UK EPR	Title: PCSR – Sub-chapter 7.1 – Design principles of the Instrumentation and Control systems
	UKEPR-0002-071 Issue 04

Total number of pages: 19	Page No.: I / III
Chapter Pilot: B. WORINGER *Name/Initials* B. Woringer *Date* *26-10-2012*	
Approved for EDF by: A. MARECHAL *Name/Initials* A.J.C. Maréchal *Date* *29-10-2012*	Approved for AREVA by: G. CRAIG *Name/Initials* G Craig *Date* *29-10-2012*

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA review	04.01.08
01	Integration of technical, co-applicant and INSA review comments	27.04.08
02	PCSR June 2009 update: - Clarification of text	26.06.09
03	Consolidated Step 4 PCSR update: - Minor editorial changes - Clarification of text - Update and addition of references - Update of Safety Function Categorisation and SCC Classification to clearly summarise Category A, B, C and Class 1, 2, 3 for I&C scope - Role of RRC-A in Defence in Depth Concept and associated allocation added (§2.4)	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 (introductory text, §0.1, §0.2, §0.3, §1, §2.4, §3, Table 2) - Addition of Table 1 to summarise the claims, arguments and evidence in 16626-709-000-RPT-0028 Issue 03.	29.10.12

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 7.1 - DESIGN PRINCIPLES OF THE INSTRUMENTATION AND CONTROL SYSTEMS

Monitoring and control of the UK EPR is carried out by the Instrumentation and Control (I&C) architecture, which consists of several sub-systems and their associated electrical and electronic equipment. The overall design of the I&C architecture and its associated equipment must comply with process, nuclear safety, and operational requirements.

The UK EPR I&C system is designed in accordance with the “defence in depth” concept (see Sub-chapter 3.1).

The different parts of the I&C architecture are classified and qualified according to their importance to safety and their conditions of operation. Sub-chapter 3.1 compares the EPR classification system with the method proposed in HSE Safety Assessment Principles (SAPs). Sub-chapter 3.2 describes the detailed classification requirements, Sub-chapter 3.6 the equipment qualification requirements and Chapter 13 the internal and external hazards that must be considered in the design.

To clarify the linkage between Sub-chapter 3.2 and Chapter 7, the following definitions are used:

I&C Function

An I&C Function represents the actions performed by the I&C equipment within a Safety Functional Group (consisting of one or more I&C Safety Features) to achieve a specific purpose as part of a Lower Level Safety Function (LLSF). The actions performed may include (but are not necessarily limited to) signal acquisition and processing, functional processing, actuation and information display. An I&C Function is categorised consistently with the Safety Category of the LLSF to which it contributes and with the safety classification principles defined in Sub-chapter 3.2 in line with IEC 61226:2009.

I&C Safety Feature

An I&C Safety Feature is a collection of I&C components generally belonging to a single system and working together to achieve a single action which is part of one or more I&C Functions. An I&C Safety Feature typically consists of only part of an I&C channel and thus usually falls into categories such as I&C instrumentation features, I&C processing features, I&C actuation features. An I&C Safety Feature inherits the Safety Classification of the Safety Functional Group of which it forms a part, consistent with the safety classification principles defined in Sub-chapter 3.2.

Further details are given in section 1 of this sub-chapter.

A deterministic approach is used for the design of I&C protection systems. More particularly, safety analysis is conducted, and the protection and the safeguard systems designed, using an iterative process in order to ensure that none of the events considered within the design basis lead to a significant release of radioactivity to the environment. See Chapter 14 for the description of the deterministic safety studies, including assumptions that have been made on the performance of the I&C protection system.

A probabilistic approach is used in parallel with the deterministic approach. Probabilistic Safety Assessments (PSA) (see Chapter 15 for the detailed description of the PSA) serve to confirm that reactor design objectives are met and to provide a basis for assessing the advantages of different design options while checking design compliance with the initial project objectives.

