UK EPR	Title: PCSR – Sub-chapter 7.7 – I&C tools, development process and substantiation **UKEPR-0002-076 Issue 04**

Total number of pages: 56	Page No.: I / V
Chapter Pilot: B. WORINGER *Name/Initials* B Woringer *Date* *06-11-2012*	
Approved for EDF by: A. MARECHAL *Name/Initials* *Date* *06-11-2012*	Approved for AREVA by: G. CRAIG *Name/Initials* G Craig *Date* *06-11-2012*

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA information	14.01.08
01	Integration of technical and co-applicant comments	27.04.08
02	PCSR June 2009 update: - Clarification of text - References added	30.06.09
03	Consolidated Step 4 PCSR update: - Document title updated to Sub-chapter 7.7 - 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 - New section 3 "Substantiation approach for software based systems" added covering Production Excellence and Independent Confidence Building Measures, and including statistical testing (§3.1.2.3) Note: This document was previously Sub-chapter 7.6	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 - Clarification of text (introduction, §1, §1.1, §1.3, §1.4.1, §2.3, §2.4.1, §4) - Details of PSOT added (§1, §1.1, §1.4, §4.1.1.2, §4.1.2.2)	06.11.2012

Continued on next page

REVISION HISTORY (Cont'd)

Issue	Description	Date
04 cont'd	Consolidated PCSR update (cont'd): - New section 3 "UNICORN Platform" added covering development of UNICORN platform and NCSS system - Section 4 (previously section 3) on substantiation approach for software based systems rewritten to include further information on justification of computerised I&C platforms, smart devices and programmable complex electronic component	

This document has been prepared by or on behalf of AREVA NP and EDF SA in connection with their request for generic design assessment of the EPR^{TM} design by the UK nuclear regulatory authorities. This document is the property of AREVA NP and EDF SA.

Although due care has been taken in compiling the content of this document, neither AREVA NP, EDF SA nor any of their respective affiliates accept any reliability in respect to any errors, omissions or inaccuracies contained or referred to in it.

Trade Mark

EPR^{TM} is an AREVA Trade Mark.

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 7.7 - I&C TOOLS, DEVELOPMENT PROCESS AND SUBSTANTIATION

The TELEPERM XS and SPPA-T2000 platforms, assisted by their associated programming tools, form part of the Instrumentation and Control (I&C) architecture monitoring and controlling the UK EPR. They must comply with process, nuclear safety and operational requirements. The tools are used in all phases of the overall safety life cycle where benefit to the assurance of quality and to the reliability of the safety-classified functions can be achieved.

The UNICORN platform is used for the Non-Computerised Safety System (NCSS). Its development process must also comply with appropriate nuclear safety standards.

This sub-chapter describes the development process and the tools used for programming the two computerised I&C platforms, TELEPERM XS for the Reactor Protection System (RPR [PS]), Reactor Control, Surveillance and Limitation system (RCSL) and Severe Accident I&C (SA I&C) and SPPA-T2000 for the Safety Automation System (SAS), Process Automation System (PAS), RRC-B SAS and Process Information and Control System (MCP [PICS]). Also described is the UNICORN development process and approach to substantiation of the two computerised I&C platforms, smart devices and programmable complex electronic components. The sub-chapter is organised as follows:

- section 1 describes the tools and development process used for the TELEPERM XS;
- section 2 describes the tools and development process used for the SPPA-T2000;
- section 3 describes the tools and development process used for UNICORN;
- section 4 describes the substantiation approach adopted for the TELEPERM XS, SPPA-T2000, smart devices and programmable complex electronic components.

1. TELEPERM XS PLATFORM

This section describes the tools and development process used for I&C programming of the RPR [PS], the RCSL, the SA I&C and the PSOT (design and coding of the I&C application software).

The RPR [PS], RCSL and SA I&C are based on TELEPERM XS technology. The engineering tools used for the RCSL and SA I&C development are the same as those used for the RPR [PS]. Therefore, although the RCSL is Class 2 and the SA I&C is Class 3, they benefit from the RPR [PS] (Class 1) requirements for the engineering tools. The software of the Rod Position Instrumentation (RPI) is included in the same TELEPERM XS database as the RPR [PS] and, as such, the tools and development processes are the same.

The PSOT is based on the Qualified Display System (QDS) platform, which although it is considered part of the TELEPERM XS product, has specific engineering tools.

The development process described in this sub-chapter starts after the functional requirements have been defined.

Note: Further details may be found in the documentation for the TELEPERM XS platform and associated engineering tool set [Ref-1] to [Ref-9].

1.1. OVERVIEW

The functionality of an I&C system using the TELEPERM XS platform is largely determined by computer software. A formalised procedure is implemented for application software development from start to finish, and for maintenance and future modifications. The TELEPERM XS platform is designed to protect the system against access to the configuration of software and hardware [Ref-1]. In addition to features provided by the I&C equipment for systems important to safety, administrative procedures will be put in place to control software and hardware configuration changes. These will be set out in the documentation and procedures supporting the site specific Nuclear Site Licence.

For software tasks, a distinction is made between:

- On-line software – this software is executed by the processing modules of the TELEPERM XS and implements I&C functions, as well as communication, self-tests, self-monitoring and service functions.
- Tool software – for engineering, configuration, test and maintenance. Tool software is executed by engineering, operation and maintenance computers independently of plant operation and does not itself directly contribute to the performance of the I&C Functions.

The on-line software comprises of the TELEPERM XS system software, developed and qualified independently from a specific I&C project, and the application software, produced by means of project-specific engineering with the aid of tools.

The TELEPERM XS platform encompasses the tools used for engineering of TELEPERM XS digital safety I&C. TELEPERM XS application software is mainly designed using the SPACE engineering system (SPecification And Coding Environment) and the QDS application software is designed using the QDS Design Tool. Engineering in this context refers to the overall process of producing and testing the I&C software:

- specification of I&C functions and hardware topology;
- verification of the specification (function diagrams and hardware diagrams);
- automatic code generation and compilation for simulation environment;
- validation of I&C functions in a simulation environment;
- automatic code generation and compilation for the target system;
- loading the software into the target system;
- testing the I&C functions on the target system.

The I&C engineering activities are planned, executed and documented according to the specific requirements described in Sub-chapter 7.1.

1.2. RELIABILITY REQUIREMENTS

The process of the application software development and the design and construction quality of the tools used for that process must be commensurate with the availability and reliability of the target system.

In order to provide a high level of reliability, correctness of the information contained in the database and correctness of results generated from the database, tools that are developed and / or maintained by the supplier will comply with Quality Assurance Plans [Ref-1].

The tools that are not developed and maintained by the supplier are subject to selection processes and criteria that aim to ensure their reliability and the correctness of their outputs.

1.3. FUNCTIONAL REQUIREMENTS

The process based requirements for the I&C Functions (functional requirements) are established by process engineers. The functional requirements constitute the main input for the RPR [PS], RCSL and SA I&C design and are used during the verification and validation steps to prove the conformance of the application software with these requirements.

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

1.4. DESIGN AND CODING

The SPACE system is based on a central database, which can be accessed with the aid of the various SPACE tools.

The SPACE editor supports specification of both the architecture (hardware topology) and the I&C Functions application software of the system. The result is a specification of:

- the I&C Functions (software specification) in the form of function diagrams;
- the topology of the hardware (hardware specification) in the form of network diagrams specifying the positions of the modules within the cabinets and the topology of the networks.

The code is generated automatically by code generators. The automatic generation is based on the software design (see section 1.4.1 below) and on the hardware design (see section 1.4.2 below) [Ref-1].

The QDS Design Tool is the graphical tool used for designing the application images for systems implemented on the QDS platform. The tool includes the library of graphical objects implemented by QDS system software. It integrates the pre-compiled QDS System Software libraries, the QDS Configuration Files Generator (QCFG) and the GCC Compiler suite [Ref-2] [Ref-3] [Ref-4].

1.4.1. Software design

For the level 1 programmable electronic systems, a software engineering method is applied which avoids manual programming of specific application software. This method uses pre-existing and qualified software modules (function blocks) [Ref-1].

The engineering process using the SPACE editor is based on the graphical "interconnection" of function blocks to produce function diagrams. A graphical specification language is used.

This provides the following:

- use of a defined set of pre-qualified (project-independent) function blocks with accurately specified and tested functionality;
- specification of the required I&C functions by means of interconnection of these blocks (generation of function diagrams);
- project specific parameter settings of the function blocks.

A feature of the engineering system is the continuous monitoring of user input for conformity to the general engineering rules. In this context, the SPACE editor applies the following types of checks or constraints:

- On-line testing of conformity to the conventions of the selected identification system for diagrams, components and signals.
- For each type of document (function diagrams and network diagrams), only one specific set of available function blocks is provided.
- All block-specific parameter settings are standardised. This means that syntax checking rules are implemented in the block-specific parameter masks for the function blocks and value ranges are limited, or a list of all possible entry values is presented for selection.
- The connections of the inputs and outputs of function blocks are standardised. The on-line monitoring ensures that only inputs and outputs of the same type can be interconnected.
- Open connection ends are marked. Similarly, connections that cross pages or diagrams and which have not been terminated are also marked.

More complex consistency and integrity checks are provided as service functions of the SPACE test tools.

An analysis tool (CPU load) for estimating the load on TELEPERM XS processing modules supplies, among other things, the following information:

- code size and data size for each one of the up to two function diagram group modules per CPU (Central Processing Unit);
- code size and data size for the complete on-line software of the CPUs;
- estimated maximum execution duration of the cyclic task running I&C functions;

- the cycle time of the CPU.

In addition, an analysis tool (net load) gives an estimate of the load on the LAN (Local Area Network) communication links engineered in the TELEPERM XS I&C system comprising:

- a list of the engineered TELEPERM XS LANs with all communication interfaces;
- expected loading of each LAN as a percentage (%).

1.4.2. Hardware design

The same engineering system in conjunction with appropriate engineering methods is also used to specify the hardware system and to assign I&C functions (software) to the hardware [Ref-1].

This provides the following:

- use of a defined set of standardised (non-project-specific) hardware modules that represent the TELEPERM XS hardware components;
- interconnection of these modules to form a hardware topology (generation of network diagrams);
- assignment of the I&C functions to the system hardware (linking of function diagrams with processor units);
- signal assignment for the input/output modules (definition of channel assignment for input/output modules).

A feature of the engineering system is the continuous monitoring of user input for conformity to the general engineering rules. In this context, the SPACE editor applies the following types of checks or constraints:

- On-line testing of conformity with the conventions of the selected identification system for diagrams, components and signals.
- For the network diagrams only one specific set of available function blocks is provided.
- The connections of the inputs and outputs of function blocks are standardised. The on-line monitoring ensures that only inputs and outputs of the same type can be interconnected.
- Open connection ends are marked. Similarly, connections that cross pages and which have not been terminated are also marked.

More complex consistency and integrity checks are provided as service functions of the SPACE test tools.

Load analysis of hardware components are performed on the basis of:

- the programming structure of the system software and the automatically generated application software source code;
- the datasheets of the implemented hardware components.

