IDM UID
27LH2V

VERSION CREATED ON / VERSION / STATUS
11 Mar 2011 / 6.1 / APPROVED

EXTERNAL REFERENCE

Guideline

Plant Control Design Handbook

The Plant Control Design Handbook defines standards, specifications and interfaces applicable to all ITER plant systems Instrumentation and Control (I&C).
Plant system I&C standards are essential for ITER to:

Maintain all plant systems I&C after delivery acceptance;
Integrate all plant systems I&C into one integrated control system;
Contain cost by economy of scale (spare parts, expertise).

This document is applicable to all ITER Procurement Arrangements which include any I&C.

Approval Process			
	Name	*Action*	*Affiliation*
Author	**Journeaux J.- Y.**	**11-Mar-2011:signed**	**IO/DG/DIP/CHD/CODAC/CDC**
CoAuthor			
Reviewers	**Bora D.** **Klotz W.- D.** **Park S.** **Wallander A.**	**15-Mar-2011:recommended** **15-Mar-2011:recommended** **15-Mar-2011:recommended** **11-Mar-2011:recommended**	**IO/DG/DIP/CHD** **IO/DG/DIP/CHD/CODAC** **IO/DG/SQS/QA** **IO/DG/DIP/CHD/CODAC/CDC**
Approver	**Haange R.**	**16-Mar-2011:approved**	**IO/DG/DIP**
Document Security: level 1 (IO unclassified) *RO: Chiocchio Stefano*			
Read Access	**LG: CODAC team, LG: [DOC] Baseline Managers, LG: KOPEC, LG: CDR - Managers, GG: MAC Members and Experts, GG: STAC Members , GG: Council Preparatory Working Group (CPWG), LG: [CCS] CCS-All, LG: [CCS] CCS-SectionLeaders, LG: [CCS] JACOBS, LG: CODAC team, LG: [CCS] CCS-Doc Control, LG: [CCS] ITER persons to access Jacobs folder, LG: [CCS] F4E, AD: ITER, AD: Only-staff, AD: External Collaborators, AD: Division - Electrical Engineering, AD: Section - CODAC, AD: Section - Remote Handling, AD: Section - Remote Handling - EXT, project administrator, RO**		