This chapter of the PCSR describes the main features of I&C systems that are the result of the design process. The chapter is organised as follows:

- Sub-chapter 7.1 presents the design principles of the I&C systems.
- Sub-chapter 7.2 describes the general architecture of the I&C and the qualification principles for the various instrumentation and control components and systems.
- Sub-chapter 7.3 describes the Class 1 parts of the I&C architecture, (i.e. the Protection System (RPR [PS]) and Safety Information and Control System (MCS [SICS])).
- Sub-chapter 7.4 describes the Class 2 parts of the I&C architecture (Safety Automation System (SAS), Reactor Control, Surveillance and Limitation system (RCSL) and Non-Computerised Safety System (NCSS)).
- Sub-chapter 7.5 describes the Class 3 parts of the I&C architecture (RRC-B Safety Automation System (RRC-B SAS), Process Information and Control System (MCP [PICS]), Process Automation System (PAS) and Severe Accident I&C System (SA I&C)).
- Sub-chapter 7.6 describes the instrumentation used. It covers the following: conventional process instrumentation, accident and severe accident instrumentation, process instrumentation pre-processing, in-core and ex-core instrumentation, rod position measurement, reactor pressure vessel water level measurement, loose parts monitoring and vibration monitoring, radiation monitoring and boron instrumentation.
- Sub-chapter 7.7 provides information for the design and development of the three I&C platforms (TELEPERM XS platform for the RPR [PS], RCSL and SA I&C, SPPA-T2000 platform for the MCP [PICS], PAS, SAS and RRC-B SAS and UNICORN platform for NCSS). Additionally, it provides information on the substantiation approach for software based systems for the TELEPERM XS and SPPA-T2000 platforms, any smart devices and any programmable complex electronic components that are subsequently used.

The UK EPR safety analysis described in PCSR Chapters 14, 15 and 16 depends on the performance of various automatic and operator initiated actions.

An analysis has been produced showing how the I&C architecture meets the UK EPR requirements specification [Ref-1] [Ref-2] and source standards, including those identified in the RCC-E [Ref-3]. The key requirements are identified and extracted and for each one a justification is given that the design does, or will, meet the key requirement. The supporting evidence for each requirement is identified and referenced.

The approach used for this analysis is a Claims, Arguments and Evidence (CAE) Report [Ref-4]. This presents the requirements on the UK EPR I&C as claims on the safety roles and capabilities of the I&C architecture, systems and equipment, including instrumentation. These claims are supported by arguments and evidence. The evidence is either in the PCSR itself or in documents that support the PCSR. In many cases, the evidence will be of the intent to perform the required process, activity or review as that process, activity or review will take place after the issue of the CAE report.

The overall claim made for the I&C described in Chapter 7 is that it adequately supports all automatic and operator initiated actions identified in the UK EPR safety analysis. The high level requirements on the I&C used to support the overall claim are:

1. to conform to standards appropriate to its functional category and safety class;
2. to be designed to provide defence in depth;
3. to be designed to be robust, reliable and safe;
4. to meet the safety functional requirements assumed by the safety analysis;
5. to be designed to enable the operators to fulfil their safety roles;
6. to continue to meet its safety functional requirements throughout its operational life.

Sub-chapter 7.1 - Table 1 details the claims given in the CAE report [Ref-4].

In addition, an analysis has been produced of how the UK EPR I&C design fulfils the required HSE Safety Assessment Principles in a claims, arguments and evidence format report [Ref-5].

The link between the CAE reports and the PCSR Chapter 7 is provided within those reports. Further information on the individual I&C systems can be found in the detailed design documentation of the I&C systems, which include quality plans, system specification reports and software and hardware design documents.

0. SAFETY REQUIREMENTS

0.1. SAFETY FUNCTIONS

The I&C systems are involved in the following main safety functions:

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

The classification principles, used to classify the systems listed above, are given in Sub-chapter 3.2.

0.2. FUNCTIONAL CRITERIA

All the means necessary to control and monitor the plant in normal operation (within specified operating limits and conditions) must be available to operators in the Main Control Room (MCR).

In addition, the operators must have at their disposal in the MCR all the operating facilities required to carry out all actions claimed in the safety case.

The I&C system must guarantee the execution of automatic actions identified in the safety case, with a reliability commensurate with that required in response to the frequency of the incident or event and within the required time period identified for that function.

If the MCR is unavailable (due to a fire for example), the operators must be able to shutdown the reactor as they leave that room and then be able to carry out monitoring and control of the plant from a Remote Shutdown Station, to allow a safe shutdown state to be reached and maintained.