1.4.3. Configuration management of the engineering data

Configuration management is performed at the level of complete databases. Each database always contains only one updated version (with a unique identifier) of the project. Different update versions can be saved / archived or restored by saving the project database on hard disk or an external storage medium and by reading the saved copies back into "empty" project databases.

Each project database in the SPACE engineering system is provided with unique identification indicating the updated version of the stored project. The following individual components are identified:

- version and revision status of the definition data used (templates and symbols);
- date and time of the last modification of each diagram and name of the authors;
- date and time of the last modification of all blocks used in diagrams, the entered block parameters, connections, signals crossing diagrams;
- the data stored in the database during the code generation (these are automatically marked with version and modification/generation date).

Identification of the user (password protected) is by means of login and password protection in the operating system of the engineering computer.

The user can fill in a modification history in the labelling area of each diagram, consisting of the following:

- modification index;
- subject;
- name;
- date.

In each case, previous entries are stored in the modification history and displayed.

1.5. INTEGRATION, INSTALLATION AND COMMISSIONING

1.5.1. Integration

During system integration, verified hardware and software components are combined and configured in a specified way. The correct performance of the system functions is verified by tests. Tests of the integrated application functions in their dedicated hardware environment contribute to the system validation (see section 1.6.2 of this sub-chapter).

Typical tests performed off-site (in the factory or in a test bay) are as follows:

- integration tests and validation tests for each TELEPERM XS I&C system [Ref-1];
- interconnection tests between TELEPERM XS I&C systems.

Level 0 equipment will not be available for the system integration tests and validation tests. Appropriate devices for the simulation of input/output signals (from plant process simulators, if necessary) are used to allow a complete test of the systems off-site.

1.5.2. Installation

Before the integration and commissioning phase, each I&C system will be installed in accordance with an installation plan, describing in particular:

- the procedures for installation (i.e. the sequence in which the various systems and equipment are to be installed);
- the criteria for declaring termination of the installation phases.

The installation is comprised of the following activities:

- on-site installation of each I&C system in a defined order:
  - erection of the equipment in accordance with the installation plan;
  - interconnection with other systems and / or with plant components (wiring and/or cabling);
  - verification of the grounding concept;
  - verification of the above installation activities.

1.5.3. Commissioning

Each function is taken into account in an overall commissioning plan, describing, in particular:

- the relationship between the different commissioning steps;
- the commissioning procedures.

The commissioning is comprised of the following activities:

- commissioning of each I&C system without the plant process:
  - connection with power supply;
  - set-up and test of system equipment;
  - set-up and test of interconnections with other systems (including the links performed by networks and the hardwired input/output verification).
- commissioning of I&C systems connected to the plant process:
  - set-up and test of process-based parameters (e.g. closed loop controls), which must be tuned and/or verified with the plant process;
  - test of particular functions together with plant components;

- o tests required for validation.

The integration, installation and commissioning activities utilise the central data management concept. The design data can be accessed with the same tools as used for the design process. Automatic routines verify and document the actual configuration i.e. consistency, used versions, verification and release status. Effective tools for linking and loading of the software, for debugging and diagnostics are used.

1.6. VERIFICATION AND VALIDATION

Verification and validation (V&V) activities for the particular I&C systems are planned, performed and documented in accordance with the safety requirements associated with the I&C systems and equipment classification and take into account the applied engineering procedures such as a Software V&V Plan [Ref-1] [Ref-2] and tools.

The following paragraphs describe the verification and validation concept for the Class 1 RPR [PS] [Ref-3]. The V&V of the RCSL and the SA I&C is appropriately graded in relation to the class of those systems.

1.6.1. Verification

A design verification strategy is applied utilising the software engineering method (see section 1.4.1 of this sub-chapter), the central data management and consistent documentation concept for all the design specification data (see section 1.4.3 of this sub-chapter).

The software is built from pre-existing modules. Before starting the application specific engineering process, the software modules and the associated tools are provided in a validated state. No further verification of the software modules or of the code structure is undertaken.

The verification is focused on the application-specific configuration of the pre-existing hardware and software components. The application-specific design procedure is undertaken in part by I&C design tools with a graphical user interface and integrated verification routines. Potential error sources are mitigated by:

- effective data input checks;
- checks of consistency, completeness and conformance with formal rules and conventions;
- checks of hardware performance [Ref-1].

The main human verification effort is concentrated on the verification that the functional requirements have been adequately translated into the I&C design. This verification is performed as follows:

- verification of I&C design documents:

  The designed application functions are consistently and completely described by graphical means (e.g. functional diagrams) which provide a format that is comprehensible to I&C and process engineers. The functional requirements and the I&C functional specification are documented in a uniform and consistent way (see section 1.3 of this sub-chapter).

The verification of the software application design is performed either by human verification (e.g. of functional diagrams), or by automatic verification (e.g. on the content of the database of the project).

1.6.2. Validation

Validation demonstrates that the RPR [PS], RCSL and SA I&C systems fulfil their functional requirements.

Validation is divided into the following steps [Ref-1]:

- software validation test:

The correct application software design is proved by software validation tests (before the system validation). The first part of the software validation testing is performed with an engineering simulator tool (SIVAT – SImulator based VAlidation Tool) and the second part on the integrated system. Tests and test procedures are designed for each environment, in order to obtain complete coverage of the software being tested.

For the TELEPERM XS based systems, the engineering tool SIVAT is used to generate a simulation environment from the project database. This simulator program allows the user to test the dynamic response of the engineered functions by specifying values or ramps for input signals and then monitoring the system response and output signals, with signal profiles and internal states recorded during this process.

- integrated system validation:

Validation (off-site) of the properties of the integrated system, which can be tested without interaction with other systems, and the plant process.

- interconnected TELEPERM XS systems validation:

Validation (off-site) of the properties of the interconnected systems, which can be tested without interaction with the plant process.

- overall validation:

Validation (on-site) of the installed and electrically commissioned I&C systems connected to the plant process. Complete process functions (I&C and mechanical systems) are validated during commissioning.

The test effort for the integrated system can be reduced by taking credit for the preceding separate tests of the application software.

An effective test environment for the integrated system, including the option to link the system to a plant process simulator, is provided (see section 1.6.1 above).

1.7. OPERATION, MAINTENANCE AND MODIFICATION

The availability of complete and consistent I&C documentation that represents the actual status of the I&C systems and equipment is essential for I&C operation, maintenance and modifications. This section describes how the tool set may be used to support these activities and outlines some of the potential uses of documentation and data made available by the tool set.

The applied design methods allow the central management of all the necessary data describing both the hardware configuration and the implemented application functions.

These data are accessed (if necessary in combination with on-line I&C status information) for:

- on-line inspection of the I&C documentation or generation of consistent paper documentation;
- supervision and diagnosis;
- tests;
- modifications.

Modifications are made on a copy of the original release database. The modifications are marked for indication in the copy for testing and approval. Code generated from this database copy will be loaded into the processing modules of the target system only if the modifications have been approved. The database copy replaces the original at this point and becomes the new version of the approved project database. The new version must also be used by the TELEPERM XS service unit.

2. SPPA-T2000 PLATFORM

This section describes the tools and development process used for the Safety Automation System (SAS), Process Automation System (PAS), RRC-B SAS (level 1 automation data) and Process Information and Control System (MCP [PICS]) HMI I&C programming. The tools support both programming design and coding. The resulting sets of application data plus the hardware configuration constitute the I&C application software for the I&C system.

Note: Further details may be found in the documentation for the SPPA-T2000 platform and associated tool set [Ref-1] to [Ref-7].

The development process described in this sub-chapter starts after the functional requirements have been defined.

2.1. OVERVIEW

Integrated tools are used to provide uniform support for all I&C engineering activities, from design and implementation of the SAS, PAS, RRC-B SAS and MCP [PICS] to operation, maintenance and future modifications. Therefore, the tools cover the entire lifecycle of the SAS, PAS, RRC-B SAS and MCP [PICS]. Administrative procedures will be put in place to control software and hardware configuration changes. These will be set out in the documentation and procedures supporting the site specific Nuclear Site Licence.

The SAS, PAS, RRC-B SAS and MCP [PICS] are supported by a single integrated tool set that uses central data management which ensures that the data are captured only once. In the same way, the documentation is generated directly from the data acquisition. Almost all design data (hardware configuration and software specifications) are stored centrally in databases, which are accessed by appropriate tools for:

- management of the data during design and subsequent modifications;
- generation of I&C documentation;
- generation of code for the application software;
- support of I&C implementation (system integration, on-site installation and commissioning);
- support of verification and validation;
- test and diagnosis during I&C operation.

This data management concept provides a method for ensuring consistency between the different engineering stages and between the I&C implementation and the associated documentation.

The I&C engineering activities are planned, performed and documented taking into account the requirements specified in Sub-chapter 7.1.

2.2. RELIABILITY REQUIREMENTS

The process of development of the application software and the design and the construction quality of the Computer Aided Design (CAD) tools, e.g. a graphical programming tool, must be commensurate with the availability and reliability of the target system.

In order to provide a high level of reliability, the correctness of the outputs and the database, CAD tools that are developed and / or maintained by the supplier will comply with Quality Assurance Plans [Ref-1].

CAD tools that are not developed and maintained by the supplier are subject to selection processes and criteria that aim to ensure their reliability and the correctness of their outputs.

2.3. FUNCTIONAL REQUIREMENTS

The process-based requirements for I&C Functions (functional requirements) are defined by process engineers. The functional requirements (captured in functional diagrams and screen formats) constitute the main input for the SAS, PAS, RRC-B SAS and MCP [PICS] design and are used during the different verification and validation steps to prove compliance with these requirements.

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

2.4. DESIGN AND CODING

2.4.1. Software design and coding

For level 1 and 2 programmable electronic systems, a software engineering method is applied that avoids manual programming of specific application software. This method is based on the re-use of pre-existing or specifically developed and qualified software components [Ref-1]. For example, the software of the digital automation systems will be built from the following types of pre-existing software:

- operating system software which can be used in multiple processing units of the same type;
- components of the operating system software that must be configured according to the requirements of the application (e.g. to manage communication inside the distributed computer system);
- standardised function modules (libraries), which must be combined and configured to perform specific application functions.

By using standardised function modules, each having a clearly defined set of parameters depending on input/output characteristics, the software is completely and unambiguously designed by selecting the required function modules, setting their parameters and defining the connections between the modules and the external signals.

This design phase is performed using the tool Tec4Function, which provides a graphical representation of the software. The function-oriented graphical representation makes the design understandable for the I&C engineer (who can design the software without programming knowledge), the process engineer (who must verify the compliance with the functional requirements) and the user (who operates the I&C system).

For the HMI (MCP [PICS]), the screen formats are designed and coded with graphical tools OM-Editor and HTML-Editor which provide a standardised format and layout and uses standard, pre-existing software modules in the design and coding of the HMI software.

Operating methods include the use of screen formats without any link with the process; they provide on-line guidance on operating procedures. They are designed and coded using the HTML-Editor graphical tool, which provides a standardised format and layout, and uses standard, pre-existing software modules for the design and coding of the operating method.