Change Log			
Version	***Latest Status***	***Date***	***Description of Change***
v6.1	Approved	11 Mar 2011	Version after PCR review see IDM comments on: https://user.iter.org/IDM/Pages/DocumentSystem.aspx?uid=47KR8J Alignment with QA template for Baseline guidelines
v6.0	Signed	10 Mar 2011	Next regular release (version after external review submitted to the PCR). From 5.2 version: Chapter 1: Add reference documents RD21, RD22. Add satellite documents for: CODAC core system overview, Guidelines for alarm handling and HMI, FAT and SAT, CWS case study, PLC software engineering handbook, Software engineering and QA, catalogues of cubicle products, rules and guidelines for PIS design, Acronyms for PCDH, PCDH glossary. PCDH picture updated accordingly. Chapter 2: R5 and R7 modified, introduction of exceptions in R11. Chapter 3: Plant system I&C supplier and designer moved to procurement I&C designer and supplier. R22 modified. R19, G48, I9, I10, I11 cancelled. Sat doc for methodology for I&C architecture simplified and PCDH section aligned, simplification of manufacture and integration phases by merging deliverables: D11, D15, D16, D73, D21, D27to D29, D33. D35 modified. D36 to D37, D45 to D47, D51 to D59, D61, D62, D64, D66 to D70, D76 cancelled. R296, R19, R26, R29, R31 to R36, R39, R42 cancelled. Chapter 4: section 4.3 aligned with new naming convention for variables: R65 to R69 modified. Section 4.4: R116 replaced by new guidelines for slow controller software development, clarification for SDD, detailed definition of COS matching RD18 introduced, new sections for HMI and alarm handling: R361 to R366 added, new standards for I&C cubicles: R140 modified, R157 and 158 added, Fast controllers: R133 modified, new cabling rules and earthing policy aligned with IO rules for cabling: R159, R160 and R313 added, R298 to R305, R307 to R308 , R319, R321 to R324 cancelled, sensor and actuator section cancelled. G47 moved to R178. Chapter 5: Definition of network hutch and panel modified. Chapter 6: Figure 6.1 updated. R218, R227 updated. R330 to R336 added. G26 to G32, R231, R239, G54 to G59, R241, R242, G53 cancelled. Section 6.2.1 rewritten. Sensor section removed. Chapter 7: R262 completed. R337 to R340, R279, R280 cancelled. R270, R271, R316, R317, R325 added, section 7.4.1 rewritten: R275 and R276 cancelled, R278 to R280 cancelled, R277 added, R341 to R360 added. Sensor section removed. Section 7.6 added. Chapter 8: no change. Chapter 9: Standards not mentioned have been removed: IEC12207, IEC61131, IAEA NS G 1&2, ISO62061. Table of risk classification removed (not used)
v5.2	Approved	08 Feb 2010	Plant Control Design Handbook v5.2
v5.1	Signed	01 Feb 2010	Changes from PCDH v5.0 to PCDH 5.1 --review report attached with PCDH v5.0 Removed: section 4.5.3 and 7.5.3, R50,R313, R138,R139,G13 Added: D76 Revised: section 1.4.2, 1.4.3, R317, 4.5.7, 8.1.1, All concerned links in section 6 & 7 due to section 4.5.3 removal. Re-arranged numbering: INPUTS I1 to I11, DELIVERABLES D1 to D9, D75 (renamed number),STATE MACHINES S1 to S9
v5.0	Approved	14 Dec 2009	Removed: RD2, D9, D10, I2, I3, S4, G12, G15, G17 to 23, G36 to G38, G41, G44, R66 to R68, R126 to R129, R141, R144 to R152, R165 to R177, R182, R183,R208 to R210, R195, R264, R270, R271, R277, R278, Table 4-1, Table 7-1,Table 7-2, section 5.3.8. Added: GL14, D75, I11, I12, G48 to G61, R296 to R340, section 1.4.3, section 6.1.1 (inserted label), section 6.2.2. Revised: R20 updated (same as in the PCDH 4.0), table naming revised to subsection label, section 4.2, section 4.3, section 4.4.8, section 4.5.4 to section 4.5.10, sections 4.5.5 and 4.5.6 merged, figure 5-1,tables 9-1, 9-2, 9-3, 9-4 revised to tables 9-1-1, 9-1-2, 9-1-3, 9-2-1, 9-2-2
v4.1	Approved	07 May 2009	
v4.0	Signed	11 Mar 2009	
v3.0	Signed	02 Jul 2008	Document presenting the scope of the prescriptive specifications of all I&C in all Plant Systems
v2.2	Signed	10 Jun 2008	Document presenting the scope of the prescriptive specifications of all I&C in all Plant Systems

v2.1	Signed	24 Apr 2008	Document presenting the scope of the prescriptive specifications of all I&C in all Plant Systems
v2.0	Signed	20 Apr 2008	Document presenting the scope of the prescriptive specifications of all I&C in all Plant Systems
v1.2	Signed	08 Feb 2008	Document presenting the scope of the prescriptive specifications of all I&C in all Plant Systems
v1.1	In Work	08 Feb 2008	Document presenting the scope of the prescriptive specifications of all I&C in all Plant Systems
v1.0	In Work	03 Aug 2007	Document presenting the scope of the prescriptive specifications of all I&C in all Plant Systems

TABLE of CONTENTS

1. INTRODUCTION

1.1. Purpose

This Plant Control Design Handbook (PCDH) document defines standards for all ITER plant system instrumentation and control (I&C). These standards are essential in order to achieve an integrated, maintainable and affordable control system to operate ITER. These standards are applicable to the development process and comprise deliverables and quality assurance requirements as well as catalogues of standard software and hardware components.

PCDH rules must be followed by everyone involved in the development of ITER plant systems I&C, i.e. plant system responsible officers (RO), plant system I&C designers and plant system I&C suppliers, regardless of their affiliation (i.e. ITER Organization (IO), domestic agency (DA), or industry).

The ITER Organization develops, supports, maintains and enforces the standards specified herein. Well established industrial standards, commercial off-the-shelf (COTS) and open source products are promoted, while custom-built solutions are strongly discouraged. Design choices and the prescribed standards are based on independent market surveys, prototype activities, benchmarking and evaluations.

PCDH is a living document, which is released at regular intervals throughout the lifetime of ITER. Versions of standards and products are subject to updates and extensions as the ITER project progresses. Obsolescence management is of particular importance due to the long timeline for ITER construction and operation.

1.1. Scope

PCDH is organized as follows:

- Chapter 1 gives an introduction with definitions and references;
- Chapter 2 gives a brief overview of plant system I&C design philosophy;
- Chapter 3 specifies plant system I&C development process and life cycle;
- Chapter 4 specifies rules and standards imposed on the plant system I&C hardware and software;
- Chapter 5 specifies the interface between plant system I&C and central I&C systems;
- Chapter 6 specifies rules and standards for Plant Interlock System;
- Chapter 7 specifies rules and standards for Plant Safety Systems;
- Chapter 8 specifies deviations policy;
- Chapter 9 contains appendices.

1.2. Definitions

Throughout this document **mandatory rules (or requirements) are enumerated and prefixed with R. Other statements are guidelines.**

Table 1-1: Paragraph identifiers, provides a list of paragraph identifiers used in this document.

AD	Applicable Document
D	Deliverable for a lifecycle phase
G	Guideline / Recommendation
GL	Glossary item
I	Input for a lifecycle phase

R	Rule / Requirement
RD	Reference Document
SD	Satellite Document
S	Operating State
TBC	To Be Confirmed
TBD	To Be Defined

Table 1-1: Paragraph identifiers

Paragraphs marked with TBD or TBC represent work in progress which will be confirmed and expanded further in the subsequent releases of this document.

1.2.1. Acronyms

ATEX	(fr.) "ATmosphères EXplosibles" (Explosive Atmospheres)
AVN	Audio-Video Network
CAD	Computer Aided Design
CATIA	Computer Aided Three-dimensional Interactive Application
CHD	CODAC & Information Technology, Heating & Current Drive, Diagnostics
CIN	Central Interlock Network
CIS	Central Interlock System
CODAC	COntrol, Data Access and Communication
COS	Common Operating State
COTS	Commercial Off-The-Shelf
CPS	Coordinated Programmable Safety
CPU	Central Processing Unit
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSN	Central Safety Networks
CSS	Central Safety Systems
CWS	Cooling Water System
DA	Domestic Agency
DC	Direct Current
DOORS	Dynamic Object-Oriented Requirements System
EDH	Electrical Design Handbook
EMC	ElectroMagnetic Compatibility
EPICS	Experimental Physics and Industrial Control System
FAT	Factory Acceptance Test
FBS	Functional Breakdown Structure
FPGA	Field Programmable Gate Array
GOS	Global Operating State
HMI	Human-Machine Interface
HPN	High Performance Networks
I&C	Instrumentation and Control
I/F	InterFace
I/O	Input / Output

IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IO	ITER Organization
IPT	Integrated Product Team
ISA	International Society of Automation
ISO	International Standards Organization
ITER	International Thermonuclear Experimental Reactor
LAN	Local Area Network
LCC	Local Control Cubicle
LED	Light Emitting Diode
LHS	Local Hardwired Safety
LPF	Local Passive saFety
LPS	Local Programmable Safety
LTM	Long Term Maintenance
MCR	Main Control Room
MF	Monitoring Function
MQP	Management and Quality Program
MTTR	Mean Time To Recovery
NS	Nuclear Safety
NTP	Network Time Protocol
OLC	Operational Limits and Conditions
OS	Occupational Safety
OSI	Open Systems Interconnection
P&ID	Process and Instrumentation Diagram
PA	Procurement Arrangement
PBS	Plant Breakdown Structure
PCDH	Plant Control Design Handbook
PCI	Peripheral Component Interconnect
PDF	Portable Document Format
PFD	Process Flow Diagram
PIN	Plant Interlock Network
PIS	Plant Interlock System
PLC	Programmable Logic Controller
PON	Plant Operation Network
POS	Plasma Operation State
PPEN	Pulsed Power Electrical Network
PS	Plant System
PSE	Plant System Equipment
PSH	Plant System Host
PSOS	Plant System Operating State
PSS	Plant Safety System
QA	Quality Assurance
RAMI	Reliability, Availability, Maintainability and Inspectability
RMS	Root Mean Square
RO	Responsible Officer

S-ICD	System Interface Control Document
SAT	Site Acceptance Test
SCC	Signal Conditioning Cubicle
SDD	Self-Description Data
SDN	Synchronous Databus Network
SF	Safety Function
SIL	Safety Integrity Level
SNMP	Simple Network Management Protocol
SRD	System Requirements Document
SSEPN	Steady State Electrical Power Network
STM	Short Term Maintenance
TCS	Test and Conditioning State
TCN	Time Communication Network
tokamak	(rus.) «toroidal'naya kamera s magnitnymi katushkami» (toroidal chamber with magnetic coils)
UTC	Universal Time Coordinated
XML	eXtensible Mark-up Language

Table 1-2: Abbreviations and acronyms

1.2.2. Glossary

[GL1] **Alarm** – a condition signalled by a plant system as having a possibility to prevent it from satisfying the operating requirements.

[GL13] **Autonomous** – ability to fulfil its own system's objective without being dependent on other interfacing systems (does not necessarily mean that no human is involved).

[GL2] **Commissioning** – a process of putting the plant system into service by means of adjustment of the system elements to enable them to operate safely and efficiently.

[GL3] **Cubicle** – a duly protected cabinet housing I&C hardware components as well as power supply and air ventilation facilities.

[GL14] **Event** – a condition signalled by plant systems as a result of plant system behaviour changes resulting from conditions, process and plasma with or without prediction. Events may occur in software or hardware.

[GL4] **Inspection** – verification that all instruments, equipment and cabling have been installed in accordance with the design documentation and that the installation conforms to I&C standards.

[GL5] **Instrument** – a device used for detecting, measuring or analyzing parameters of the process or equipment.

[GL6] **Instrumentation and Control** – synthesis of hardware and software applied as necessary to a technical process in order to attain the process' objective.

[GL7] **Interlock** – one or a combination of preventive and protective actions for investment protection.

[GL8] **Investment Protection** – protection of a system from material damage which would result in significant cost or schedule implications.

[GL9] **Operational Limits and Conditions** – a set of rules setting forth parameter limits, the functional capability and the performance levels of equipment and personnel safety..

[GL10] **Plant System (PS)** – an autonomous part of the ITER Plant implementing and responsible for a given technical function.

[GL11] **Safety** – a condition of being protected from nuclear, non-nuclear (conventional) and personnel hazards.

[GL15] **Signal** – analogue or binary state or command information that comes on a physical medium from/to a plant system sensor or actuator to/from a control system signal interface or controller.

[GL12] **Trip** – an automatic protective action against excursion beyond the defined limits.

[GL16] **Variable** – digitized representation of signals or representation of properties related to or derived from signals. Once signals have been digitized in a signal interface, the I&C controllers work with variables.

1.3. Related documents

1.3.1. Applicable Documents

The following documents, of the exact issue shown, form part of the documentation to the extent specified herein.

[AD1] Project Requirements (27ZRW8 v4.6, 07 May 2010).

[AD2] SRD-45 (CODAC) from DOORS (28C2HL v2.0, 29 Oct 2009).

[AD3] SRD-46 from DOORS (2EVTP5 v2.0, 17 Sep 2009).

[AD4] SRD-48 from DOORS (2EBF97 v2.0, 17 Sep 2009).

1.3.2. Reference Documents

The following documents are referenced in this document:

[RD1] ITER Instrumentation & Control – primer (32J454 v1.1, 29 Jan 2010).

[RD3] ITER Numbering System for Parts/Components (28QDBS v1.3, 04 Sep 2008).

[RD4] ITER Electrical Design Handbook (EDH) - Part 1: Introduction (2F7HD2 v1.4, 15 Sep 2009).

[RD5] EDH Part 4: Earthing, EMC and Lightning Protection (2ELREB v2.0 or higher).

[RD6] ITER Quality Assurance Program (22K4QX v7.3, 26 Jan 2007),

[RD7] MQP Deviations and Non Conformances (for EXT) (22F53X v4.4, 11 Apr 2008).

[RD14] Room book for buildings / areas on ITER Site (2A9NBX), dynamic database.

[RD15] Design Review Procedure (2832CF).

[RD16] ITER Procurement Quality Requirements (22MFG4 v4.0, 30 Mar 2009).

[RD17] ITER Function Category and Type for ITER Numbering System for Parts/Components (2FJMPY v1.2). (new version in progress)

[RD18] Operations Handbook – 2 Operational States (2LGF8N).

[RD19] Deviations and Non Conformances (for IO) (2LZJHB v1.1),

[RD20] Functional Breakdown Structure for ITER (43RRBR).

[RD21] IO cabling rules (335VF9 v1.2).

[RD22] CODAC Space requirements in Plant Buildings (2DVWUM v1.2), 23 Sep 2008.

[RD23] Control Room Concept Design - Environmental Performance Specification (2MT875 v1.2), 12 Jan 2011.

[RD24] ITER Human Factor Integration Plan (2WBVKU v1.1)

1.3.3. Satellite Documents

PCDH is made of a core document [this document] which presents the plant system I&C life cycle and provides the main rules to be applied on the Plant System I&Cs for industrial controls, interlock controls, occupational safety controls and access safety controls. Some I&C topics are further detailed in dedicated documents associated to PCDH so called satellite documents and referenced [SDXX]as presented in Figure 1.

These satellite documents provide guidelines, recommendations and explanations, but no mandatory rules. Only PCDH core document is part of the baseline and contractually binding.

The Operation Handbook [RD18] is mentioned as a reference document for definition of Common Operating States.

[SD1] Plant System I&C Architecture (32GEBH v2.3),
[SD2] Methodology for PS I&C specifications (353AZY v3.3),
[SD3] I&C signal and variable naming convention (2UT8SH v7.3),
[SD4] Self description schema documentation (34QXCP v2.0),
[SD5] The CODAC - Plant System Interface (34V362 v2.0),
[SD6] PS factory acceptance plan (3VVU9W v1.5)
[SD7] ITER operator user interface (3XLESZ, v2.0)
[SD8] ITER alarm system management (3WCD7T, v2.0)
[SD9] I&C signal interface (3299VT v4.4),
[SD10] PLC software engineering handbook (3QPL4H, v1.3)
[SD11] Software engineering and QA (2NRS2K, v2.1)
[SD12] Slow Controller catalogue (333J63 v1.7),
[SD13] Guidelines for fast controllers (333K4C v1.3),
[SD14] Fast Controller products catalogue (345X28 v1.3),
[SD15] Cubicle products catalogue (35LXVZ v2.3),
[SD16] Guidelines for the design of the PIS (3PZ2D2, v2.4),
[SD17] CWS case study specifications (35W299 v3.3),
[SD18] ITER CODAC glossary (34QECT v1.2),
[SD19] ITER CODAC Acronym list (2LT73V v2.2),
[SD20] CODAC Core System Overview (34SDZ5 v2.5).
[SD21] Plant Control Design Handbook for Nuclear control systems (2YNEFU v2.1)
[SD22] Management of local interlock functions (TBD)
[SD23] Guidelines for diagnostic data structure and plant system status information (TBD)

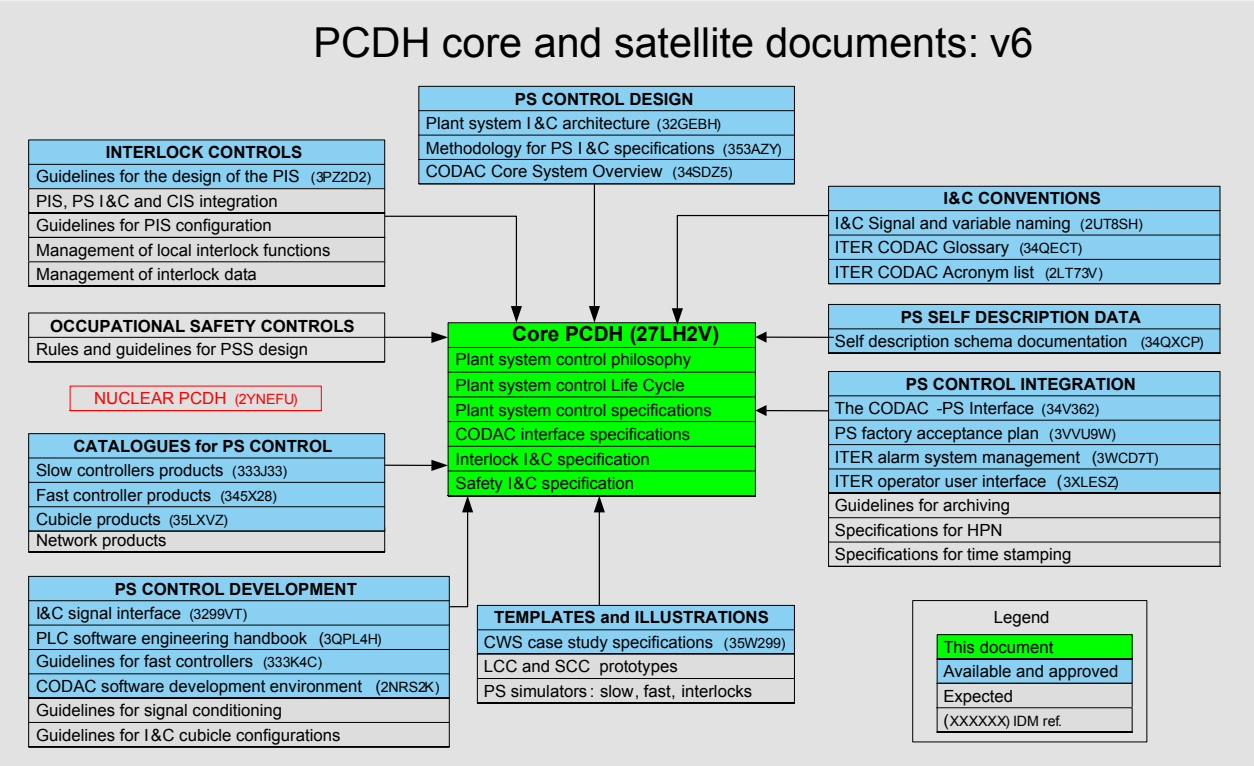

Figure 1-1: PCDH related documents

2. PLANT SYSTEM I&C DESIGN PHILOSOPHY

2.1. Introduction

This chapter gives a brief overview of ITER I&C System architecture before outlining the design philosophy of plant system I&C and its main functions. ITER Instrumentation & Control primer document [RD1] provides an introduction to ITER I&C system, CODAC system and plant systems.

2.2. Functional role of systems

The ITER I&C System is divided into three vertical tiers with two horizontal layers as shown in Figure 2-1.

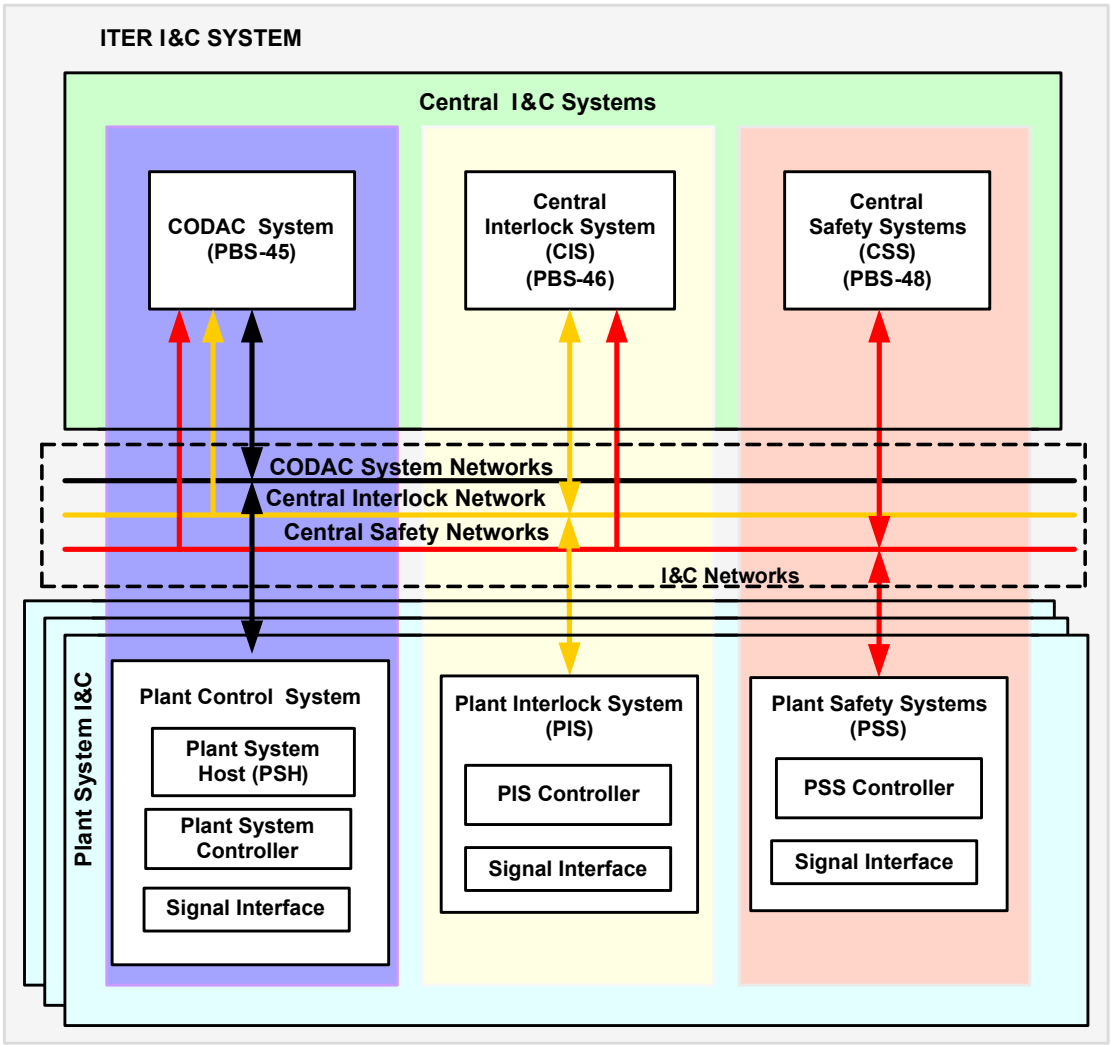

Figure 2-1: ITER I&C System – CODAC System, Central Interlock System, Central Safety Systems and plant systems I&C

- **ITER I&C System** – All hardware and software required to operate the ITER machine. Comprises plant systems I&C, central I&C systems and I&C networks.
- **Central I&C Systems** – All hardware and software required to coordinate and orchestrate all plant systems I&C, including plant-wide investment protection and safety functions and to provide the human-machine interface (HMI). It comprises the CODAC System, Central Interlock System and Central Safety Systems.

- **Plant System I&C** – All hardware and software required to control a plant system including local investment protection and safety functions. Comprises Plant Control System, Plant Interlock System and Plant Safety Systems.
- **CODAC System** – Provides overall plant systems coordination, supervision, plant status monitoring, alarm handling, data archiving, plant visualization (HMI) and remote experiment functions. Communicates with plant control systems using CODAC networks.
- **Central Interlock System (CIS)** – Provides plant-wide investment protection functions. Communicates with Plant Interlock Systems using Central Interlock Network. Provides status to CODAC System.
- **Central Safety Systems (CSS**) – Provide plant-wide nuclear and occupational safety functions. Communicate with Plant Safety Systems using Central Safety Network. Provide status to Central Interlock System and CODAC System.
- **I&C Networks** – Provide physical interface between Central I&C Systems and plant systems I&C. