through the qualification program should be explicitly identified in the equipment product line documentation.

3.4. QUALIFICATION PRINCIPLES

Qualification of an I&C item may be achieved by:

- tests;
- analysis; and
- operating experience.

These may be used individually or in any combination depending upon the particular properties of the I&C item.

3.4.1. Tests

Tests are separated into type tests and plant-specific tests.

Type tests are performed independently from the intended use of the I&C item in the plant.

Plant-specific tests are performed to give assurance that the I&C items meet the plant-specific requirements.

Type tests

All equipment used in Class 1 and 2 systems will be type tested.

Type tests are performed on a sample of I&C items of the same design.

Type tests of I&C equipment using simulated environmental conditions constitute the preferred method for demonstrating that the sample complies with the requirements of the I&C item when submitted to the most severe environmental conditions, including post accident conditions, under which the I&C items are required to perform their task.

Normally type tests are performed in the context of non-plant-specific qualification.

Plant-specific tests

Specific tests are carried out in addition to the type tests in order to cover the specific use in the plant of the I&C item. Specific tests can be carried out mostly in the supplier's factory and completed by operational tests on site.

3.4.2. Analysis

Analysis is used in most steps of the qualification process. Some examples below describe the use of analysis.

Analysis of the I&C item specifications is the basic method for the definition of the qualification plan.

In particular, analysis is the basic method for evaluating hardware and software development (e.g. this analysis evaluates hardware and software design, component tests, verification/validation and documentation).

Analysis (e.g. failure effect analysis, critical load analysis ...) is appropriate for the evaluation of properties that cannot be demonstrated by tests.

Analysis of the results of type tests and evaluation against the acceptance criteria forms the assessment of compliance for type-tested properties.

3.4.3. Operating experience

A conventional (as opposed to computer based) I&C item that has operated successfully may be qualified for equal or less severe service (i.e. less severe operating conditions for the I&C item with a similar functional task) on the basis of operating experience.

Operating experience may also support the evaluation of the quality of already available items including software.

Operating experience will be evaluated on the basis of both:

- the accumulated length of operation of the already available I&C item; and
- the history of failure reports and modifications for the already available I&C item.

Operating experience requires accurate collection of the above mentioned data on operating history including similarity of use. Traceable documentation requires an early involvement of suppliers and users.

3.5. EQUIPMENT QUALIFICATION

Equipment qualification is preferably performed by tests.

Type tests have to demonstrate the compliance of the components and intended configurations with their specifications when submitted to the environmental conditions that they must withstand.

Some properties of the components can be evaluated and assessed only if they operate together with other components. Test configurations of components are therefore used to evaluate and assess the component properties.

For programmable equipment, specific test software must be loaded into the test configurations so as to make it possible to demonstrate that the items perform their functions correctly during the test (e.g. for EMI and seismic tests).

In most cases evaluations and assessments of components and test configurations of the selected equipment product line are already available.

These already available evaluations are analysed for the purpose of verifying whether the test configurations cover the specified properties of all permitted configurations of the equipment product line: (mounting, installation, load and temperature distribution inside the cabinets, application functions running during EMI and seismic tests, etc...).

Additional plant-specific tests may be necessary depending on the results of this analysis.

Refer to Sub-chapter 7.7 for additional details on production excellence and independent confidence building activities used to support the selection and substantiation of the system platforms.

3.6. SPECIFIC QUALIFICATION FOR I&C SYSTEMS

This section addresses evaluations and assessments that are additional to those specified in section 3.5 above.

It focuses on computer based I&C systems built up from equipment product lines. These are the most complete and most usual cases [Ref-1] to [Ref-3].

The qualification requirements of conventional I&C systems may be derived from this section.

The qualification plan distinguishes between different properties of the system, software and the development tools (see Sub-chapter 7.2 - Figure 11).

The qualification plan takes as much advantage as possible from pre-existing evaluations that can be assessed in a non plant-specific qualification step.

Non plant-specific evaluations address:

1. Properties of components and anticipated configurations,
2. The properties of the system software, covering for example:
    - Operational Software.
    - Application software libraries.
    - System testing software.
    - Operating features (service functions, self test, modes of operation ...).
3. The properties of the development tools used for example for:
    - Configuration.
    - Implementation.

However, additional evaluations are required to give assurance that the I&C system complies with its specifications.

Plant-specific evaluations address:

1. The properties of the application software.
2. The properties of the integrated and configured hardware and system software.
3. The properties of the complete I&C system.

The following properties are considered when establishing a qualification plan and are evaluated and assessed in terms of compliance with the I&C system specification.

3.6.1. Properties of components and intended configurations

If the qualification plan requires evaluation and assessment of I&C system properties, the already available evaluations of the properties of the equipment product line are analysed to check whether the components and the permitted configurations cover the specified properties of the I&C system.

The degree of evaluation and assessment depends on the equipment classification of the I&C system:

- Functional properties are related to the different types of application functions that the I&C system is able to execute.

In order to give assurance that the I&C system is able to execute the specified application functions, the functional properties are evaluated and assessed.

- Performance properties are related to the speed and accuracy with which the I&C system executes the application functions.

These properties may be evaluated together with the functionality properties, because independent evaluation is impossible in many cases.

- Safety integrity properties are related to the reliability of the I&C system. This depends on:
  - the reliability of the I&C system hardware that can be calculated on the basis of reliability data for the components and for the I&C system architecture; and
  - the safety integrity of software that can be evaluated by qualitative analysis of the development process in order to assess a sufficient degree of confidence in the software. Refer to Sub-chapter 7.7 for details of Production Excellence and Independent Confidence Building Measures.

3.6.2. Properties of system software

The evaluation of confidence in the system software is particularly important for the assessment of the safety integrity achievable for the specified application functions.

The system software must be consistent in terms of safety integrity estimated on the basis of the reliability of the system equipment.

The analysis of confidence in the system software is strongly linked to the development process.

Development proceeds in requirement stages for Class 1, 2 and 3 equipment. These requirements concern, for example:

- the design of the equipment and software architecture;
- the development process;
- the verification and validation process;
- the appropriate use of commercial components supplied by third parties (processors made by Intel, Motorola,…); and
- additional validation tests.

The evaluation of confidence is based on an analysis of the development documentation.

The analysis verifies:

- the content of the documentation;
- that the development process follows well defined stages;
- that the results of each stage are verified by analysis or testing; and
- that the software is validated after integration into the equipment.

The I&C IT systems constructed from equipment product lines represent the most complete and the most up-to-date case. Thus, this evaluation is carried out by analysing the documentation of the equipment product line. Already available evaluations are used to assess confidence in the system software.

Gradation of requirements

The evaluation and assessment of the confidence in system software components depends on the equipment classification.

Gradation criteria for the individual equipment classes follow the different system specification requirements.

Within the system software, there are functions of different importance for the execution of the application functions. A graduated scale of confidence is assessed within each class of equipment. The criteria can be set out as follows:

- The highest confidence level is demanded for the functions whose results directly affect the application functions (for example, application software libraries and exception processing in the event of errors...).
- A lower level of confidence is demanded for:
  a) functions designed to have their results verified off-line;
  b) operating functions whose results do not affect the application functions; and
  c) operating functions whose results have only an indirect influence on the operation of the unit (e.g. production of messages or diagnostic signals on the state of equipment, recording data, modifying parameters, periodic testing).
- Confidence assessment is not required for functions which are not used, in the sense that they do not call into question the confidence in the system software.

3.6.3. I&C system development tools evaluation and assessment

The evaluation and the assessment of development tools depend on:

- the task supported by the development tool (e.g. transformation of source code into executable code, verification and validation of the application software, service, hardware configuration);
- the consequences of errors potentially introduced by the development tools; and
- what verification might detect or mitigate errors introduced by a development tool.

The development tools that influence the safety integrity of the safety functions (notably the corresponding executable code) are identified in the qualification plan.

An evaluation and an assessment of these tools is necessary if all of the conditions below are met:

- the tool output can directly introduce, or induce, an error into the executable code;
- the tool output is not systematically verified;
- alternative development processes and methods do not exist to mitigate the consequences of errors induced by tools; and

- the tool does not benefit from a large amount of operating experience for similar use.

3.6.4. Application software evaluation and assessment

The evaluation of confidence in the application software analyses:

- the application software, in well defined steps; and
- the verification and validation process, which is part of the development cycle of the application software.