This approach allows the I&C software design to be stored in a database. Thus the central data management concept for the entire I&C lifecycle, described in section 2.1 of this sub-chapter, is also followed for the software. This has several advantages:

- the consistency of I&C design data can be verified by programming tools;
- the documentation (e.g. implementation diagrams, screen formats) can be generated automatically thus ensuring consistency between the implemented software and the documentation.

Because the I&C design approach unambiguously defines the software, coding can be performed by an automatic tool that combines and configures the pre-existing software modules in the specified way.

The software I&C design tool is combined with a graphical hardware design tool for the digital I&C system. The associated hardware is designed by selecting and configuring standard equipment modules for processing, interfacing with process sensors and actuators, and for communicating between processing units and with peripheral devices. After software has been allocated to the processing units on which it is to be executed and the external functional diagram signals have been assigned to input/output devices, all necessary information is available to configure the application-dependent part of the operating system software. This is performed by an automatic tool.

The software design and coding approach provides a software engineering process which assists in avoiding error-prone conventional programming. For safety applications, this approach meets the requirements and offers the following capabilities:

- the development and verification of the application software benefit from the use of software modules and engineering tools which are validated in advance;
- the standardised function modules are small and simple, allowing extensive test coverage;
- the repeated usage of software modules in each application, together with a feedback process, leads to a greater awareness of any adverse experience. The representation of the software in an implementation diagram reduces errors during software design and enables verification of the compliance with the functional requirements;
- the automatic generation of software coding reduces the potential for errors.

2.4.2. Hardware design

The hardware design and configuration is based on standard catalogues for processing and communication equipment and for instrumentation and actuator set-ups and arrangements [Ref-1]. Tool support allows:

- hardware design in an appropriate, preferably graphical, format which is structured according to the design documentation required;
- central management of design data;
- generation of documentation.

The following hardware design activities for level 1 and 2 systems are supported by tools:

- choice of devices based on standard catalogues;
- interconnection between devices;
- arrangement in cabinets, racks;
- assignment of inputs from, and outputs to, level 0 equipment.

2.5. INTEGRATION, INSTALLATION AND COMMISSIONING

During system integration, verified hardware and software components are combined and configured as specified by the design. The correct operation of the system functions is verified by tests. Tests of the integrated application functions in their dedicated hardware environment contribute to the system validation (see section 2.6.2 of this sub-chapter).

The integration of level 1 and level 2 I&C systems is performed off-site (in the factory, on a test platform). Where testing requirements are specified, interconnected I&C systems can be integrated and tested in combination before their installation on-site.

Level 0 equipment is normally not available for system integration tests. To allow complete off-site system tests, input/output signal simulation devices can be used, where testing requirements are specified (including plant process simulators).

Installation and commissioning comprises the following activities:

- on-site installation of each I&C system in a predefined order;
- commissioning of each I&C system without connection to the plant process;
- commissioning of I&C systems connected to the plant process.

The integration, installation and commissioning activities all use the central data management concept. The design data can be accessed with the same tools used for the design process. Automatic routines verify and document the consistency, used versions, verification and release status of the current configuration. Tools are used for application software configuration management, code generation, software loading and diagnostics.

2.6. VERIFICATION AND VALIDATION

V&V activities for the I&C systems are planned, performed and documented in accordance with the safety requirements associated with the I&C systems and equipment classification and take into account the engineering procedures and tools applied.

The following sections describe the V&V concepts for the SAS, PAS, RRC-B SAS and MCP [PICS].

2.6.1. Verification

A design verification strategy is applied utilising the software engineering method (see section 2.4.1 of this sub-chapter), the central data management and consistent documentation concept for the design specification data (see section 2.1 of this sub-chapter).

The software is built from pre-existing modules. Before the start of the application specific engineering process, the software modules and the associated tools are provided in a validated state. No further verification of the software modules or of the code structure is undertaken.

Verification is based on the application-specific configuration of the pre-existing hardware and software components. The application-specific design process is undertaken using the I&C design tools utilising the graphical user interface and integrated verification routines. Potential error sources are mitigated by:

- effective data input checks;
- checks of consistency, completeness and conformance with formal rules and conventions;
- checks of hardware performance [Ref-1] [Ref-2].

The main human verification effort is concentrated on the verification that the functional requirements have been adequately translated into the I&C design. This verification is performed as follows:

- verification of I&C design documents:

  The application functions are consistently and completely described by graphical means (e.g. implementation diagrams), making them easy for I&C and process engineers to understand. Furthermore, functional requirements are documented in a uniform and consistent way (see section 2.3 of this sub-chapter). This provides the basis for consistent document verification.

2.6.2. Validation

Validation demonstrates that the SAS, PAS, RRC-B SAS and MCP [PICS], connected to other systems and to the plant process, fulfil their functional requirements.

Validation is divided into the following steps:

- systems validation:

  Validation (off-site) of the system properties of the interconnected systems that can be tested without interaction with the plant process. Complete I&C Functions which can be distributed over more than one I&C system are validated. In addition, process sensors and actuators can be simulated by test equipment connected to the I&C systems cabinets [Ref-1].

- overall validation:

  Validation (on-site) of the installed and electrically commissioned I&C systems connected to the plant process.

2.7. OPERATION, MAINTENANCE AND MODIFICATION

The availability of complete and consistent I&C documentation that represents the actual status of the I&C systems and equipment is essential for I&C operation, maintenance and modification.

The design methods applied allow the central management of all necessary data describing both the hardware configuration and the implemented application functions.

These data are accessible (if necessary in combination with acquired I&C status information) for:

- on-line inspection of the I&C documentation or the generation of consistent paper documentation;
- supervision and diagnosis;
- tests;
- modifications.

The modification of the I&C follows the same procedures using the same suite of tools as those used during the original I&C design and implementation, including the required verification and validation steps.

Applying the forward documentation principle, the modification starts with the modification of the I&C design data (using a copy of the currently valid database) to describe the resulting configuration of the modified I&C.

From this database the modified I&C and its documentation are generated in a consistent manner. The current database is replaced at the same time as the modified I&C is integrated into the plant.

3. UNICORN PLATFORM

The UNICORN platform is an I&C product, which is being developed within the frame of the UK EPR project. The primary purpose of the UNICORN platform is to provide the technology platform required to implement the Non-Computerised Safety System (NCSS). The NCSS has been introduced to meet the required overall reliability figures for I&C safety systems and to manage I&C processing in the event of total loss of computerised I&C. As such, the UNICORN platform is required to implement safety functions using non-computerised technology.

This section describes the development processes for both the UNICORN platform and the NCSS system. Additionally the engineering tools used to assist design activities are discussed.

3.1. UNICORN PLATFORM DEVELOPMENT

The UNICORN platform has been designed for the NCSS requirements for the UK EPR. It consists of:

- electronic modules for:
    - implementing safety functions, mostly based on magnetic dynamic logic and discrete components;
    - implementing monitoring or maintenance functions;
- other electronic modules (hardware + software for gateway and datalogger), which are used for communication purposes;
- cabinet / racks / wiring concept;
- engineering tools for designing a system using UNICORN and for simulating system functions;
- tools to perform commissioning, maintenance and periodic tests;
- tools used for modules development / automatic test of individual modules after manufacturing.

The following sections discuss the development process for the UNICORN platform along with the verification and validation activities.

3.1.1. Development process

The process for the full design of the UNICORN platform is defined in the platform quality plan [Ref-1] and aligns with appropriate IEC standards [Ref-2]. It is divided into the following four phases.

- platform basic design;
- platform detailed design and components manufacturing;

- platform qualification;
- representative platform related activities.

Each phase consists of a sequence of steps, and the decision to conclude each phase of the engineering process, and to initiate the next phase, is taken in phase reviews.

3.1.1.1. Platform basic design

Platform basic design consists of two main steps, a planning step and a platform specification step. The planning step primarily requires the production of the five main plans, which govern the engineering of the UNICORN platform:

- platform quality plan [Ref-1];
- platform configuration management plan;
- platform V&V and monitoring plan;
- platform qualification plan [Ref-2];
- platform security plan.

The platform specification step takes into account all platform design requirements [Ref-3] [Ref-4] [Ref-5] to produce a general platform specification [Ref-6], and specific module and tool specifications [Ref-7] [Ref-8] [Ref-9] [Ref-10].

Additionally, a preliminary justification is provided that the platform’s reliability and the response time for a typical automatic function implemented on the UNICORN platform can satisfy the requirements [Ref-11] [Ref-12].

3.1.1.2. Platform detailed design and components manufacturing

The detailed design phase covers the design, implementation and manufacture of the individual electronic modules, communication modules and tools. Detailed design reports are produced from the appropriate specifications.

3.1.1.3. Platform qualification

The qualification process follows the requirements of RCC-E, and the UNICORN platform will comply with appropriate IEC standards [Ref-1].

Testing and qualification activities are carried out on each of the electronic modules, communication modules and tools. Qualification tests prove functionality of the platform components under normal operation and extreme environmental conditions.

Test plans and qualification plans are produced for each module specifying the scope, approach, resources, and schedule of the testing/qualification activities for the module. It identifies the items to be tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the associated risks. It also specifies details of the tests to be performed and includes the test design, as well as the test procedures and test cases.

Test reports and qualification reports then record the results of the tests/qualification performed on each module, and provide an analysis of these results. For each test, the report indicates whether the test is successful, and, if not, it lists the revealed anomalies.

Test plans and reports are also produced for tools.

3.1.1.4. Representative platform related activities

This phase is the last phase of the platform development cycle covering platform integration and qualification. Platform integration deals with basic tests performed on the assembled cabinets and is concluded with the factory acceptance report.

Platform qualification covers the functional testing against the platform specification along with EMC and mechanical qualification.

3.1.2. Verification and validation

Verification and validation activities are to be set out in the UNICORN platform V&V plan and will include:

- electronic modules validation tests;
- communication modules validation tests;
- validation tests of tools;
- validation tests of datalogger and gateway software.

Independence is provided between the design team and the V&V team as required by IEC 61513. Personnel performing verification and validation activities must be not involved in the design of the system, and vice versa.

The electronic modules of the UNICORN platform which are used to implement the safety functions are non-computerised. However, some of the communication modules, the datalogger and gateway, contain software to allow communication to computerised systems. These software components shall be substantiated using the production excellence and independent confidence building measure approach used for software based systems as discussed in section 4 [Ref-1].

3.2. NCSS SYSTEM DEVELOPMENT

3.2.1. Development process

The development of the NCSS system from the specification to validated system is based upon the five phases of the system safety life cycle as defined by IEC 61513:

- specification requirements;
- specification;
- detail design and implementation;

- integration;
- validation.

A phase review is organised at the end of each phase to decide if next phase can be initiated.

3.2.1.1. Specification requirements

Initially a high level description of the system requirements is produced, independent of the decision to adopt any specific technical solution. These include requirements on:

- functions of the system [Ref-1];
- constraints of the design of the system [Ref-2] [Ref-3];
- boundaries and interfaces with other systems;
- interfaces with the users;
- environmental conditions of the system;
- qualification required.