0.3. REQUIREMENTS RELATING TO THE DESIGN

The requirements on the I&C systems are derived from the principles given in Sub-chapter 3.2.

0.3.1. Requirements

0.3.1.1. Functional classification of the system

Each of the I&C Functions must be categorised in accordance with the approach summarised in section 1.2.5 of Sub-chapter 3.1 and the principles detailed in Sub-chapter 3.2.

0.3.1.2. Single failure criterion

The Single Failure Criterion (SFC) will be taken into account in the design of Class 1 systems by ensuring a sufficient degree of redundancy, adequate independence/diversity and physical and electrical separation. The SFC must apply at the system level for Class 1 systems (including during any preventive maintenance or periodic system testing). A particular application for the MCS [SICS] is described in detail in Sub-chapter 7.3.

The SFC is applied at the functional level for Class 2 systems involved in the mitigation of the Plant Condition Category (PCC) faults studied in Chapter 14. Class 2 systems used under normal operations or used to implement the diverse line of protection (Sub-chapter 16.5) are not subject to the SFC, provided that reliability claims made in the PSA are met without application of this criterion.

0.3.1.3. Emergency power supplies

The electrical power supply to the Class 1 systems, and Class 2 systems involved in the mitigation of the faults studied in Chapter 14, must be backed-up (by the emergency diesel generators and associated batteries) so that these systems can continue to perform their functions in the event of loss of external electrical power supplies. This electrical power supply must be derived from the electrical supply train of the I&C equipment concerned.

The provision of emergency power supplies is applied on a case by case basis for Class 2 systems not involved in the mitigation of the PCC faults studied in Chapter 14, and for Class 3 systems.

0.3.1.4. Qualification under operating conditions

I&C systems must be qualified according to their safety role and for the environmental conditions described in RCC-E (including electromagnetic interference) in which they perform their mission.

I&C systems must be qualified according to the requirements defined in Sub-chapter 3.6.

0.3.1.5. Electrical and instrumentation and control classification

The electrical and instrumentation and control classes, and design requirements, of I&C equipment are defined on the basis of the principles in Sub-chapter 3.2.

0.3.1.6. Seismic classification

I&C systems must be seismically classified according to the requirements defined in Sub-chapter 3.2.

0.3.1.7. Periodic testing

All systems must be designed to permit periodic testing in order to confirm their ability to perform their required functions. The type of testing used will be determined by the function that the system is undertaking. Surveillance test intervals are derived from reliability studies of the I&C systems and are calculated to ensure that the probability of failure of the I&C system to perform the function is lower than the reliability claim.

0.3.2. Other regulatory requirements

0.3.2.1. Basic safety rules

Certain French government regulations, compatible with UK regulations (as discussed in Sub-chapter 1.4), apply to the design of EPR I&C systems, namely:

- RFS II.4.1.a - Software for safety-classified electrical systems. This specific code is applicable to the design of F1A (Class 1) and F1B (Class 2) electrical systems. Regulations relating to “software for 1E programmable systems" must be followed for software supporting F1A (Category A) functions, and those for "software for safety-classified programmable systems not classified 1E" must be followed for software supporting F1B (Category B) functions.

- RFS IV.2.b - Regulations for the design, qualification, implementation and operation of electrical equipment in safety-classified electrical systems. These requirements must be taken into account for F1A (Class 1) and F1B (Class 2) electrical systems. Requirements relating to “1E electrical equipment" must be followed for F1A (Class 1) I&C systems, and those relating to "safety-classified electrical equipment and not classified 1E" must be followed for F1B I&C (Class 2) systems.

0.3.2.2. Technical guidelines

The Technical Guideline for the design and the erection of the new generation of PWR reactor stated in letter DGSNR/SD2/0729/2004 dated 28 September 2004 "Options de sûreté du projet de réacteur EPR", in particular in paragraphs A1.2, A.2.2, B.2.1, B.2.2.2, C.2.1, G.3, G.4, are applicable to the design of I&C systems (see section 2 of Sub-chapter 3.1).