In most cases the application software is specified and developed by means of functional diagrams. The executable code is generated automatically from these diagrams. The whole development process is supported by I&C system tools.

Starting from the functional diagram, the specification of the application software is based on existing qualified application software libraries. The resulting application software contained in a database constitutes the starting point for the automatic generation of the code that will be processed by the computer based I&C system.

This way of specifying the application software facilitates the evaluation of the confidence. In effect the application software specifications can be verified by process engineers. This method of application software generation is recommended for all the classes of I&C systems.

3.6.5. Evaluation and assessment of the plant-specific configurations

Many of the I&C system properties depend also on plant-specific configurations, operation and maintenance procedures.

The plant-specific configurations are evaluated and assessed against the general design requirements of RCC-E (see section 3 of Sub-chapter 3.8) complemented with specific data for the EPR project.

3.6.6. Integration and validation of the application software in the I&C system.

Before the I&C system is installed in the plant, the application software is validated after integration of the executable code in the I&C system using a test platform outside the plant.

Evaluation and assessment gives assurance that the validation is carried out and documented in accordance with the I&C system validation plan.

SUB-CHAPTER 7.2 - TABLE 1

Allocation of types of I&C function to systems

Types of I&C Functions	I&C Function category	Level 1 systems	Level 2 systems	
			Commands note 1	Display
Normal operation, non safety related	non-categorised	PAS	MCP [PICS]	MCP [PICS]
Normal operation safety related, not seismically qualified	Cat C /B / non-categorised Non seismically qualified	PAS or RCSL	MCP [PICS]	MCP [PICS]
Core control	Cat B	RCSL	MCP [PICS] and MCS [SICS]	MCP [PICS] and MCS [SICS]
LCO surveillance	Cat B or C	RCSL or PAS note 2	MCP [PICS]	MCP [PICS]
Limitation	Cat B or C Non seismically qualified	RCSL or PAS note 2	MCP [PICS]	MCP [PICS]
Safety related and seismically classified functions	Cat B seismically qualified	SAS	MCP [PICS] and MCS [SICS]	MCP [PICS] and MCS [SICS]
Reactor Protection	Cat A	RPR [PS] SAS NCSS	PSOT and MCS [SICS]	MCP [PICS], PSOT and MCS [SICS]
Post-accident functions	Cat B	SAS (optionally RPR [PS])	MCP [PICS] and MCS [SICS] (optionally PSOT)	MCP [PICS] and MCS [SICS] (optionally PSOT)
Autonomous safety systems support	Cat B	SAS	MCP [PICS] note 3 or local control stations	MCP [PICS] note 3 or local control stations
Prevention of significant radioactive release	Cat B	SAS	MCP [PICS] and MCS [SICS] or local control stations	MCP [PICS] and MCS [SICS] or local control stations

Types of I&C Functions	I&C Function category	Level 1 systems	Level 2 systems	
			Commands note 1	Display
Faults resulting in PCC-3 or PCC-4.	Cat B	SAS	MCP [PICS] and MCS [SICS]	MCP [PICS] and MCS [SICS]
Mitigation of Common Cause Failure (CCF) impacting RPR [PS]	Cat B	SAS	MCP [PICS]	MCP [PICS]
Mitigation of CCF impacting mechanical safety systems	Cat B or C	PAS, RCSL, SAS or RPR [PS]	MCP [PICS] or PSOT	MCP [PICS] or PSOT
RRC-A functions				
Type 1 (not a diverse LOP, non-seismic, not an SPPA-T2000 initiated fault sequence)	Cat C	PAS	MCP [PICS]	MCP [PICS]
Type 2 (diverse LOP or seismic, not an SPPA-T2000 initiated fault)	See note 4	SAS	MCP [PICS] and MCS [SICS]	MCP [PICS] and MCS [SICS]
Type 3 (SPPA-T2000 initiated fault sequence)	See note 5	RCSL or RPR [PS]	MCS [SICS] or PSOT	MCS [SICS or PSOT]
Severe accident mitigation functions:	Cat C seismically qualified			
RRC-B LOOP scenario		SA I&C	Severe accident panel	Severe accident panel
RRC-B other scenarios		RRC-B SAS	MCP [PICS] for some functions	MCP [PICS]
Total loss of computerised I&C	See note 6	NCSS	MCS [SICS]	MCS [SICS]

Note

1) MCP [PICS] commands to higher class systems are validated at the level 1 system prior to implementation. RPR [PS] commands are entered by the operator and validated on PSOT
2) The initialisation sub function can also be implemented in the RPR [PS].
3) Limited to surveillance of main parameters.
4) Category A functions for diverse line implemented in a class 2 system due to seismic claim.
5) Category C functions implemented in a class 2 system due to diversity claim.
6) Functions up to Category A implemented in a class 2 system to support the overall reliability claim on the I&C.

SUB-CHAPTER 7.2 - TABLE 2

I&C systems classification and reliabilities

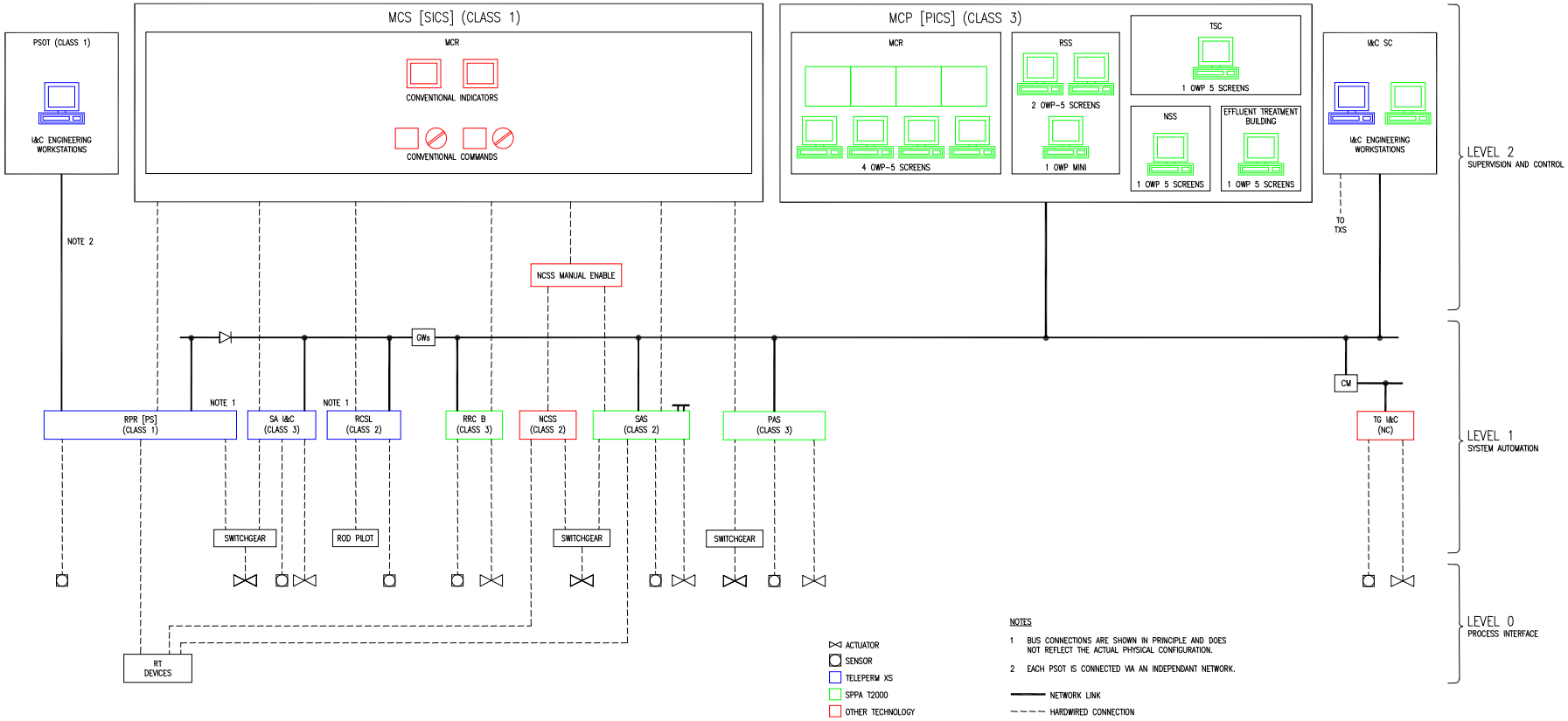
I&C Systems	Classification	Claimed reliability (failure per demand or per year as appropriate)
Protection System (RPR [PS])	Class 1	10^{-4}
Safety Information and Control System (MCS [SICS])	Class 1	Note 1
Safety Automation System (SAS)	Class 2	10^{-2}
Reactor Control, Surveillance and Limitation System (RCSL)	Class 2	10^{-2}
Non-Computerised Safety System (NCSS)	Class 2	10^{-3}
Process Automation System (PAS)	Class 3	10^{-1}
Process Information and Control System (MCP [PICS])	Class 3	10^{-1}
RRC-B Safety Automation System (RRC-B SAS)	Class 3	10^{-1}
Severe Accident I&C system (SA I&C)	Class 3	10^{-1}

Note

1) No claimed reliability has been provided for MCS [SICS] as it is not considered a separate system and its discrete devices are effectively considered as part of the elementary systems that they support.