The quality plan [Ref-4] sets out the lifecycle and management activities of the system development.

3.2.1.2. Specification

The specification phase includes the production of the verification and validation plan [Ref-1], qualification plan and security plan.

The design of the system is realised and outlined in the system specification [Ref-2] which aims to:

- identify pre-existing components to be used to implement part or the whole of the system;
- partition the system into a number of interconnected components which provide the required redundancy and reconfiguration capability;
- assign input signals to functions;
- assign voting process, priority handling, equipment protection functions;
- assign links of output control actions to actuators.

3.2.1.3. Detail design and implementation

The detailed design of the system includes detailing all hardware components of the system and their interfaces. Failure mode and effect analysis is performed along with response time and accuracy analysis.

3.2.1.4. Integration

The integration phase focuses upon testing the integrated hardware components of the system. Test specifications for the integrated system are produced along with appropriate reports indicating the success of the tests.

3.2.1.5. Validation

The validation phase ensures appropriate testing of the integrated system to ensure compliance with functional, performance and interface specifications.

3.2.2. Verification and validation

Verification and validation activities are set out in the V&V plan [Ref-1]. Verification activities are planned throughout the first four phases of the development process, with validation activities focusing on the final phase.

Independence is provided between the design team and the V&V team as required by IEC 61513. Personnel performing verification and validation activities must be not involved in the design of the system, and vice versa.

3.2.2.1. Verification

During the specification requirements phase, the objective of the verification activity is to ensure that the system requirements specification is complete and consistent with the stakeholders needs. Checks are made that:

- the requirements are traceable and consistent with the requirements for the system established in the architectural design and functional assignment of the overall I&C;
- interface requirements are consistent with those of the interfacing systems and equipment;
- requirements that unnecessarily increase the complexity of the system are identified.

Verification activities in the specification phase ensure that the system design is complete and consistent with the specification requirements.

The detailed design and implementation verification includes several specific analyses including:

- failure modes and effects analysis;
- assessment of system suitability;
- consistency check on periodic testing;
- verification of system security;
- analysis of response time and accuracy.

The V&V team are also responsible for preparation of the level test specification, the goal of this is to specify, for each test level, test cases and test procedures to apply for test execution.

3.2.2.2. Validation

The system validation concerns the test of the real system. It is performed during the last phase of the engineering life cycle with the objective of ensuring that the system is consistent with the system requirements specification.

3.2.3. Installation, operation and maintenance

The NCSS will be installed in accordance with an installation plan describing:

- procedural and technical measures for installation of the system on site;
- procedural and technical measures to check and provide assurance that the system is ready for operational use;

An operation plan will be provided which addresses the way the system is to be operated and the requirements applicable during system operation.

A maintenance plan will include procedural and technical measures to be taken to maintain the functionality of the operational system.

3.3. ENGINEERING TOOLS

Two engineering tools are provided to assist with UNICORN system design activities.

- UNICORN Design Tool (UDT) is a Computer-Aided Design tool similar to or based on the schematic software MS Visio.
- Valid_UDT tool is based on a simulator called ALICES, which models the UDT blocks, performing the simulation, to create and to play the verification scenarios. All elements from the UDT Library have a software model, which can be executed in this simulator. A parser is able to automatically translate the drawings produced using UDT into executable software.

The adequacy of these tools will be ensured as part of the platform qualification [Ref-1].

During the specification phase, the architecture is defined and a hardware requirements specification (HRS) is produced with UDT. This aims at defining an I&C system from a functional approach. It enables representation of the I&C system from the data acquisition to the actuators and the required functional blocks for the realisation of a function.

These diagrams are then verified using Valid_UDT. This tool enables the user to create and execute scenarios to describe event sequences and to ensure the compliance of the results with the system requirements specification.

During the detail design and implementation phase, the hardware design description is produced. It provides the detailed design of the system using UDT. It consists of detailed diagrams, which contain all the required physical elements for the execution of the functions of the system. This approach enables the allocation of the electronic modules and their functions, the positioning of various elements (electronic modules, fans, etc) in the cabinets, the wiring of the cabinets and definition of the interfaces with the others systems.

These diagrams are then verified by means of Valid_UDT.

To provide data for analysis, UDT also enables data extractions from the previous diagrams, which are used to:

- give the number of electronic modules;
- give the number of cabinets;
- make up a list of all connections between racks;
- make up a list of all connections between cabinets;
- give the constitution of all cabinets;
- configure the GATEWAY and the DATALOGGER.

Tools for module design/development, commissioning, maintenance and periodic tests will be developed and appropriately qualified prior to use.

4. SUBSTANTIATION APPROACH FOR SOFTWARE BASED SYSTEMS

The system reliability of the TELEPERM XS based systems, SPPA-T2000 based systems and smart devices is dependent upon the performance of computer software and related hardware. Substantiation will be established via compliance with appropriate standards and practices throughout the software development lifecycle, commensurate with the level of reliability required to meet the safety classification. The quality of the development process and the final product will be demonstrated via a process that involves production excellence activities and Independent Confidence Building Measures (ICBMs) [Ref-1] [Ref-2] [Ref-3] [Ref-4].

“Production excellence” requires a demonstration that appropriate standards, procedures and practices have been used in all aspects of production, from initial specification through to the commissioned system. This can be demonstrated via comprehensive testing, compliance with standards, including quality assurance standards, and application of consistent design principles to accepted standards from initial requirements to implementation.

ICBMs should provide confidence that the required functionality has been delivered to a required integrity level and is fit for purpose. This can be demonstrated via activities including external examinations of the development process, statistical testing, static analysis and failure modes and effects analyses depending on the nature and classification of the equipment being assessed. This evidence of challenges to the system lifecycle should have appropriate elements that are independent of the equipment supplier.

The approach described in the following sections applies to I&C systems using the TELEPERM XS and SPPA-T2000 platforms, to I&C equipment for smart devices and to programmable complex electronic components. A graded approach is adopted for the production excellence and ICBMs implemented in accordance with the class allocated to each I&C system or item of I&C equipment.

4.1. TELEPERM XS BASED SYSTEMS

The TELEPERM XS is a digital platform that provides reactor protection functions when used for the class 1 RPR [PS] and is also used for the class 2 RCSL and the class 3 SA I&C. Substantiation of reliability claims for the I&C systems implemented on the TELEPERM XS product uses the multi-legged safety case approach described above. Also refer to Sub-chapter 7.2, section 3 for qualification aspects.

4.1.1. Production excellence

The multi-legged procedure requires a demonstration of production excellence covering initial specification through to the finally commissioned system. This covers:

- thorough application of technical design practice consistent with current accepted standards for the development of software for computer based systems;
- implementation of an adequate quality assurance programme and plan in accordance with appropriate quality assurance standards;
- application of a comprehensive testing programme formulated to check every system function.

The standards include requirements for quality assurance and testing. The demonstration of compliance with standards includes coverage of appropriate quality assurance and testing activity.

For a specific sub-system, each software component may contain two sub items (system software and application software). For computer-based systems important to safety, production excellence applies to and must be demonstrated for both system software (including operating system) and application specific software.

4.1.1.1. TELEPERM XS platform

The TELEPERM XS platform, including the system software, is common to the RPR [PS], RSCL and SA I&C. Compliance with the standards applicable for class 1 equipment and a reliability claim of 10^{-4} pfy/pfd are considered for the TELEPERM XS product excluding QDS.

4.1.1.1.1. Standards compliance

Technical TELEPERM XS design practice is compliant with the requirements of nuclear sector standards appropriate to a class 1 system. The TELEPERM XS platform was specially developed to be used for class 1 safety I&C systems of nuclear power plants. Compliance of the hardware and system software with the quality and design requirements specified in the applicable international nuclear codes and standards will be demonstrated. These standards will include: IEC 61226, IEC 61513, IEC 60709, IEC 62340, IEC 60880, IEC 60780, IEC 62566, RCC-E Section B and IEC 60987 [Ref-1] [Ref-2] [Ref-3] [Ref-4].

4.1.1.1.2. Other specific measures

Other specific measures that contribute to “production excellence” are detailed below:

- **Simple design principles**

  Simple design principles have been implemented in the design of the TELEPERM XS platform. These principles include in particular the strictly cyclic operation of the software and the communication means, the absence of process-controlled interrupts, and the highly standardised, simple software structure, assured by automatic code generation [Ref-1].

- **Robust hardware components**

  The majority of the hardware components are series produced, service proven industrial components that are qualification tested for use in safety I&C systems. During the design of the components developed for TELEPERM XS, particular attention was focused on their structural simplicity and robustness [Ref-2] [Ref-3].

- **Reliable software**

  In addition to compliance with international nuclear codes and standards, in-house tests and trials were backed up by inspections at all stages of the development by independent external experts. The system software and the application-specific software are strictly separated. The project application-specific software is automatically generated from engineering diagrams (hardware architecture and function diagrams). This provides consistency between specification, documentation and application software.

- **Tool-supported engineering in all phases**

The engineering process is structured in phases with reliable and quality controlled tools supporting the related workflow. The phases comprise all steps in a project: requirements specification, configuration of the system architecture, design of interfaces to the plant and the I&C Functions, code generation with verification and validation, and finally the preparation of the installation and commissioning documents. The service proven simulation tool SIVAT makes it possible to test the application software at an early stage in the engineering process, independently of the availability of the target system hardware. The use of pre-validated application software significantly reduces efforts in the test field. The SIVAT tool has also been used to validate extensive modifications to installed systems. Experience shows that prior simulation with SIVAT reduces the need for modifications during the commissioning and trial operation to a minimum.

- **Independent assessment and licensing**

Independent assessment demonstrates that the hardware and software components of the TELEPERM XS platform meet the most stringent requirements of international nuclear codes and standards (IEC, IEEE, EPRI and KTA). They are thus suitable for all safety I&C tasks. Also, the generic properties of the system platform have been verified in a plant-independent system test performed with the participation of independent experts.

External assessment of the TELEPERM XS platform has been carried out by GRS (German Reactor Safety Association), ISTec (Institute for safety technology) and TUV (technical inspection agency). This focused on a generic qualification of the platform’s components, reusable software components and generic system functions [Ref-4] [Ref-5].

In May 2000, the U.S. Nuclear Regulatory Commission (NRC) issued the generic approval for the use of the TELEPERM XS platform in all safety applications, including protection systems.

4.1.1.2. RPR [PS], RCSL and SA I&C systems

The RPR [PS] will be developed in line with the requirements of nuclear sector standards applicable to a class 1 system. This will cover IEC 61226, IEC 61513, IEC 60709, IEC 62340, IEC 60880, IEC 60987, RCC-E section B and IEC 60780 and IEC 62566. PSOT is considered part of the RPR [PS] and will be developed in line with these standards [Ref-1] to [Ref-5].

The RCSL will be developed in line with the requirements of nuclear sector standards applicable to a class 2 system. This will cover IEC 61226, IEC 61513, IEC 60709, IEC 62138, IEC 60987 and RCC-E section B and IEC 60780 [Ref-1].

The SA I&C will be developed in line with the requirements of nuclear sector standards applicable to a class 3 system. This will cover IEC 61226, IEC 61513, IEC 60709, IEC 62138 and RCC-E section B and IEC 60780. The SA I&C will be developed in compliance with IEC 60987 hardware design requirements for computer based systems applicable to class 1 and class 2 hardware, since the same technology is to be used [Ref-1].

4.1.1.3. Compensating measures

If the assessment of production excellence identifies any gaps or weaknesses, compensating measures shall be identified and applied. Compensating measures cannot be specified in advance, as these activities are determined by the nature of the gaps identified in the production excellence. The activities could include commissioning tests, prior use, static analysis, dynamic analysis, statistical testing, review and audit of manufacturer's V&V, tool review, amongst others. Selection of compensating measures will take account of, and be diverse from, those measures selected as ICBMs.

4.1.2. Independent confidence building measures

Independent Confidence Building Measures provide an independent and thorough assessment of a safety system's fitness for purpose. This comprises the following elements:

a) Complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers, including:

  - independent product checking providing a searching analysis of the product;
  - independent checking of the design and production process, including activities needed to confirm the realisation of the design intention;

b) Independent assessment of the test programme, covering the full scope of test activities.

ICBMs will take account of, and be diverse from, any measures used as compensating measures for production excellence.

The following describes the ICBMs implemented for the TELEPERM XS platform (class 1), RPR [PS] (class 1), RCSL (class 2) and SA I&C (class 3) systems.

ICBM activities are carried out on the finally commissioned system, independently of the TELEPERM XS platform supplier, designer and manufacturer by suitably qualified individuals and organisations.

4.1.2.1. TELEPERM XS platform ICBMs

The following ICBM activities have been identified as appropriate for a class 1 system with a reliability claim of 10^{-4} fpd/fpy [Ref-1] and will be carried out on the TELEPERM XS platform [Ref-2]:

- independent review of type test;
- independent reviews of quality plan;
- independent reviews of product development process;
- independent assessment of the test programme;
- independent tool review;
- independent review of tool-assisted dynamic analysis of the code;

- independent desktop review and tool-assisted static analysis;
- compiler validation.

A description and scope of the static analysis and compiler validation ICBMs is provided in the RPR [PS] ICBM section.

4.1.2.2. RPR [PS] ICBMs

The following ICBM activities have been identified as appropriate for a class 1 system with a reliability claim of 10^{-4} fpd/fpy [Ref-1] and will be carried out on the RPR [PS] [Ref-2]:

- independent review of type test;
- independent reviews of quality plan;
- independent reviews of product development process;
- participation in reviews of application software development;
- witnessing of application software validation tests;
- independent inspections of the application software development quality;
- equipment manufacturing surveillance;
- commissioning tests on site;
- independent assessment of the test programme;
- independent tool review;
- independent review of tool-assisted dynamic analysis of the code;
- independent desktop review and tool-assisted static analysis;
- statistical testing;
- compiler validation.

The PSOT will also be subject to these ICBMs with the exceptions that statistical testing will not be carried out as it is not considered reasonably practical for a continuous HMI system, and due to the PSOT’s lower reliability claim of 10^{-3} fpd/fpy it is not considered necessary to perform compiler validation and the approach to static analysis will differ [Ref-3].

Independent review of tool-assisted dynamic analysis of the code

The system software and firmware will be subject to Modified Condition/Decision Coverage (MCDC) metrics to determine test coverage. An independent review shall be performed on the level of coverage achieved, the target being 100%. The review will be based upon IEC 60880 requirements [Ref-2].

The determination of test coverage for the application software will be based upon defining check-points for each functional block. An independent review shall be performed on the level of coverage achieved, the target being 100% [Ref-2].

Independent desktop review and tool-assisted static analysis

There is a scope and programme of work to address functional static analysis for the UK EPR Protection System using the MALPAS static analysis tool [Ref-4]. This is to include the following checks:

- MALPAS integrity checks for checking features of the programming language are used in a valid context;
- MALPAS semantic analysis for comparing the functionality of the software with the software specification to detect functional errors;
- MALPAS compliance analyser for generating proof obligations.

The scope covers both RPR [PS] application software and TELEPERM XS system software and firmware on both the RPR [PS] core and interface units.

Statistical testing

There is a statistical testing programme for the UK EPR Protection System (covering the Protection System Core as well as the Protection System Interface Units) [Ref-5]. It is proposed to run 50,000 tests on the final software release, which will provide a 99% confidence level that the reliability level of 10^{-4} pfd/pfy is met.

During the course of the development, typical fault transients and time delays in the RPR [PS] have been considered, a format has been established for a typical test case, the RPR [PS] logic has been reviewed, and permissive and reset requirements examined. Based on Sizewell B and recent statistical testing experience, the times required to develop and commission a Test System, develop the fault transient data and the RPR [PS] Test Division have been estimated. These inputs have led to the development of the proposed statistical testing programme.

Compiler validation

There is a scope and programme of work to address the validation of the compilation tools used to translate the source code into machine code in the UK EPR Protection System [Ref-4]. The scope covers both RPR [PS] application software and TELEPERM XS system software and firmware on the RPR [PS] core. The interface units, due to their lower reliability claim of 10^{-3} fpd/fpy, will only be part of the scope if it is considered reasonably practical to do so.

4.1.2.3. RCSL ICBMs

The following ICBM activities have been identified as appropriate for a class 2 system with a reliability claim of 10^{-2} fpd/fpy [Ref-1] and will be carried out on the RCSL [Ref-2]:

- independent review of type test;
- independent reviews of quality plan;
- independent reviews of product development process;

- participation in reviews of application software development;
- witnessing of application software validation tests;
- independent inspections of the application software development quality;
- equipment manufacturing surveillance;
- commissioning tests on site;
- independent assessment of the test programme;
- independent tool review;
- independent review including access to source.

Independent review including access to source

The RCSL application code will be checked to ensure that the code is fit for purpose. Sampling of the application code using the MALPAS tool will be performed with the aim of demonstrating that the RCSL application is of similar quality to the RPR [PS] application.

4.1.2.4. SA I&C ICBMs

The following ICBM activities will be carried out on SA I&C [Ref-1]. These activities are in excess of those required for a class 3 system with a reliability claim of 10^{-1} fpd/fpy [Ref-2] because of the same use of TXS technology as the higher classified RPR [PS] and RCSL:

- certification of compliance with quality standards;
- review of operational experience;
- commissioning tests on site;
- independent assessment of the test programme;
- independent review of type test;
- independent reviews of quality plan;
- independent reviews of product development process;
- participation in reviews of application software development;
- witnessing of application software validation tests;
- independent inspections of the application software development quality;
- equipment manufacturing surveillance;
- independent tool review.

4.1.2.5. Independence of ICBMs

Independence will be assured for all ICBM activities. The ICBM activities will be carried out by companies and individuals independent of the supplier, designer and manufacturer of the I&C systems.

Independent oversight of these activities will be carried out by, or on behalf of, the licensee organisation. The licensee is responsible for the design assurance carried out, through a design review and acceptance process. Design assurance activities will be carried out both on the main computer based equipment and system design by the supplier, and the ICBM reporting.

For all the ICBM activities, findings will be reviewed by a ‘sentencing board’. The ‘sentencing board’ will be responsible for the final evaluation of the impact of the findings, and for recommending how the findings will be addressed.

4.2. SPPA-T2000 BASED SYSTEMS

The SPPA-T2000 is a digital platform consisting of an automation part and an operation and monitoring system. The SAS, RRC-B SAS, PAS and MCP [PICS] use the SPPA-T2000 product.

This section describes the production excellence activities and ICBMs implemented for the SPPA-T2000 based systems.

4.2.1. Production excellence

The multi-legged procedure requires a demonstration of production excellence covering initial specification through to the finally commissioned system. This covers:

- thorough application of technical design practice consistent with current accepted standards for the development of software for computer based systems;
- implementation of an adequate quality assurance programme and plan in accordance with appropriate quality assurance standards;
- application of a comprehensive testing programme formulated to check every system function.

The standards include requirements for quality assurance and testing. The demonstration of compliance with standards includes coverage of appropriate quality assurance and testing activity.

For a specific sub-system, each software component may contain two sub items (system software and application software). For computer-based systems important to safety, production excellence applies to and must be demonstrated for both system software (including operating system) and application specific software.

4.2.1.1. SPPA-T2000 platform

The SPPA-T2000 platform is a combination of two parts, the automation part and the operation and monitoring system, and compliance with standards is based upon the highest classification of the system using the component. The automation part is common to the SAS, RRC-B SAS and PAS and therefore has must comply with class 2 standards with a reliability claim of 10^{-2} pfd/pfy. The operation and monitoring system is used by MCP [PICS] and, as such, must comply with class 3 standards with a reliability claim of 10^{-1} pfd/pfy.

4.2.1.1.1. Standards compliance

Technical SPPA-T2000 design practice for the automation part is compliant with the standards appropriate to class 2 I&C equipment with a reliability claim of 10^{-2} pfd/pfy. This includes IEC 61513, IEC 62138, IEC 60987, RCC-E Section B and IEC 60780 [Ref-1] [Ref-2].

Technical SPPA-T2000 design practice for the operation and monitoring system part is compliant with the standards appropriate to class 3 I&C equipment with a reliability claim of 10^{-1} pfd/pfy. This includes IEC 61513, IEC 62138, RCC-E Section B and IEC 60780 [Ref-1] [Ref-3].

4.2.1.2. SAS, RRC-B SAS, PAS and MCP [PICS]

The SAS will be developed in line with the requirements of nuclear sector standards applicable to a class 2 system. This will cover IEC 61226, IEC 61513, IEC 60709, IEC 62138, IEC 60987, RCC-E section B and IEC 60780 [Ref-1] [Ref-2].

The RRC-B SAS, PAS and MCP [PICS] will be developed in line with the requirements of nuclear sector standards applicable to a class 3 system. This will cover IEC 61226, IEC 61513, IEC 60709, IEC 62138, RCC-E section B and IEC 60780 [Ref-1].

4.2.1.3. Compensating measures

If the assessment of production excellence identifies any gaps or weaknesses, compensating measures shall be identified and applied. Compensating measures cannot be specified in advance as these activities are determined by the nature of the gaps identified in the production excellence. The activities could include commissioning tests, prior use, static analysis, dynamic analysis, statistical testing, review and audit of manufacturer’s V&V, tool review, amongst others. Selection of compensating measures will take account of, and be diverse from, those measures selected as ICBMs.

4.2.2. Independent confidence building measures

Independent Confidence Building Measures provide an independent and thorough assessment of a safety system’s fitness for purpose. This comprises the following elements:

a) Complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers, including:

- independent product checking providing a searching analysis of the product;

- independent checking of the design and production process, including activities needed to confirm the realisation of the design intention;

b) Independent assessment of the test programme, covering the full scope of test activities.

ICBMs will take account of, and be diverse from, any measures used as compensating measures for production excellence.

The following sections describe the ICBMs to be implemented on the SAS (class 2), RRC-B SAS (class 3), PAS (class 3) and MCP [PICS] (class 3).

ICBM activities are carried out on the finally commissioned system, independently of the SPPA-T2000 platform supplier, designer and manufacturer by suitably qualified individuals and organisations.

4.2.2.1. SAS ICBMs

The following ICBM activities have been identified as appropriate for a class 2 system with a reliability claim of 10^{-2} fpd/fpy [Ref-1] and will be carried out on the SAS [Ref-2]:

- independent review of type test;
- independent reviews of quality plan;
- independent reviews of product development process;
- participation in reviews of application software development;
- witnessing of application software validation tests;
- independent inspections of the application software development quality;
- equipment manufacturing surveillance;
- commissioning tests on site;
- independent assessment of the test programme;
- independent tool review;
- independent review including access to source.

Independent review including access to source

A full analysis of all SPPA-T2000 software is estimated as many tens of man years of effort, and in the context of a class 2, 10^{-2} fpd/fpy, system, is not considered reasonably practical. Instead, a limited software review will be performed with an additional dynamic testing ICBM applied.

The limited software review will be based on sampling some key software elements associated with the category A automatic protection functions. A functional analysis will be carried out to identify key parts of the system to consider in this review. Sample size will be limited to extent of reasonable practicability in the context of the complete proposal. A different approach to C code could be possible with sample integrity checking carried out, whereas the assembler language would consist of an ‘eyeball’ review.

The additional dynamic testing ICBM (using statistical testing principles) will require a representative SAS test platform to be available, targeting the category A automatic protection functionality. Five hundred independent tests based on representative plant transients will be developed for this testing. A dynamic test system will also be required to be developed, to test the representative SAS test platform, and to determine the correctness of the test results.

A feasibility study to look at how to achieve this testing will be carried out to consider the requirements, in particular, for the representative SAS test platform. This will consider modelling of inter-divisional communications and the cubicle allocation of the SAS category A automatic protection functions to decide whether testing only a subset of these is the best way to achieve a programme of dynamic testing (and limiting the extent of the test platform required). The aim of this study is to recommend a practical strategy for the dynamic testing.

The proposed testing will include tests of the system software and the application software.

4.2.2.2. RRC-B SAS and PAS ICBMs

The following ICBM activities will be carried out on RRC-B SAS and PAS [Ref-1]. These activities are in excess of those required for a class 3 system with a reliability claim of 10-^{1} fpd/fpy [Ref-2] because of the same use of SPPA-T2000 technology as the higher classified SAS.

- certification of compliance with quality standards;
- review of operational experience;
- commissioning tests on site;
- independent assessment of the test programme;
- independent review of type test;
- independent reviews of quality plan;
- independent reviews of product development process;
- participation in reviews of application software development;
- witnessing of application software validation tests;
- independent inspections of the application software development quality;
- equipment manufacturing surveillance.

4.2.2.3. MCP [PICS] ICBMs

The following ICBM activities have been identified as appropriate for a class 3 system with a reliability claim of 10^{-1} fpd/fpy [Ref-1] and will be carried out on the MCP [PICS] [Ref-2]:

- certification of compliance with quality standards;
- review of operational experience;

- commissioning tests on site;
- independent assessment of the test programme.

4.2.2.4. Independence of ICBMs

Independence will be assured for all of the ICBM activities. The ICBM activities will be carried out by companies and individuals independent of the supplier, designer and manufacturer of the I&C systems.

Independent oversight of these activities will be carried out by, or on behalf of, the licensee organisation. The licensee is responsible for the design assurance carried out, through a design review and acceptance process. Design assurance activities will be carried out both on the main computer based equipment and system design by the supplier, and the ICBM reporting.

For all the ICBM activities, findings will be reviewed by a ‘sentencing board’. The ‘sentencing board’ will be responsible for the final evaluation of the impact of the findings, and for recommending how the findings will be addressed.

4.3. SMART DEVICES

A smart device may be defined as an instrument, sensor or plant component (instrument, valve etc.) which contains built-in “intelligence” in the form of a microprocessor or complex electronic component (e.g. ASICs/FPGAs) to provide specialised capabilities enhancing the functionality of the device.

A feature of smart devices is that they are not programmed by the end user via a fully variable programming language such as C or other similar means. The end-user may be able to perform limited configuration of the device by selecting an option from a display panel or by typing in a set of numerical limits but cannot add new functionality and cannot modify the existing functionality in a fundamental way.

It should be noted that the use of a traditional device (i.e. one without embedded software) will take priority over the use of a smart device provided it performs the same required functionality and reliability.

The methodology used to qualify smart devices for nuclear safety applications is based upon a lifecycle approach. This lifecycle will be detailed in the smart device’s qualification plan and consists of the following steps [Ref-1]:

- definition of the requirements applicable to the smart device;
- assessment of the feasibility of the device qualification;
- characterisation of the smart device to be qualified;
- hardware qualification;
- software assessment;
- production of summary qualification documentation;
- production/update of the reference file;

- surveillance of manufacturing;
- assessment of impact of modifications (if applicable);
- periodic manufacturer follow-up.

The software assessment is primarily the step which differentiates the smart qualification approach from that of a traditional device.

The software used in smart devices may suffer from systematic design faults in the same way as software used in computer based systems important to safety. Smart devices require similar justifications and arguments to those presented for software used in computer based systems important to safety, i.e. demonstration of production excellence, including appropriate lifecycle, well-supported tools and thorough testing, and independent confidence-building measures that are sufficiently searching for the claimed integrity.

This section describes the software assessment step of the qualification lifecycle in terms of the production excellence activities and ICBMs implemented for smart devices. Smart devices may be required to be class 1, 2 or 3 depending upon the reliability claim made upon the safety function they support, as such the application of production excellence activities and ICBMs will be graded according to class.

4.3.1. Justification for class 1 smart devices

For class 1 smart devices used in the UK EPR, the limit on the reliability claim is 10^{-3} fpd/fpy and the requirements for production excellence and ICBMs are discussed below. Access to source code is required for class 1 smart devices due to the high reliability claim.

4.3.1.1. Production excellence

The basis of production excellence is demonstration of compliance with IEC standards, either the “IEC Nuclear safety standards” for devices designed originally to be used in nuclear safety applications or “IEC Industrial safety standard” for devices not specifically designed to be used in nuclear safety applications.

If the smart device is to be assessed against IEC Nuclear safety standards it will need to be compliant to class 1 for IEC 61513, IEC 60880, IEC 60987 and IEC 62566 [Ref-1].

If the smart device is to be assessed against IEC Industrial safety standards it will need to be compliant with IEC 61508:2010 SIL 3 [Ref-1]. The assessment of compliance with IEC 61508:2010 is performed using the EMPHASIS method [Ref-2].

4.3.1.2. Compensating measures

Where gaps are found in the argument of production excellence, additional compensating measures shall be identified and applied. Compensating measures cannot be specified in advance as these activities are determined by the nature of the gaps identified in the production excellence, however they shall be diverse from those measures selected as ICBMs.

4.3.1.3. Independent confidence building measures

The following ICBM activities have been identified as appropriate for class 1 smart devices [Ref-1]:

- commissioning tests to demonstrate that the device adequately performs its required functions;

- type test (audit the type test procedures and records when manufacturer performed type test or new tests if evidence of type testing is missing);

- examination, inspection, maintenance and testing (EIMT) arrangements or existing records if the device has been previously used within the licensee organisation;

- data on prior use, provided by the manufacturer and from previous use within the licensee organisation, the nuclear industry and other reputable sources (where available);

- evidence of the manufacturer's pedigree as a well-established producer with a track record of supplying good-quality instruments for safety applications in the nuclear and other sectors;

- Failure Modes and Effects Analysis (FMEA) of the hardware;

- independent desktop review and tool-assisted static analysis of the source code - including functional analysis;

- dynamic analysis of the source code (structural coverage) to justify that all statements and branches are fully covered by the tests performed.

This list of ICBMs is not exhaustive and is not intended to rule out the use of other appropriate techniques not mentioned here.

ICBMs will take account of, and be diverse from, any measures used as compensating measures for production excellence.

4.3.1.4. STT1 temperature transmitter (class 1 smart device)

The STT1 temperature transmitter is a smart device that is being qualified for use at class 1. The STT1 temperature transmitter scans inputs from thermocouples and resistance temperature detectors to provide a linearised analogue output signal to the TELEPERM XS systems.

The qualification approach is set out in the smart device's qualification plan [Ref-1]. Accordingly, a definition of requirements has been produced [Ref-2], along with a characterisation of the smart device to be qualified [Ref-3].

The production excellence leg of the software assessment has been performed against IEC 61508:2010 SIL 3 using the EMPHASIS method and the following ICBM activities performed [Ref-4]:

- type testing;

- operational experience;

- manufacturer’s pedigree;
- EIMT & commissioning tests;
- FMEA;
- code review;
- dynamic analysis.

The initial release of the summary qualification document [Ref-5] concludes that the STT1 temperature transmitter is likely to be appropriate for class 1 reliability, noting that assessment work is still in progress.

4.3.2. Justification for class 2 smart devices

4.3.2.1. Production excellence

If the smart device is to be assessed against IEC Nuclear safety standards it will need to be compliant to class 2 for IEC 61513, IEC 62138 and IEC 60987 [Ref-1].

If the smart device is to be assessed against IEC Industrial safety standards it will need to be compliant with IEC 61508:2010 SIL 2 [Ref-1]. The assessment of compliance with IEC 61508:2010 is performed using the EMPHASIS method [Ref-2].

4.3.2.2. Compensating measures

Where gaps are found in the argument of production excellence, additional compensating measures shall be identified and applied. Compensating measures cannot be specified in advance as these activities are determined by the nature of the gaps identified in the production excellence, however they shall be diverse from those measures selected as ICBMs.

4.3.2.3. Independent confidence building measures

The following ICBM activities have been identified as appropriate for class 2 smart devices [Ref-1]:

- commissioning tests to demonstrate that the device adequately performs its required functions;
- type test (audit the type test procedures and records when manufacturer performed type test or new tests if evidence of type testing is missing);
- examination, inspection, maintenance and testing (EIMT) arrangements or existing records if the device has been previously used within the licensee organisation;
- data on prior use, provided by the manufacturer and from previous use within the licensee organisation, the nuclear industry and other reputable sources (where available);

- evidence of the manufacturer's pedigree as a well-established producer with a track record of supplying good-quality instruments for safety applications in the nuclear and other sectors;
- Failure Modes and Effects Analysis (FMEA) of the hardware;
- an independent review including access to source. This could include a desktop review, integrity check or review of evidence for application tools by the supplier.

ICBMs will take account of, and be diverse from, any measures used as compensating measures for production excellence.

This list of ICBMs is not exhaustive and is not intended to rule out the use of other appropriate techniques not mentioned here.

Access to source code is preferred for class 2 smart devices, however due to its commercially sensitive nature it is not systematically required. Where there is exclusion of source code analysis, evidence must be provided that unsuccessful attempts were made to access the source code and that there are no other appropriate alternative smart devices exist which do allow access to the source code. In such cases, the independent review including access to source will be replaced with an alternative appropriate ICBM such as statistical testing.

4.3.2.4. Yokogawa DX1000 chart recorder (class 2 smart device)

The Yokogawa DX1000 chart recorder is a smart device that is being qualified for use at class 2. The Yokogawa DX1000 chart recorder is being proposed to be used to record various analogue values as a part of MCS [SICS] operations.

The qualification approach is set out in the smart device’s qualification plan [Ref-1]. Accordingly, a definition of requirements has been produced [Ref-2], along with a characterisation of the smart device to be qualified [Ref-3].

The production excellence leg of the software assessment has been performed against IEC 61508:2010 SIL 2 using the EMPHASIS method and the following ICBM activities performed [Ref-4]:

- type testing;
- RCC-E review;
- operational experience;
- manufacturer’s pedigree;
- EIMT and commissioning tests;
- code review;

The summary qualification document [Ref-5] concludes that the Yokogawa DX1000 chart recorder is likely to be appropriate for class 2 reliability, noting that some further assessment work is still required.

4.3.3. Justification for class 3 smart devices

4.3.3.1. Production excellence

If the smart device is to be assessed against IEC Nuclear safety standards it will need to be compliant to class 3 for IEC 61513 and IEC 62138 and class 2 for IEC 60987 [Ref-1].

If the smart device is to be assessed against IEC Industrial safety standards it will need to be compliant with IEC 61508:2010 SIL 1 [Ref-1]. The assessment of compliance with IEC 61508:2010 is performed using the EMPHASIS method [Ref-2].

4.3.3.2. Compensating measures

Where gaps are found in the argument of production excellence, additional compensating measures shall be identified and applied. Compensating measures cannot be specified in advance as these activities are determined by the nature of the gaps identified in the production excellence, however they shall be diverse from those measures selected as ICBMs.

4.3.3.3. Independent confidence building measures

The following ICBM activities have been identified as appropriate for class 3 smart devices [Ref-1]:

- commissioning tests to demonstrate that the device adequately performs its required functions;
- examination, inspection, maintenance and testing (EIMT) arrangements or existing records if the device has been previously used within the licensee organisation;
- data on prior use, provided by the manufacturer and from previous use within the licensee organisation, the nuclear industry and other reputable sources (where available);
- evidence of the manufacturer's pedigree as a well-established producer with a track record of supplying good-quality instruments for safety applications in the nuclear and other sectors. This list of techniques and measures is not exhaustive and is not intended to rule out the use of other techniques not mentioned here.

ICBMs will take account of, and be diverse from, any measures used as compensating measures for production excellence.

4.4. PROGRAMMABLE COMPLEX ELECTRONIC COMPONENTS

I&C equipment and systems important to safety can make use of Programmable Complex Electronic Components (PCECs) such as PLDs, FPGAs and ASICs. These programmable complex electronic components may suffer from systematic design faults in the same way as software and, as such, it is appropriate to make similar arguments as those presented for software, i.e. development excellence, including appropriate lifecycle, well-supported tools and thorough testing, plus independent confidence-building measures that are sufficiently searching for the claimed integrity.

4.4.1. Approach to justification of PCECs

For pre-developed equipment containing PCECs, justifications will be made for their adequacy. This could include:

- review of their development;
- review of their operating history;
- review of their test records;
- review of their fault records;
- assessment against standards;
- justification of any gaps.

For newly developed class 1 equipment, compliance is required with IEC 62566. For class 2 equipment, a comparison will be performed against IEC 62566 and gaps will be considered acceptable due to the reduced reliability claim where suitable justifications can be provided. It is noted that IEC 62566 has only recently been introduced and, as such, pre-developed equipment may not be fully compliant. Where this is the case, suitable justifications will be made.

4.4.2. PCECs in TELEPERM XS

PCECs used within TELEPERM XS equipment and systems must follow a set of design and coding guidelines. This ensures compliance with relevant standards.

PCECs developed for the TELEPERM XS platform prior to these guidelines were regarded as part of the hardware development and qualification process. Although no specific PCEC tests were performed, components type test would have revealed any errors in the simple programming of the PCEC connections. Furthermore, compliance analysis with the design and coding guidelines is being performed on all existing PCECs to produce all required documentation and ensure compliance. Any discrepancies will be examined.

4.4.3. PCECs in SPPA-T2000

For PCECs used within the SPPA-T2000 platform an approach is to be developed, which will be based on production excellence and ICBMs, and compliance with standards, and may be similar to the approach that is used for smart devices.

SUB-CHAPTER 7.7 – 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. TELEPERM XS PLATFORM

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

[Ref-2] TELEPERM XS – System Data. TXS-1008-76 V4.1. AREVA. January 2012. (E)

[Ref-3] TELEPERM XS – A Digital Reactor Protection System. EMF-2110(NP)(A) V1.0. AREVA. July 2000. (E)

[Ref-4] S Richter. Architecture of TXS Online Software. NGLT/2004/en/0023 Revision A. AREVA. October 2004. (E)

[Ref-5] Operation principles and safety features of the TXS system platform Release 3.5.x PTLD-G/2010/en/0355 Revision A. AREVA. December 2010. (E)

[Ref-6] J-U Wittig. TELEPERM XS Simulation - Concept of Validation and Verification. NGLP/2004/en/0094 Revision A. AREVA. July 2004. (E)

[Ref-7] A Lindner. Assessment of application of tools for TELEPERM XS. ISTec – A – 1085 Revision 0. ISTec. June 2006. (E)

[Ref-8] C Hessler. Overview of approach for TXS hardware qualification. NLTC-G/2007/en/0072 Revision A. AREVA. November 2007. (E)

[Ref-9] TXS Self-monitoring and Fail-safe behaviour from Core-Software Release 3.6.2. PTLC-G/2011/en/0059 Revision A. AREVA. January 2012. (E)

1.1. OVERVIEW

[Ref-1] Operation principles and safety features of the TXS system platform Release 3.5.x PTLD-G/2010/en/0355 Revision A. AREVA. December 2010. (E)

1.2. RELIABILITY REQUIREMENTS

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

1.3. FUNCTIONAL REQUIREMENTS

[Ref-1] IEC 61513 ed. 2001 §6.1.1 Mapping to FA3 PS documentation. AREVA. June 2012. (E)

1.4. DESIGN AND CODING

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

[Ref-2] Protection System Operator Terminal Basis of Safety Case. ECECC120489 Revision A. EDF. May 2012. (E)

[Ref-3] Design Principles for QDS Application. NLS-F DC 10145 Revision C. AREVA. May 2012. (E)

[Ref-4] QDS Design Tool Software User Manual. NFLS DC 215 Revision H. AREVA. October 2012. (E)

1.4.1. Software design

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

1.4.2. Hardware design

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

1.5. INTEGRATION, INSTALLATION AND COMMISSIONING

1.5.1. Integration

[Ref-1] TXS I&C Systems Verification and Validation Plan. PELV-F DC 28 Revision A. AREVA. June 2012. (E)

1.6. VERIFICATION AND VALIDATION

[Ref-1] R. Fehn. Phase Model for the Development of Software Components for TELEPERM XS, Engineering Procedure. FAW No. TXS-1.1en. Revision A. AREVA. October 2006. (E)

[Ref-2] Dr. B. Schnitzer. Software Verification and Validation Plan (V&V Plan), Engineering Procedure. FAW No.TXS-1.6en. Revision A. AREVA. March 2006. (E)

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

1.6.1. Verification

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

1.6.2. Validation

[Ref-1] TXS I&C Systems Verification and Validation Plan. PELV-F DC 28 Revision A. AREVA. June 2012. (E)

2. SPPA-T2000 PLATFORM

[Ref-1] Kristel. System specification file. SY710 Version 6.0. Siemens. March 2009. (E)

[Ref-2] Engineering tools detail specification. DE 410 Version 3.0. Siemens. November 2007. (E)

[Ref-3] Detail software specification - Engineering tools. DE 403 Version 9.0. Siemens. November 2008. (E)

[Ref-4] Test specification for control equipment. 80.C.012.EPRUK.00 Revision A. EDF. July 2011. (E)

[Ref-5] System Qualification Program. NLF-F DC 14 Revision D. AREVA. March 2009. (E)

[Ref-6] Basis of Safety Case of SPPA-T2000. PEL-F DC 13 Revision A. AREVA. June 2012. (E)

[Ref-7] Self test coverage analysis. QU003 Revision 0.1. Siemens. February 2012. (E)

2.2. RELIABILITY REQUIREMENTS

[Ref-1] Quality plan for engineering of FA3 standard I&C based on SPPA T2000. NLF-F DC 82 Revision C. AREVA. April 2008. (E)

2.3 FUNCTIONAL REQUIREMENTS

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

2.4. DESIGN AND CODING

2.4.1. Software design and coding

[Ref-1] Quality Plan for engineering of FA3 Standard I&C based on SPPA T2000. NLF-F DC 82 Revision C. AREVA. April 2008. (E)

2.4.2. Hardware design

[Ref-1] Quality Plan for engineering of FA3 Standard I&C based on SPPA T2000. NLF-F DC 82 Revision C. AREVA. April 2008. (E)

2.6. VERIFICATION AND VALIDATION

2.6.1. Verification

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

[Ref-2] Module dependability analysis for SPPA-T2000 (S7) AS620B/SPPA-T2000 - OM components/Safety parameter determination approach. QU019. Revision 0. Siemens. February 2012. (E)

2.6.2. Validation

[Ref-1] Application Software Test Program. NLF-F DC 89 Revision C. AREVA. December 2009. (E)

3. UNICORN PLATFORM

3.1. UNICORN PLATFORM DEVELOPMENT

3.1.1. Development process

[Ref-1] Platform Quality Plan. TA-2057230 Revision D. AREVA TA. June 2012. (E)

[Ref-2] Non-Computerised Safety System – Basis Of Safety Case. PTL-F DC 5 Revision A. AREVA. August 2012. (E)

3.1.1.1. Platform basic design

[Ref-1] Platform Quality Plan. TA-2057230 Revision D. AREVA TA. June 2012. (E)

[Ref-2] Platform Qualification Plan. TA-2073805 Revision D. AREVA TA. July 2012. (E)

[Ref-3] Requirements for Non-Computerized I&C Platform. PTI DC 2 Revision E. AREVA. April 2012. (E)

[Ref-4] Non Computerized Safety System - Diversity Criteria. PELL-F DC 11 Revision C. AREVA. August 2012. (E)

[Ref-5] NCSS Characterization for platform sizing evaluation. PTI DC 7 Revision B. AREVA. August 2012. (E)

[Ref-6] Platform Specification. TA-2060143 Revision C. AREVA TA. May 2012. (E)

[Ref-7] UNICORN project - Module Common Requirements Specification. TA-2084059 Revision A. AREVA TA. May 2012. (E)

[Ref-8] SCAT Module Specification NTA-228830. TA-2080785 Revision A. AREVA TA. May 2012. (E)

[Ref-9] VOPER Module Specification NTA-228831. TA-2080787 Revision A. AREVA TA. May 2012. (E)

[Ref-10] AVACT Module Specification NTA-228835. TA-2080788 Revision A. AREVA TA. June 2012. (E)

[Ref-11] Justification of Platform Reliability and Response Time on a Typical Automatic Function. TA-2082935 Revision B. AREVA TA. July 2012. (E)

[Ref-12] Justification of Reliability Allocation. TA-2096900 Revision A. AREVA TA. June 2012. (E)

3.1.1.3. Platform qualification

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

3.1.2. Verification and validation

[Ref-1] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

3.2. NCSS SYSTEM DEVELOPMENT

3.2.1. Development process

3.2.1.1. Specification requirements

[Ref-1] Functional Requirements on Non-Computerised Safety I&C Functions. NEPR-F DC 551 Revision C. AREVA. July 2012. (E)

[Ref-2] Non Computerized Safety System - Diversity Criteria. PELL-F DC 11 Revision C. AREVA. August 2012. (E)

[Ref-3] Safety Requirements for Non-Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

[Ref-4] NCSS Quality Plan. TA-2061589 Revision C. AREVA TA. July 2012. (E)

3.2.1.2. Specification

[Ref-1] NCSS System Verification and Validation Plan. TA-2065953 Revision C. AREVA. July 2012. (E)

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

3.2.2. Verification and validation

[Ref-1] NCSS System Verification and Validation Plan. TA-2065953 Revision C. AREVA. July 2012. (E)

3.3. ENGINEERING TOOLS

[Ref-1] Platform Quality Plan. TA-2057230 Revision D. AREVA TA. June 2012. (E)

4. SUBSTANTIATION APPROACH FOR SOFTWARE BASED SYSTEMS

[Ref-1] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

[Ref-2] Justification for Production Excellence and Independent Confidence Building Measures used for Teleperm XS Based Systems. ECECC111557 Revision B. EDF. July 2012. (E)

[Ref-3] UK EPR Protection System - Overall scope of Independent Confidence Building Measures. ENSECC110173 Revision B. EDF. June 2012. (E)

[Ref-4] UK EPR Computer Systems Safety Production Excellence Independent Confidence Building SPPA-T2000. ECECC120398 Revision B. EDF. August 2012. (E)

4.1. TELEPERM XS BASED SYSTEMS

4.1.1. Production excellence

4.1.1.1. TELEPERM XS platform

4.1.1.1.1. Standards compliance

[Ref-1] Justification for Production Excellence and Independent Confidence Building Measures used for Teleperm XS Based Systems. ECECC111557 Revision B. EDF. July 2012. (E)

[Ref-2] Compliance of the TXS system platform and development processes with IEC 61513. PTLC-G/2010/en/0047 Revision B. AREVA. June 2012. (E)

[Ref-3] TXS Platform: Compliance Analysis IEC 60880 ed 2.0.
PTLD-G/2010/en/0383 Revision A. AREVA. December 2011. (E)

[Ref-4] Compliance of the TXS Hardware design and Engineering process with IEC60987 Ed.2 – Platform Part. NLTC-G/2008/en/0053 Revision A. AREVA. July 2008. (E)

4.1.1.1.2. Other specific measures

[Ref-1] Dr. Heinz-Wilhelm Bock, W Dreves, S Richter. Operation Principles and Safety Features of the TELEPERM XS System Platform. NGLT/2003/en/0045 Revision D. AREVA. January 2004. (E)

[Ref-2] Field Failure Rate Calculation and Statistics of TELEPERM XS.
PTLD-G/2010/en/0191 Revision A. AREVA. July 2010. (E)

[Ref-3] 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-4] TXS Test Report Module Test: Runtime Environment 2.7.2. NLTD-G/2008/de/0152 Revision B. AREVA. November 2009. (De)

[Ref-5] Technical Report on the assessment of the plant independent system test of the digital safety instrumentation and control system TELEPERM XS. TXS-AUST-0599-02. ISTec GmbH and TÜV Nord. May 1999. (E)

4.1.1.2. RPR [PS], RCSL and SA I&C systems

[Ref-1] Justification for Production Excellence and Independent Confidence Building Measures used for Teleperm XS Based Systems. ECECC111557 Revision B. EDF. July 2012. (E)

[Ref-2] Protection System Operator Terminal Basis of Safety Case. ECECC120489 Revision A. EDF. May 2012. (E)

[Ref-3] TELEPERM XS I&C System Compliance Analysis with IEC 61513. PEL-F DC 8 Revision A. AREVA. June 2012. (E)

[Ref-4] TELEPERM XS I&C Systems Compliance Analysis with IEC 60880. PEL-F DC 9 Revision A. AREVA. June 2012. (E)

[Ref-5] TELEPERM XS I&C Systems Compliance Analysis with IEC 60987. PEL-F DC 10 Revision A. AREVA. June 2012. (E)

4.1.2. Independent confidence building measures

4.1.2.1. TELEPERM XS platform ICBMs

[Ref-1] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

[Ref-2] UK EPR Protection System - Overall scope of Independent Confidence Building Measures. ENSECC110173 Revision B. EDF. June 2012. (E)

4.1.2.2. RPR [PS] ICBMs

[Ref-1] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

[Ref-2] UK EPR Protection System - Overall scope of Independent Confidence Building Measures. ENSECC110173 Revision B. EDF. June 2012. (E)

[Ref-3] Protection System Operator Terminal Basis of Safety Case. ECECC120489 Revision A. EDF. May 2012. (E)

[Ref-4] UK EPR Protection System - Scope and programme of work to address functional static analysis and compiler validation. ENSECC110123 Revision B. EDF. June 2012. (E)

[Ref-5] UK EPR - Programme of statistical testing activities. ECECC111521 Revision B. EDF. June 2012. (E)

4.1.2.3. RCSL ICBMs

[Ref-1] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

[Ref-2] Justification for Production Excellence and Independent Confidence Building Measures used for Teleperm XS Based Systems. ECECC111557 Revision B. EDF. July 2012. (E)

4.1.2.4. SA I&C ICBMs

[Ref-1] Justification for Production Excellence and Independent Confidence Building Measures used for Teleperm XS Based Systems. ECECC111557 Revision B. EDF. July 2012. (E)

[Ref-2] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

4.2. SPPA-T2000 BASED SYSTEMS

4.2.1. Production excellence

4.2.1.1. SPPA-T2000 platform

4.2.1.1.1. Standards compliance

[Ref-1] UK EPR Computer Systems Safety Production Excellence Independent Confidence Building SPPA-T2000. ECECC120398 Revision B. EDF. August 2012. (E)

[Ref-2] SPPA-T2000 IEC 62138 Justification for AS620B. QU042 Revision 0.1 Siemens. April 2012. (E)

[Ref-3] SPPA-T2000 IEC justification for OM690. QU041 Revision 0.2. Siemens. April 2012. (E)

4.2.1.2. SAS, RRC-B SAS, PAS and MCP [PICS]

[Ref-1] UK EPR Computer Systems Safety Production Excellence Independent Confidence Building SPPA-T2000. ECECC120398 Revision B. EDF. August 2012. (E)

[Ref-2] IEC 61513 and 62138 justification for SAS. DN 2.2.24 Issue 3.0. Siemens. January 2010. (E)

4.2.2. Independent confidence building measures

4.2.2.1. SAS ICBMs

[Ref-1] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

[Ref-2] UK EPR Computer Systems Safety Production Excellence Independent Confidence Building SPPA-T2000. ECECC120398 Revision B. EDF. August 2012. (E)

4.2.2.2. RRC-B SAS and PAS ICBMs

[Ref-1] UK EPR Computer Systems Safety Production Excellence Independent Confidence Building SPPA-T2000. ECECC120398 Revision B. EDF. August 2012. (E)

[Ref-2] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

4.2.2.3. MCP [PICS] ICBMs

[Ref-1] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

[Ref-2] UK EPR Computer Systems Safety Production Excellence Independent Confidence Building SPPA-T2000. ECECC120398 Revision B. EDF. August 2012. (E)

4.3. SMART DEVICES

[Ref-1] Lifecycle approach to qualify Smart Devices used in nuclear safety applications. ENSECC110106 Revision B. EDF. March 2012. (E)

4.3.1. Justification for class 1 smart devices

4.3.1.1. Production excellence

[Ref-1] Justification of smart devices for nuclear safety applications. ENSECC110102 Revision B. EDF. May 2012. (E)

[Ref-2] EMPHASIS tool evaluation. ENSECC110110 Revision B. EDF. March 2012. (E)

4.3.1.3. Independent confidence building measures

[Ref-1] Justification of smart devices for nuclear safety applications. ENSECC110102 Revision B. EDF. May 2012. (E)

4.3.1.4. STT1 temperature transmitter (class 1 smart device)

[Ref-1] Assessment Plan for Class1 Smart Device Trial. ECECC121333 Revision A. EDF. August 2012. (E)

[Ref-2] Standard Temperature Transmitter - Requirements Identification File. ECECC121334 Revision A. EDF. July 2012. (E)

[Ref-3] Standard Temperature Transmitter - Equipment Identification File. ECECC121335 Revision A. EDF. July 2012. (E)

[Ref-4] Software Assessment Report for STT1 Temperature Transmitter. ECECC121336 Revision A. EDF. August 2012. (E)

[Ref-5] Summary Qualification Report for STT1 Temperature Transmitter. ECECC121337 Revision A. EDF. August 2012. (E)

4.3.2. Justification for class 2 smart devices

4.3.2.1. Production excellence

[Ref-1] Justification of smart devices for nuclear safety applications. ENSECC110102 Revision B. EDF. May 2012. (E)

[Ref-2] EMPHASIS tool evaluation. ENSECC110110 Revision B. EDF. March 2012. (E)

4.3.2.3. Independent confidence building measures

[Ref-1] Justification of smart devices for nuclear safety applications. ENSECC110102 Revision B. EDF. May 2012. (E)

4.3.2.4. Yokogawa DX1000 chart recorder (class 2 smart device)

[Ref-1] Qualification plan for Yokogawa DX1000. ECECC111779 Revision A. EDF. February 2012. (E)

[Ref-2] SICS chart recorder - Requirements Identification File. ECECC120095 Revision B. EDF. June 2012. (E)

[Ref-3] SICS chart recorder - Equipment Identification File. ECECC120096 Revision B. EDF. June 2012. (E)

[Ref-4] Report on software assessment of Yokogawa DX1000 series electronic chart recorders. ECECC121090 Revision A. EDF. June 2012. (E)

[Ref-5] Summary Qualification Report for Yokogawa DX1000. ECECC121091 Revision A. EDF. June 2012. (E)

4.3.3. Justification for class 3 smart devices

4.3.3.1. Production excellence

[Ref-1] Justification of smart devices for nuclear safety applications. ENSECC110102 Revision B. EDF. May 2012. (E)

[Ref-2] EMPHASIS tool evaluation. ENSECC110110 Revision B. EDF. March 2012. (E)

4.3.3.3. Independent confidence building measures

[Ref-1] Justification of smart devices for nuclear safety applications. ENSECC110102 Revision B. EDF. May 2012. (E)