0.3.2.3. EPR-specific texts

Class 1, 2 and 3 systems must comply with the RCC-E (section 3 of Sub-chapter 3.8) and relevant standards (e.g. IEC standards), supplemented by specific data from the EPR project and site specific data.

0.3.3. Hazards

I&C systems must be protected against common cause failures that could result from internal or external hazards, according to the requirements defined in the relevant sections of Sub-chapter 3.1 (internal and external hazards).

0.4. TESTS

I&C systems must be subjected to pre-operational testing to confirm, after installation, that they conform to their design requirements.

Other appropriate tests (i.e. type and plant specific tests) are addressed in Sub-chapter 7.2.

The requirements for periodic testing are addressed in section 0.3.1.7 of this sub-chapter.

1. SAFETY CLASSIFICATION

The objectives of the safety classification given in Sub-chapter 3.2 are:

- to identify items that are important to safety;
- to divide them into safety classes according to their safety significance;
- to design, construct, and maintain them so that their quality and reliability remain commensurate with their safety classification.

As a general rule, the safety classification principles rely on a two-step process. The first step categorises safety functions into three categories (A, B or C) based on criteria that represent an assessment of the contribution of the safety functions to overall plant safety. The second step assesses the importance of Safety Functional Groups (SFGs) in the fulfilment of the safety functions. This second assessment identifies safety classes (1, 2, 3 and NC). More details are provided in Sub-chapter 3.2.

Based on these safety classes, the design requirements for the SFGs can be derived as detailed in Sub-chapter 3.2.

For the purposes of Chapter 7, the terms ‘I&C Function’ and ‘I&C Safety Feature’ have been introduced and defined at the beginning of this sub-chapter. I&C systems are classified globally based upon the highest safety class of I&C safety features they support.

In accordance with the safety principles of Sub-chapter 3.2, the I&C safety classification of I&C Safety Features, systems and equipment is defined by the highest category I&C Function that they are involved in performing.

The relationship between “I&C Functions categorisation”, "I&C Safety Features, systems and equipment classification” and “I&C components classification” is detailed in Sub-chapter 7.1 - Table 2.

2. DESIGN BASIS

2.1. DESIGN OF THE I&C SYSTEM ARCHITECTURE

The overall I&C design approach to achieve the safety goals is based on:

- the safety principles for classification (see Sub-chapter 3.2);
- the organisation of I&C in levels (see section 2.2);
- the defence in depth concept;
- the priority of requirements between the different I&C functions;
- the grouping of the I&C functions into types (see section 2.3);
- the requirements of the Human-Machine Interface (HMI)

in accordance with the safety requirements given in section 0 of this sub-chapter.

2.2. ORGANISATION OF THE I&C SYSTEMS INTO LEVELS

The I&C systems are structured in three levels:

- Level 0: the interface with the process. This mainly comprises the measurement and actuation functions (responsible for controlling the actuators and electrical switchgear);
- Level 1: the control (automation) level. This covers the automated functions and the interface with the other systems and equipment;
- Level 2: the monitoring and operating level of the unit. This comprises the functions that enable the operator to monitor and operate the plant.

2.3. TYPES OF FUNCTION

The I&C functions are sub-divided into the following types:

- Limiting Conditions of Operation (LCO) functions;
- limitation functions;
- operator aid functions;
- protection functions;
- post accident management functions;

- Risk Reduction Category (RRC) functions;
- control functions.

LCO functions are functions implemented to avoid extended operation beyond the limits prescribed in the safety case. These functions initiate corrective measures if the limiting conditions of operation (LCO) are exceeded. The LCO functions and associated operator actions contribute to maintaining the plant conditions within the envelope assumed in accident studies.

The limitation functions are those functions which are implemented to initiate (manually or automatically) corrective measures to avoid the need for protection actions and to maintain plant availability.

The operator aid functions are functions which provide significant help to the operator in monitoring and controlling the plant.

The protection functions are functions which are necessary to limit the effects of a Plant Condition Category event (PCC) and to reach the controlled state following the detection of such a PCC.

The post-accident management functions are the functions necessary to bring the unit from the controlled state to the safe shutdown state and to maintain it in this state after initiating events in categories PCC-2 to PCC-4.

The RRC functions are the functions implemented to limit the consequences of RRC events.

The control functions are the functions used to operate the plant under normal operations.

2.4. CONCEPT OF DEFENCE IN DEPTH

The safety of the unit is based on the concept of defence in depth which is based on the levels of defence as described in section 1 of Sub-chapter 3.1.

A requirement for independence between the functions belonging to the various lines of defence is established in order to meet the deterministic safety criteria and the safety objectives of the probabilistic analysis. Depending on the reliability figures used in Failure Modelling (see Chapter 15), high-frequency initiating events may need up to three lines of defence to achieve the probabilistic safety targets. Thus, the concept of defence in depth assigns the I&C functions to the following lines of defence:

- Preventive line of defence that controls main plant parameters within their expected operating range and prevents potential deviations from normal operation (limitation);
- Main line of defence for limiting the effects of PCC-2 to PCC-4 events (see Chapter 14 for more details). For frequent postulated initiating events, this line is required to be composed of a first line of protection and a diverse line of protection;
- A risk-reduction line of defence, forming part of the measures to reduce the risk of core melt and to limit the radioactivity release in the event of a core melt.

The structural organisation of the I&C systems and components must be such that sufficient independence between the lines of defence can be established in order to achieve the probabilistic targets (see Chapter 15). This includes considering functions where a failure of a system could be the initiating event and therefore the allocation of subsequent levels of defence has to be on a diverse platform. For example, if an RRC-A function addresses a fault sequence that could be initiated by the failure of a control or safety system, then the resultant diverse RRC-A function would be implemented on a platform that is diverse from the initiating system platform [Ref-1].

2.5. PRIORITY

Depending on the different tasks of the I&C functions, contradictory commands can be sent at the same time by different I&C functions to some actuators. As a consequence, general priority rules must be established.

The following general rules are applied to all actuators:

- Higher-class functions have priority over lower-class functions. The priority order is as follows:
    - Category A has priority over;
    - Category B, which has priority over;
    - Category C, which has priority over;
    - Non-Categorised functions.
- The order of priority within each category is as follows:
    - System and component protection has priority over;
    - Automated functions, which have priority over;
    - Manual functions.

Automatic functions can be switched off if the process conditions allow it.

2.6. REQUIREMENTS OF HUMAN-MACHINE INTERFACES (HMI)

The HMI design requirements which have an impact on the functional structure are described in Sub-chapter 18.1.

3. DEVELOPMENT LIFECYCLE REQUIREMENTS

The design and development of the I&C systems follow management and quality procedures and include the following documentation and phases (also see Sub-chapter 7.1 - Figure 1):

- Acquisition and Planning:
    - Overall Planning – including Quality Plans [Ref-1] [Ref-2], Qualification Plan (see section 3 of Sub-chapter 7.2), Configuration Plan, Security Plan, Test Plan and Commissioning Plan.
    - Acquisition of Requirements – including Safety Requirements, Operational Requirements, Plant Constraints [Ref-3] and Functional Requirements (see Chapters 14 to 16).
- Overall I&C design:
    - Engineering of I&C architecture – including Architecture Description and Allocation of I&C Functions [Ref-4].
    - Definition of Design Constraints for I&C systems – including Decoupling Concept, Failure Handling and Alarm Management, Periodic Tests, Maintenance, IT Security and Operating and Monitoring Concept from RCC-E [Ref-5] and relevant standards (e.g. IEC standards).
- System Life Cycle of I&C systems:
    - Including System Planning, Qualification Plan, Systems Requirements Specification (The FA3 Standard I&C systems CSCT [Ref-6] gives an example of specific requirements, an equivalent document will be produced for UK EPR), System Specification, Software and Hardware Detailed Design (see sections 1.4 and 2.4 of Sub-chapter 7.7), Analyses and System Validation.
- Qualification:
    - Overall I&C Integration – including Test Specifications and reports for Overall I&C Tests.
    - Analyses – including Common Cause Failure Analysis, Failure Mode and Effect Analysis, Reliability and Availability Study, Hazard Analysis, Human Factors Assessment, Test Coverage Analysis and Qualification Analysis.

The I&C design process must follow and comply with the relevant standards (e.g. IEC standards) including those identified in the RCC-E, and the technical guidelines (see Sub-chapter 3.1 - Table 1).

Individual I&C systems shall be compliant with consistent standards. Where there are no direct standards available, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, will be applied.

SUB-CHAPTER 7.1 - TABLE 1

Breakdown of I&C Claims from the Top Level Claim, to 6 High Level Claims and 40 Claims [Ref-1]

No.	**Top Level Claim:** The I&C System Supports the Safety of the UK EPR Power Plant
	Claim
	1. The I&C conforms to standards appropriate to its category and class. The I&C equipment has been designed, manufactured, tested, substantiated and commissioned to standards appropriate to its category and class.
1a	The I&C equipment shall conform to a structured safety function ***categorisation*** scheme.
1b	The I&C shall conform to a structured safety ***classification*** scheme.
1c	All I&C systems important to safety are designed, manufactured and installed to ***standards*** appropriate to their class.
1d	All I&C equipment shall be suitably ***qualified*** to demonstrate its suitability for the use intended.
1e	All I&C systems are ***validated*** to ensure they perform their safety function.
1f	***Commissioning***, testing and in-service inspection shall demonstrate that the as built design intent and future needs of I&C systems important to safety are met.
	2. The I&C architecture has been designed to provide 'defence in depth'. This takes account of the IAEA guidance (see NS-R-1) on the provision of defence-in-depth, including the application of diversity and independence.
2a	The UK EPR is designed and operated so that ***defence in depth*** is achieved by the provision of several levels of protection.
2b	***Common Cause Failure*** are considered to reach appropriate independence between I&C systems of the architecture.
2c	***Functional Diversity*** is incorporated as appropriate within the designs of I&C systems that form the main line of defence.
2d	***Independence*** is provided between redundant parts of systems and different lines of defence.
2e	***Electrical Isolation*** is used to avoid interference, reduce adverse interactions and prevent failure propagation.
2f	Where multiple ***commands*** can act on specific plant items, ***priorities*** are identified and acted on.
2g	The I&C architecture incorporates ***equipment diversity.***
2h	***Physical separation*** is used to prevent internal hazard spread.
2i	***Auxiliary services*** for I&C systems are designed in accordance with the I&C system requirements including those arising from the system's role within the I&C architecture.
	3. The I&C has been designed to be robust, reliable and safe. This takes into account measures to ensure safe reliable operation (including SFC, fault identification / avoidance and security).
3a	***Faults*** of I&C important to safety can be ***identified.***
3b	I&C systems important to safety exhibit a ***failure characteristic*** appropriate to their class.
3c	The requirements of the ***Single Failure Criterion*** have been implemented as appropriate for the category of safety function.
3d	The I&C is able to meet the required ***reliability*** claims.
3e	The I&C architecture includes measures to ***avoid*** the generation and propagation of ***faults.***
3f	I&C systems important to safety exhibit a ***behaviour*** appropriate to their class.
3g	Actions in response to plant faults are ***automatic*** and continue to completion.
3h	I&C systems important to safety ***minimise and manage complexity*** as far as possible.
3i	I&C important to safety includes conservative ***design margins*** suited to its class and expected lifetime.
3j	***Security measures*** protect the I&C architecture and systems against deliberate and intelligent attacks that may jeopardise functions important to safety.
	4. The I&C meets the safety functional requirements defined from consideration of the safety analysis. These topics identify the safety functional requirements, demonstrate they are appropriate, sufficient and implemented in design, manufacture & operation.
4a	The requirement for I&C systems important to safety and their ***functional requirements*** are determined.
4b	The safety analysis identifies the ***plant transients*** that are to be detected and the ***specific actions*** required from the I&C.
4c	Appropriate ***variables*** have been identified to monitor plant transients.
4d	The I&C is able to fulfil the actions required by the safety analysis (i.e. it has the appropriate Range / Accuracy / Stability / Setpoint / Time Response ***characteristics***).
4e	The ***capability*** of each I&C system is defined and its adequacy demonstrated.
4f	The ***design basis*** for each I&C system important to safety is established and documented.
4g	Appropriate ***plant constraints*** have been identified.
	5. The I&C systems enable the operators to fulfil their safety roles. These topics cover the MCR, RSS and other operator interfaces.
5a	A ***Main Control Room*** has been provided and can be used in all operational states.
5b	***Other*** control and monitoring ***locations*** are provided as required by the plant design and safety case.
5c	***Operator Interfaces*** enable operating staff to confirm the plant's nuclear safety status and carry out necessary manual control at all times.
5d	A suitable ***grace time*** is allowed for all claims for operator action.
5e	I&C systems important to safety have been designed according to ***human factors*** principles.
	6. The I&C Systems will continue to meet their functional safety requirements throughout their operational life. This is to ensure that the systems continue to meet their requirements and perform as intended.
6a	The I&C systems important to safety are assessed for ***reliability, availability and maintainability*** throughout their operating life.
6b	***In-service management*** processes ensure that 'qualification' is maintained.
6c	The I&C is subject to ***periodic testing*** according to the operational duty and class.

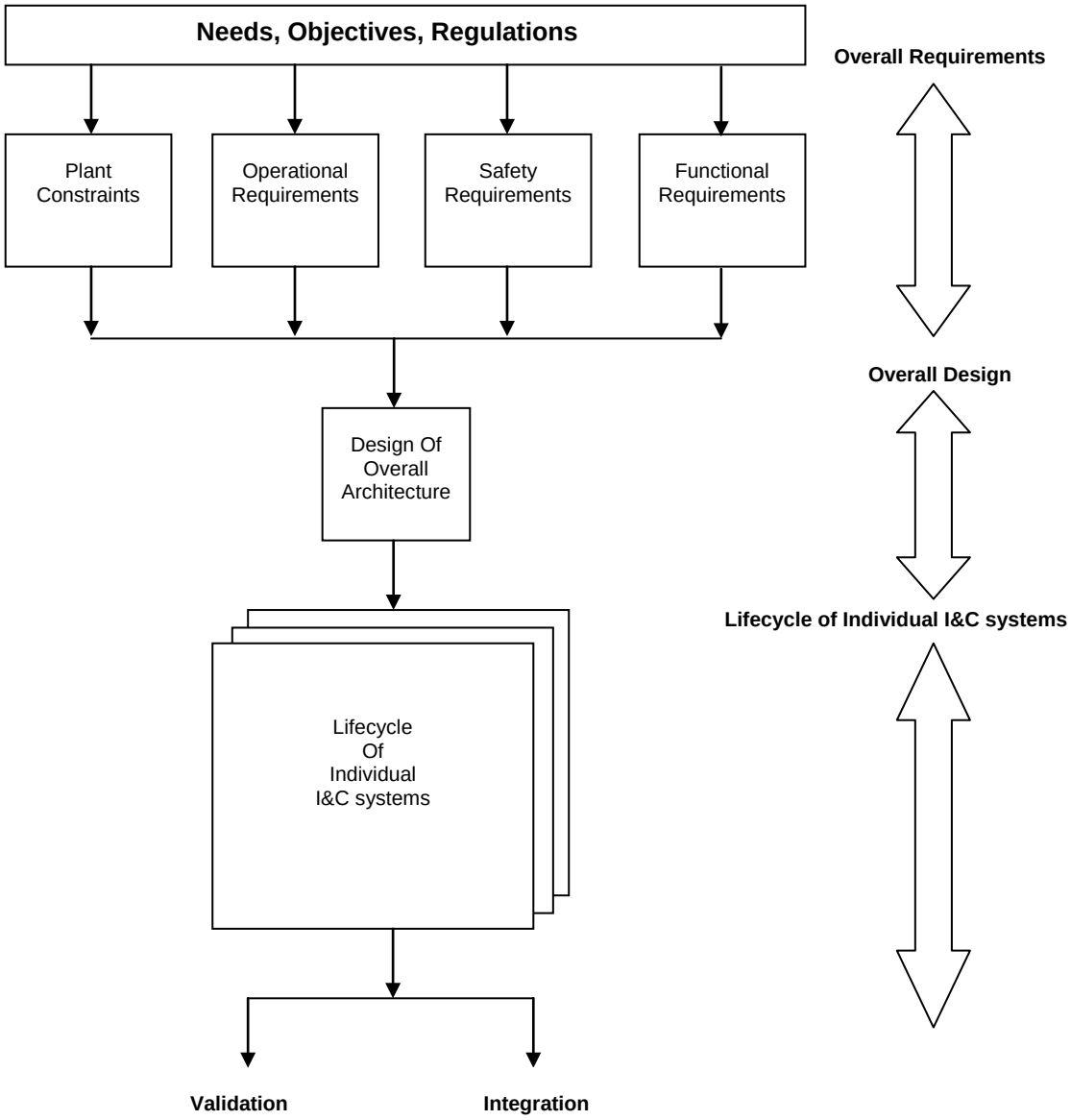
SUB-CHAPTER 7.1 - TABLE 2

Relationship between I&C function category, I&C safety features, systems and equipment class and requirements applicable to I&C components

	I&C Function categorisation	Classification requirements applicable to I&C Safety Features, systems and equipment	Classification requirements applicable to I&C Components
SAFETY CLASS	**Category A:** See Sub-chapter 3.2	**Class 1: Principal** **Class 2: Significant contribution** See Sub-chapter 3.2	**Class 1 Components:** - Design and construction must conform to the specific common requirements detailed in the RCC-E (see Sub-chapter 3.8) and relevant standards (e.g. IEC standards). - A Quality Assurance Program must be applied to the overall life cycle activities of the system. - Qualification for operating conditions. - Seismic classification as defined in Sub-chapter 3.2 section 6.1.
	Category B: See Sub-chapter 3.2	**Class 2: Principal** **Class 3: Significant Contribution** See Sub-chapter 3.2	**Class 2 Components:** - Design and construction must conform to the specific common requirements detailed in the RCC-E (see Sub-chapter 3.8) and relevant standards (e.g. IEC standards). - A Quality Assurance Program must be applied to the overall life cycle activities of the system. - Qualification for operating conditions. - Seismic classification as defined in Sub-chapter 3.2 section 6.1.
	Category C: See Sub-chapter 3.2	**Class 3: Principal** See Sub-chapter 3.2	**Class 3 Components:** - Design and construction must conform to the specific common requirements detailed in the RCC-E (see Sub-chapter 3.8) and relevant standards (e.g. IEC standards). - A Quality Assurance Program must be applied to the overall life cycle activities of the system. - Qualification for operating conditions. - Seismic classification as defined in Sub-chapter 3.2 section 6.1.

SUB-CHAPTER 7.1 - FIGURE 1

Engineering process



SUB-CHAPTER 7.1 – 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.

[Ref-1] Plant I&C requirement specification. ECECC100744 Revision A. EDF. June 2010. (E)

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

[Ref-3] Design and Construction Rules for Electrical components of nuclear islands. RCC-E. AFCEN Edition. December 2005. (E)

[Ref-4] UKEPR GDA I&C System CAE Document. 16626-709-000-RPT-0028 Issue 03. AMEC. June 2012. (E)

[Ref-5] Update of Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C. 16626-709-000-RPT-0031 Issue 02. AMEC. June 2012. (E)

2. DESIGN BASIS

2.4. CONCEPT OF DEFENCE IN DEPTH

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

3. DEVELOPMENT LIFECYCLE REQUIREMENTS

[Ref-1] UK EPR GDA Project Quality Plan. ECP3070095 Revision E. EDF. August 2010. (E)

[Ref-2] Overall I&C System Quality Plan. NLN-F DC 132 Revision A. AREVA. June 2010. (E)

[Ref-3] Plant I&C requirement specification. ECECC100744 Revision A. EDF. June 2010. (E)

[Ref-4] Architecture of instrumentation and control systems EPR UK: design principles and defense-in-depth. ECECC100831 Revision B. EDF. October 2012. (E)

[Ref-5] Design and Construction Rules for Electrical components of nuclear islands. RCC-E. AFCEN Edition. December 2005. (E)

[Ref-6] EPR - Technical Specifications and Conditions (CSCT) for Standard Instrumentation & Control General presentation report - CCF 01.
ECECC010055 Revision F1. EDF. October 2009. (E)

ECECC010055 Revision F1 is the English translation of ECECC010055 Revision F.

SUB-CHAPTER 7.1 - TABLE 1

[Ref-1] UKEPR GDA I&C System CAE Document. 16626-709-000-RPT-0028 Issue 03. AMEC. June 2012. (E)