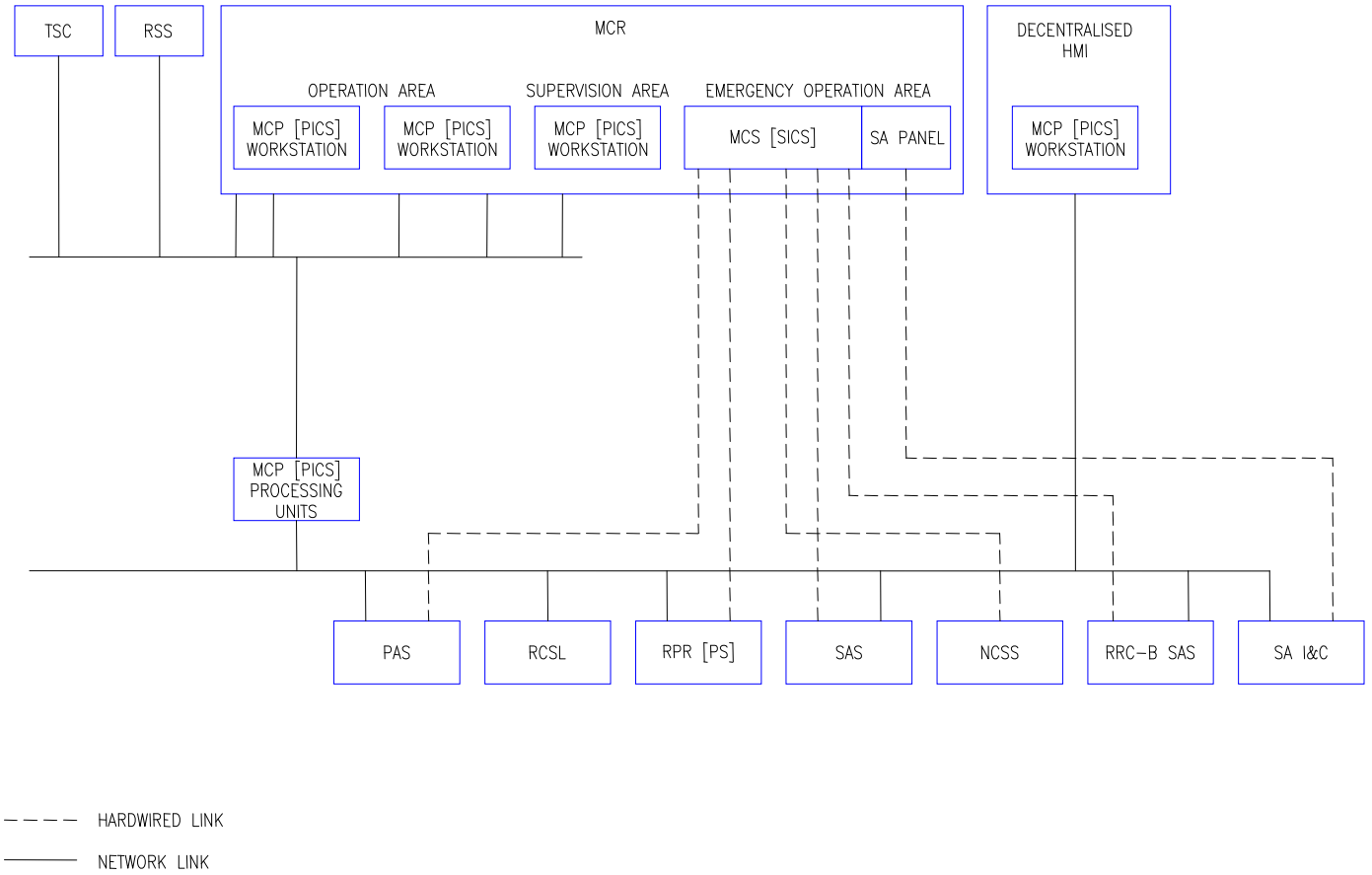
SUB-CHAPTER 7.2 - FIGURE 1

Overall I&C architecture



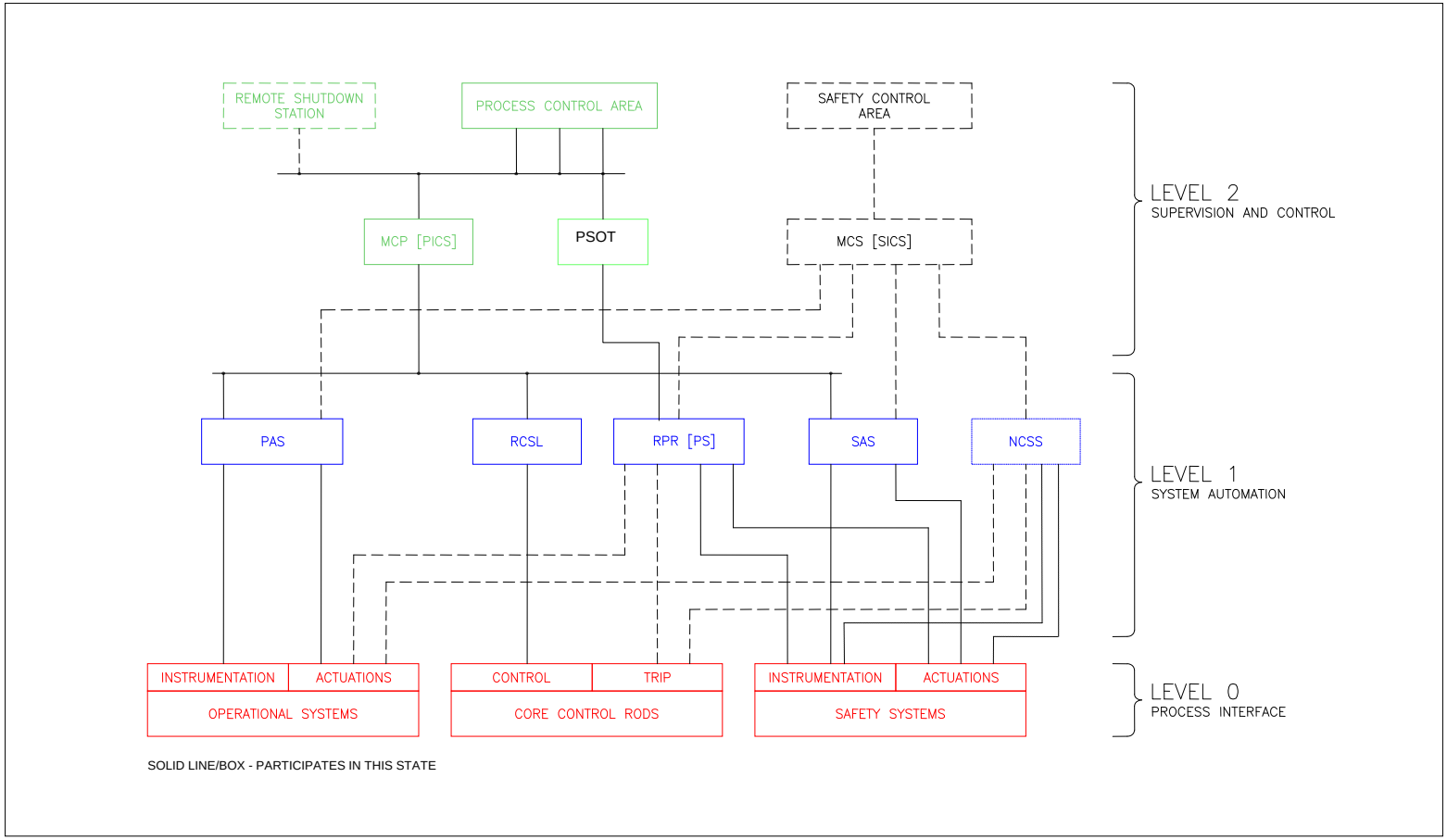
SUB-CHAPTER 7.2 - FIGURE 2

Structure of level 2



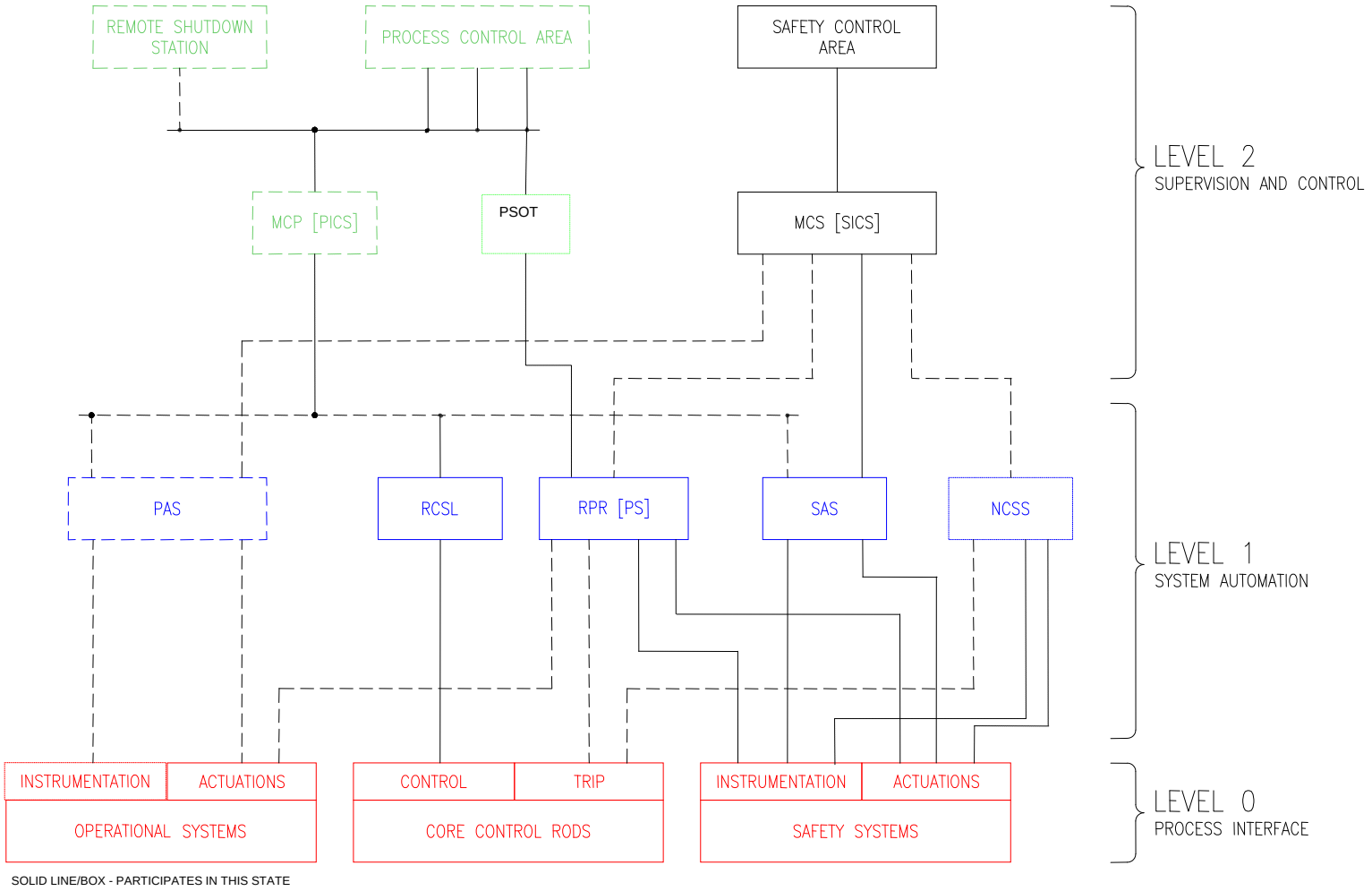
SUB-CHAPTER 7.2 - FIGURE 3

Normal operation



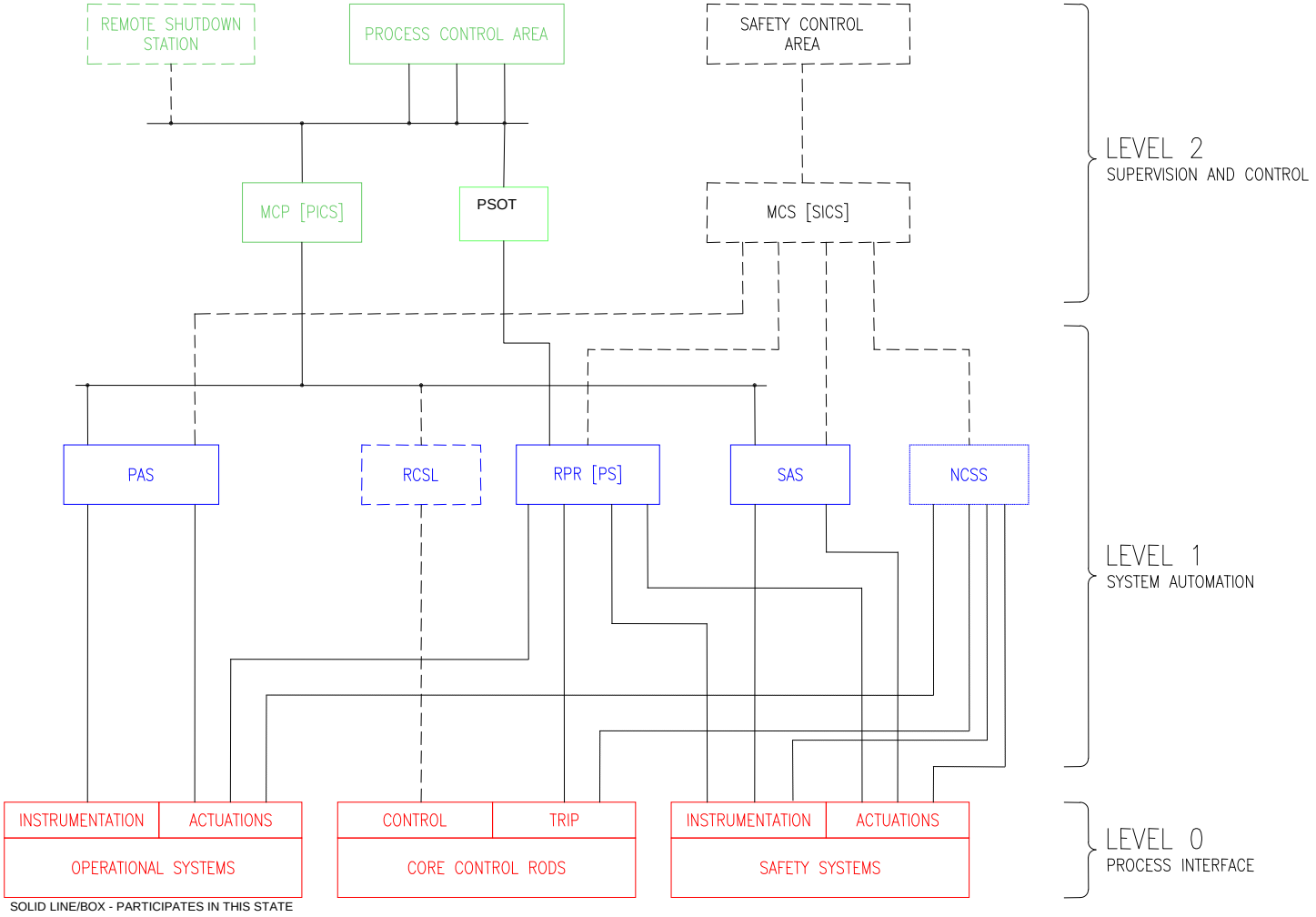
SUB-CHAPTER 7.2 - FIGURE 4

Operation with class 1 and 2 safety I&C systems only



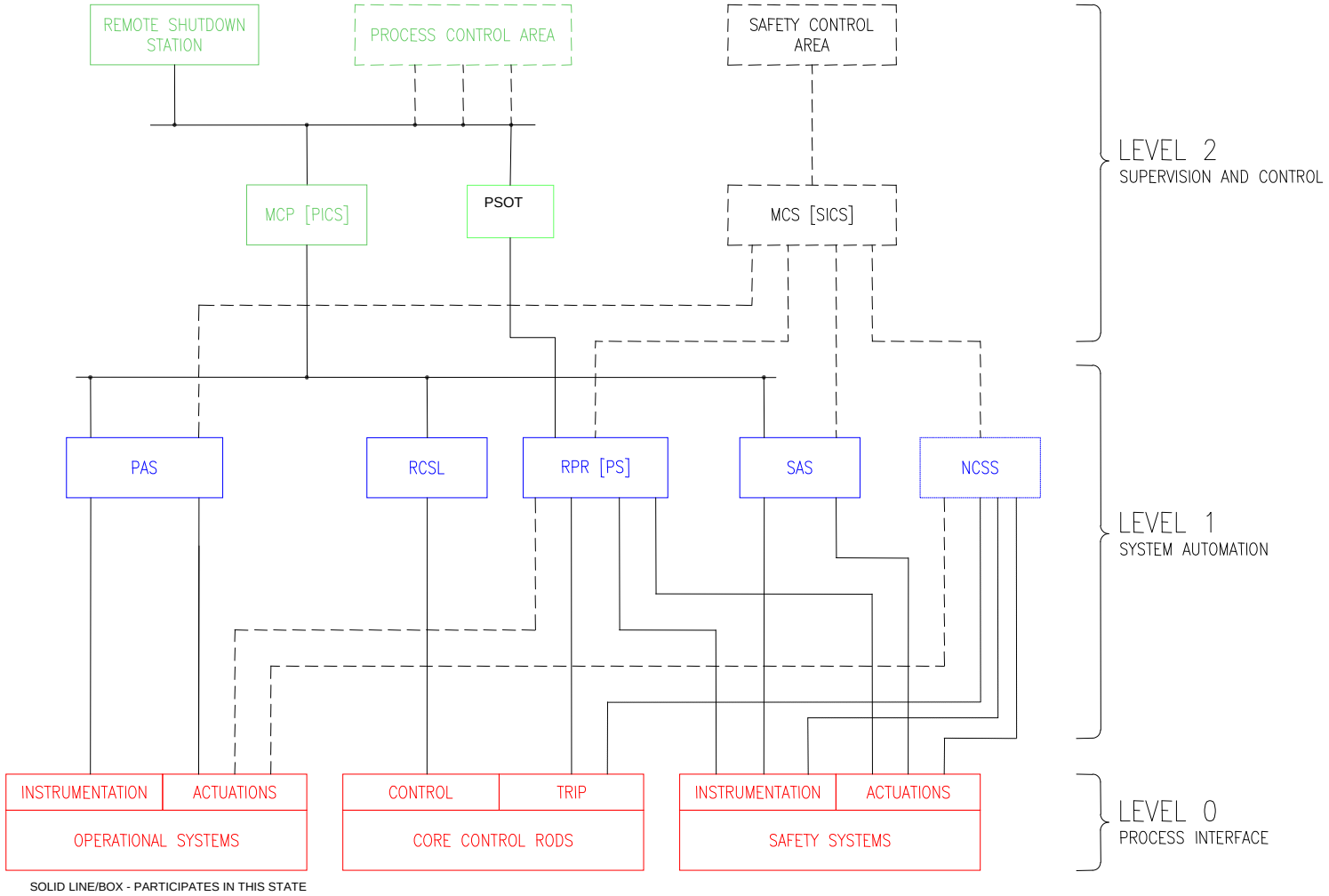
SUB-CHAPTER 7.2 - FIGURE 5

Operation during accident mitigation with the operational I&C systems



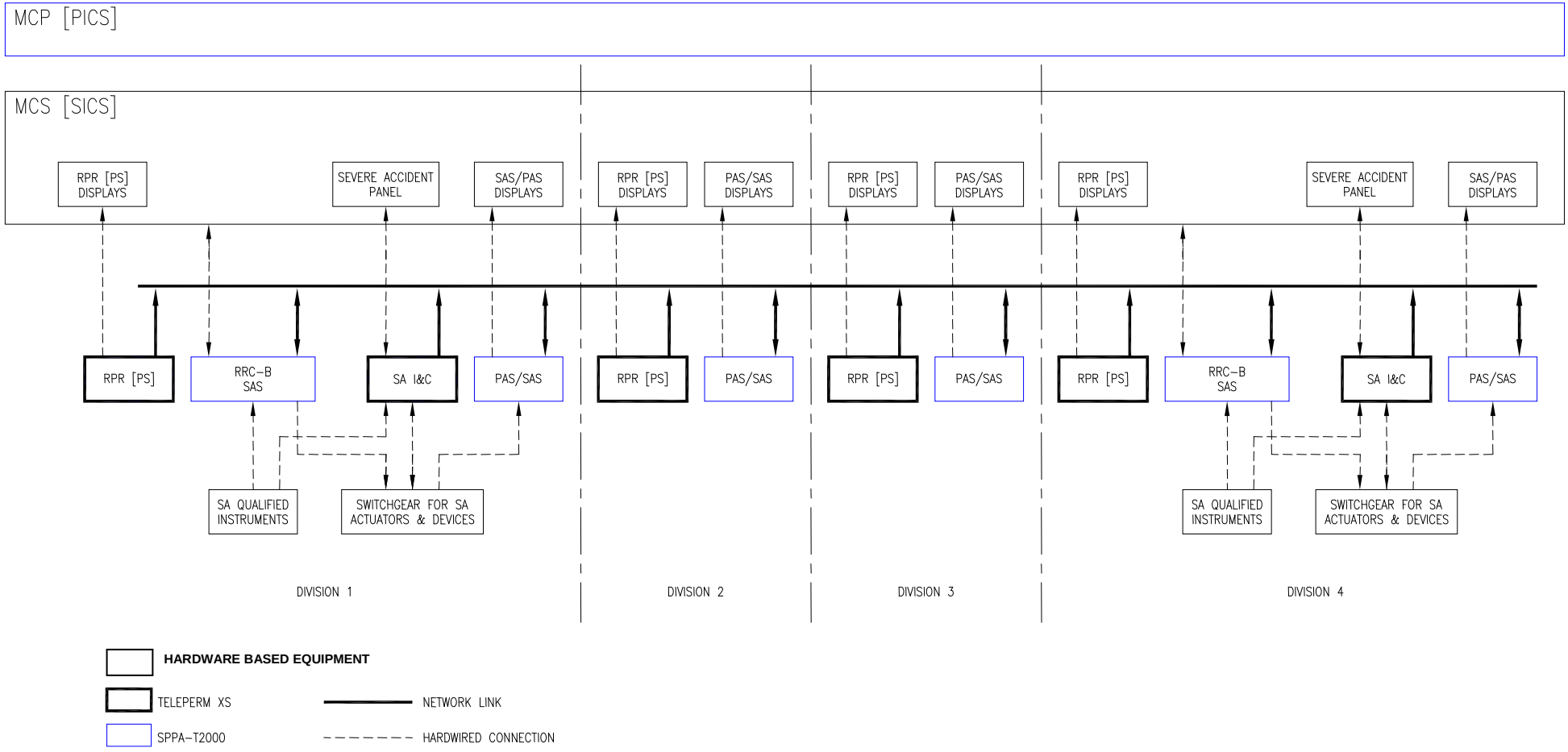
SUB-CHAPTER 7.2 - FIGURE 6

Operation from the remote shutdown station



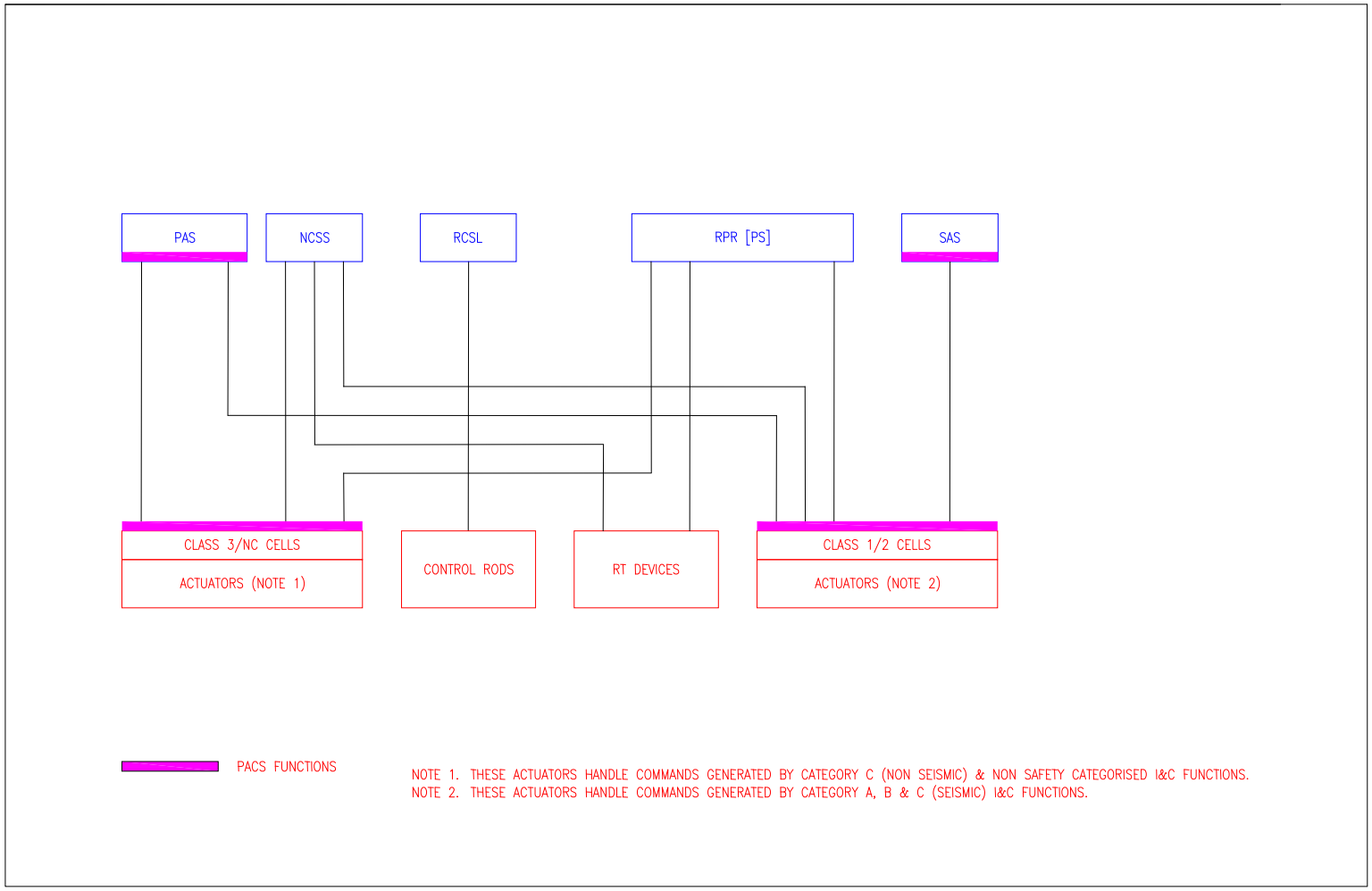
SUB-CHAPTER 7.2 - FIGURE 7

Severe accident I&C principles



SUB-CHAPTER 7.2 - FIGURE 8

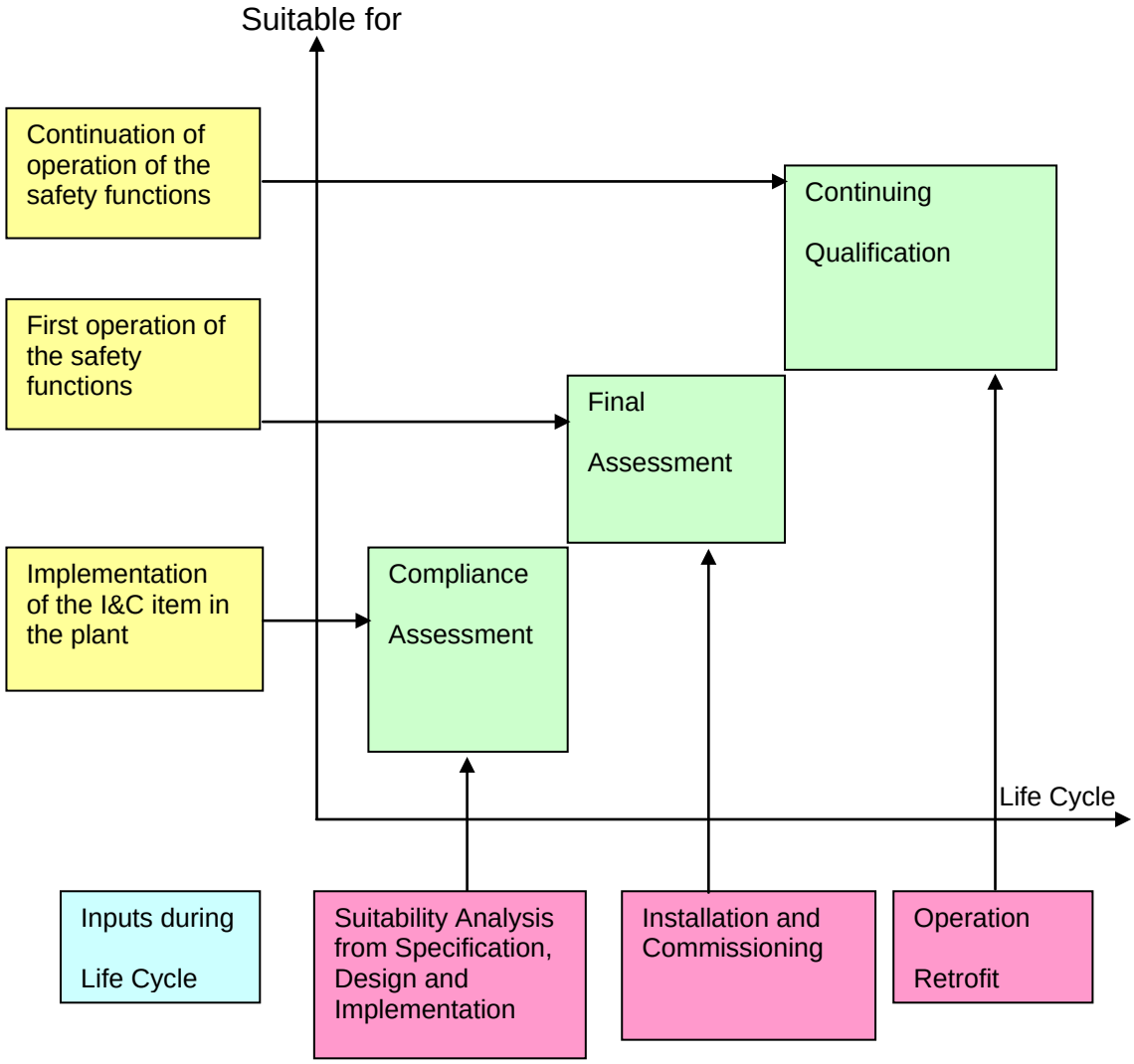
PACS function allocation



SUB-CHAPTER 7.2 - FIGURE 9

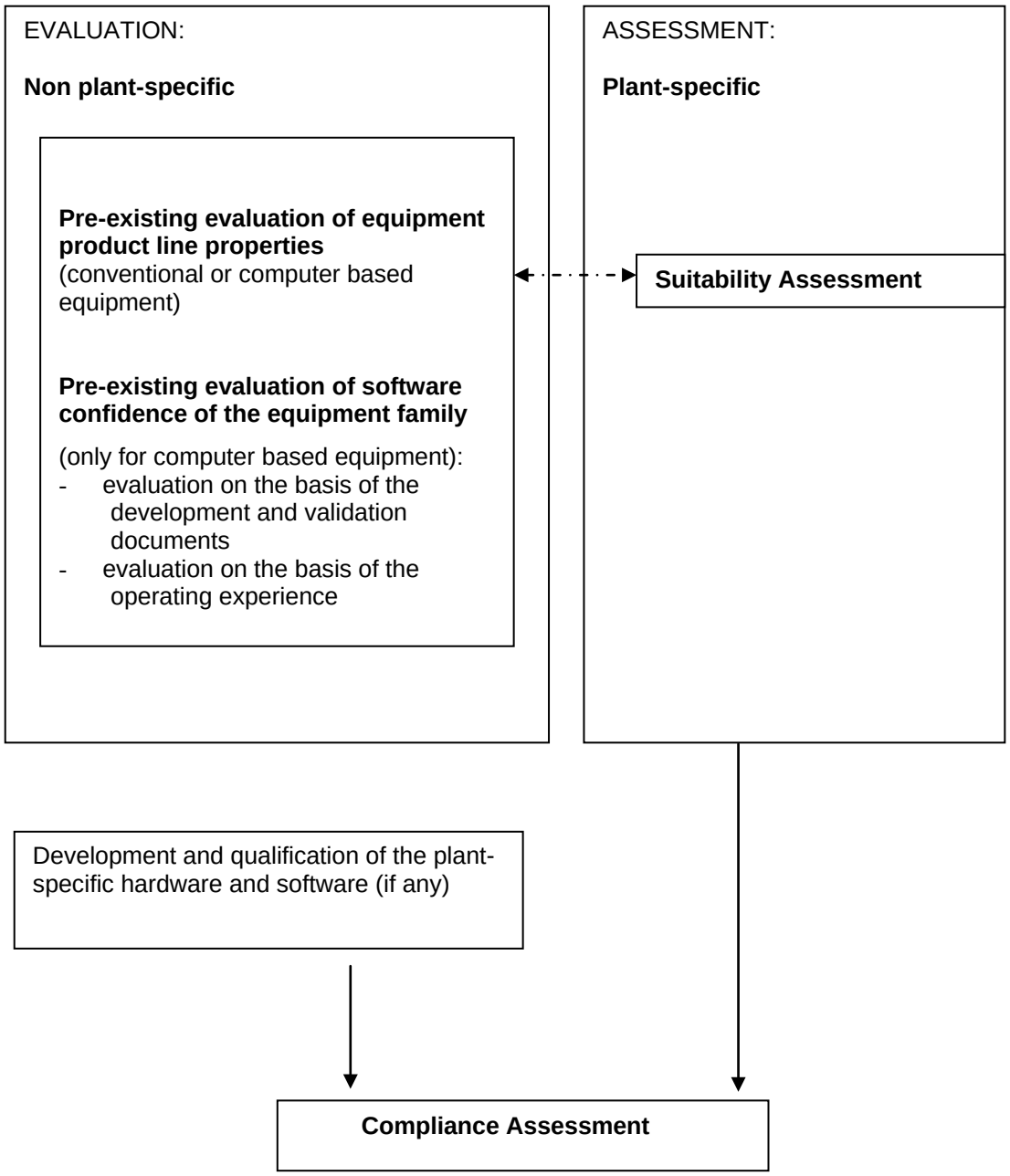
Qualification and life cycle of the I&C item

(Qualification for continuing operation)



SUB-CHAPTER 7.2 - FIGURE 10

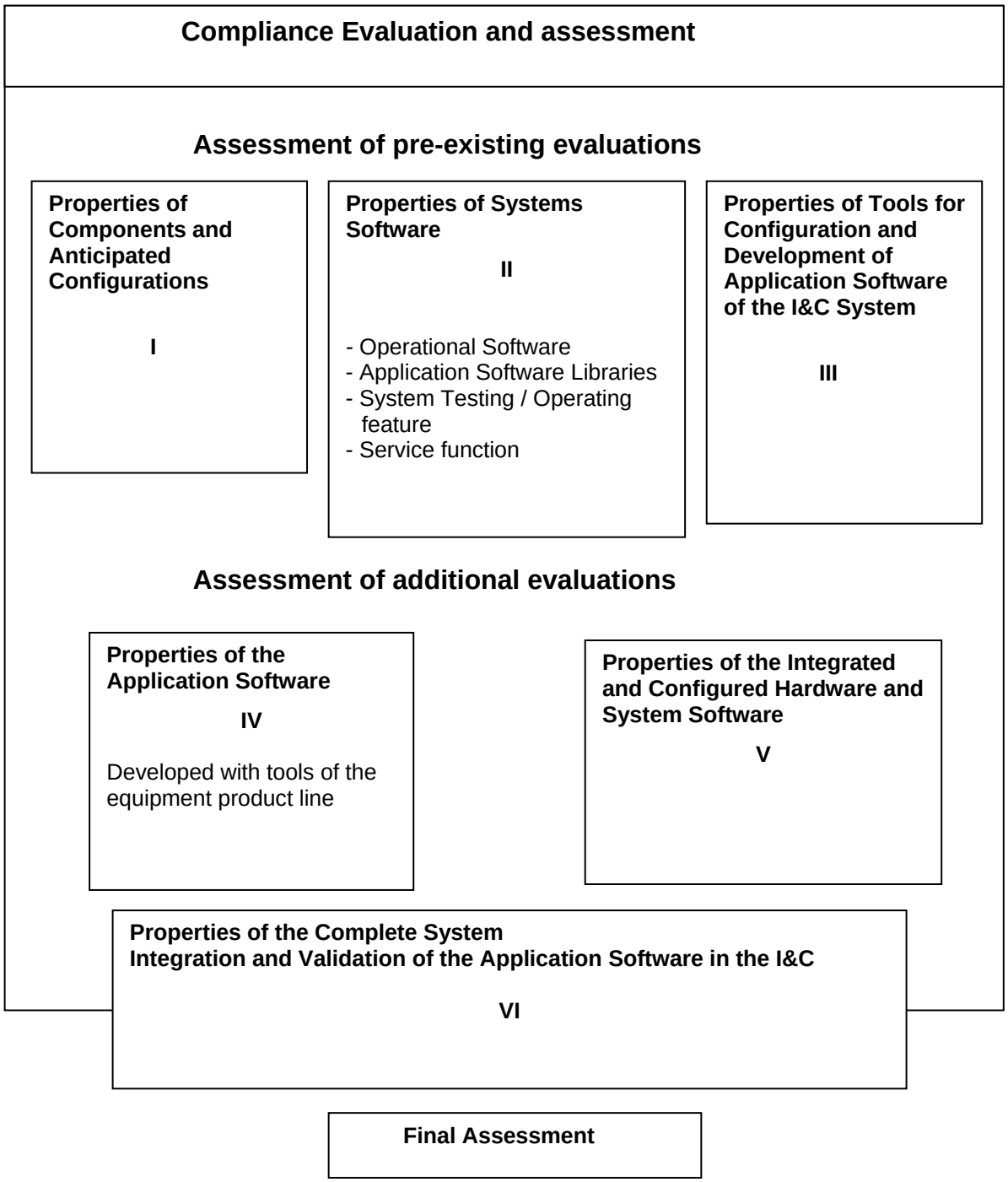
Qualification and life cycle of the I&C item (process summary)



SUB-CHAPTER 7.2 - FIGURE 11

Qualification and life cycle of the I&C item

(System, software and development tools)



SUB-CHAPTER 7.2 – 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. OVERALL INSTRUMENTATION & CONTROL ARCHITECTURE

1.2. DESIGN BASIS

1.2.1. Safety requirements

[Ref-1] UK EPR Generic Design Assessment - Classification of I&C safety features. ECEF091489 Revision E. EDF. October 2012. (E)

1.3. DESCRIPTION OF INSTRUMENTATION & CONTROL SYSTEM ARCHITECTURE

1.3.2. Level 1

[Ref-1] Safety Principles applied to the UK EPR I&C architecture in terms of the requirements for diversity and independence. PEPS-F DC 90 Revision C. AREVA. August 2012. (E)

[Ref-2] Classification of Structures Systems and Components. NEPS-F DC 557 Revision D. AREVA. October 2012. (E)

[Ref-3] UK Health and Safety Executive (HSE). Safety Assessment Principles for Nuclear Facilities 2006 Edition. Revision 1. January 2008. (E)

1.3.3. Level 2

1.3.3.1. Computerised systems

[Ref-1] Substantiation of Independence between PICS and SAS. ECECC121458 Revision A. EDF. July 2012. (E)

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

[Ref-3] Class 1 Control and Display facilities in the Main Control Room and the Remote Shutdown Station. ECECC111829 Revision B. EDF. August 2012. (E)

[Ref-4] Kristel. System specification file. Annex 8: Interlock between HMIs (MCP-SICS-PDR). SY710 Version 6.0. Siemens. March 2009. (E)

1.3.3.2. Conventional systems

[Ref-1] Kristel. System specification file. Annex 8: Interlock between HMIs (MCP-SICS-PDR). SY710 Version 6.0. Siemens. March 2009. (E)

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

1.3.3.3. Locations

[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] 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-3] Class 1 Control and Display facilities in the Main Control Room and the Remote Shutdown Station. ECECC111829 Revision B. EDF. August 2012. (E)

1.3.4. Communication between the instrumentation and control systems

[Ref-1] Analysis Network Qualification - Part 2 Plant Bus and Island Bus. DN 2.2.14 Revision 2.0. Siemens. September 2009. (E)

[Ref-2] Justification of time response end to end on Terminal Bus Plant Bus. ECECC111368 Revision B. EDF. August 2012. (E)

1.3.5. Technology

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

[Ref-2] Protection System – System Description. NLN-F DC 193 Revision C. AREVA. April 2012. (E)

[Ref-3] RCSL - Detailed Specification. NLP-G\2006\en\1007 Revision H. AREVA. June 2009. (E)

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

[Ref-5] NCSS System Specification. TA-2062484 Revision C. AREVA. July 2012. (E)

1.3.6. Independence and Diversity

1.3.6.1. Independence and diversity in Level 0

[Ref-1] Diversity Criteria for Sensors & Conditioning. PELL-F DC 82 Revision C. AREVA. October 2012. (E)

[Ref-2] Functional Analysis For Sensors' Common Cause Failure. PEPR-F DC 83 Revision C. AREVA. October 2012. (E)

[Ref-3] Diversity Implementation plan for sensors & conditioning. PELA-F DC 3 Revision C. AREVA. October 2012. (E)

[Ref-4] 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)

[Ref-5] UKEPR Basis of Substantiation for the Reliability Claims for the PACS Modules. ECECC121662 Revision A. EDF. August 2012. (E)

[Ref-6] Diversity criteria definition for Priority Actuation Control (PAC) module. ECECC120443 Revision B. EDF. August 2012. (E)

[Ref-7] EPR UK - Diversity implementation plan for PAC Modules. ECESN120472 Revision A. EDF. July 2012. (E)

1.3.6.2. Independence and diversity in Level 1

[Ref-1] Architecture of instrumentation and control system EPR UK: design principles and defence-in-depth. ECECC100831 Revision B. EDF. October 2012. (E)

[Ref-2] Safety Principles applied to the UK EPR I&C architecture in terms of the requirements for diversity and independence. PEPS-F DC 90 Revision C. AREVA. August 2012. (E)

[Ref-3] 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)

[Ref-4] Diversity Criteria between Protection System and Safety Automation System. PTL-F DC 3 Revision B. August 2012. (E)

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

[Ref-6] Justification of Diversity between I&C Systems Implemented in I&C Platforms. PELZ-F DC 2 Revision B. AREVA. October 2012. (E)

[Ref-7] Unicorn Project - Platform Specification. TA-2060143. Revision C. AREVA. May 2012. (E)

1.3.6.3. Independence and diversity in Level 2

[Ref-1] Safety Principles applied to the UK EPR I&C architecture in terms of the requirements for diversity and independence. PEPS-F DC 90 Revision C. AREVA. August 2012. (E)

[Ref-2] Overall Approach to Diversity of UK EPR I&C Systems. ECECC121713 Revision A. EDF. August 2012. (E)

1.3.6.4. Functional diversity

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

1.3.6.5. Lifetime management of independence and diversity

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

1.3.7. Reliability

1.3.7.1. RPR [PS] reliability

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

1.3.7.2. SAS reliability

[Ref-1] Reliability Analysis SPPA-T2000/S7. QU018.Revision 0. Siemens. February 2012. (E)

1.3.7.3. NCSS reliability

[Ref-1] Non-Computerised Safety System – Basis Of Safety Case. PTL-F DC 5 Revision A. AREVA. August 2012. (E)

[Ref-2] Justification of Platform Reliability and Response Time on a Typical Automatic Function. TA-2082935 Revision B. AREVA TA. July 2012. (E)

1.4. PRIORITY AND ACTUATION CONTROL (PACS)

[Ref-1] Interfaces entre systèmes de contrôle commande et cellules actionneurs HTA et BT. ECEMA071141 Revision A. EDF. November 2007.
Note: this document is in French and is provided for information only.

[Ref-2] Schémas type (relais) des cellules de tableaux 10kV de la distribution électrique de la tranche EPR FA3. ECEMA080091 Revision A. EDF. October 2008.
Note: this document is in French and is provided for information only.

1.4.3. Design Basis

1.4.3.1. Diversity Requirements

[Ref-1] Diversity criteria definition for Priority Actuation Control (PAC) module. ECECC120443 Revision B. EDF. August 2012. (E)

[Ref-2] EPR UK – Diversity implementation plan for PAC modules. ECESN120472 Revision A. EDF. July 2012. (E)

1.4.5. Power supply

[Ref-1] Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. AFCEN Edition. December 2005. (E)

1.5. OPERATING MODES

1.5.1. Normal operation

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

[Ref-2] E. Marotte. KC. Plant System File - Level 1 Instrumentation and Control Equipment Document Part 1 - DSE History. ECECC070931 Revision B1. EDF. September 2009. (E)

[Ref-3] E. Marotte, G. Saoutieff. KC. Plant System File - Part 2: KC. System operation. ECECC070539 Revision B1. EDF. September 2009. (E)

[Ref-4] E. Marotte, G. Saoutieff. KC. Plant System File – Part 3: Design KC. System. ECECC070902 Revision B1. EDF. September 2009. (E)

[Ref-5] E. Marotte, G. Saoutieff. KC. Plant System File – Part 4: KC. System Mechanical Diagrams. ECECC070935 Revision B1. EDF. September 2009. (E)

[Ref-6] E.Marotte, G. Saoutieff. KC. Plant System File - Part 5: KC. System I&C. ECECC070903 Revision B1. EDF. September 2009. (E)

1.5.3. Internal hazards

[Ref-1] Class 1 control and display facilities in the Main Control Room and the Remote Shutdown Station. ECECC111829 Revision B. EDF. August 2012. (E)

2. EQUIPMENT ARRANGEMENT

2.1. ENVIRONMENTAL CONDITIONS

[Ref-1] D. Soaret. EMC (immunity) standards and requirements to be specified for electrical equipment. ENSECC090082 Revision A1. EDF. June 2009. (E)

ENSECC090082 Revision A1 is the English translation of ENSECC060193 Revision A.

2.3. EQUIPMENT ARRANGEMENT AND LAYOUT

[Ref-1] ETC-F: EPR Technical Code for Fire protection. ENGSIN050312 Revision B. EDF. August 2007. (E)

[Ref-2] J. Ferrari. Habitability of the Main Control Room in the event of fire. ECEF051003 Revision A1. EDF. October 2008. (E)

3. QUALIFICATION PRINCIPLES FOR THE VARIOUS INSTRUMENTATION & CONTROL COMPONENTS AND SYSTEMS

3.6. SPECIFIC QUALIFICATION FOR I&C SYSTEMS

[Ref-1] Test specification for control equipment. BTR 80.C.012.EPRUK.00. Revision A. EDF (SEPTEN). July 2011. (E)

[Ref-2] System Qualification Program. NLF-F DC 14 Revision D. AREVA. March 2009. (E)

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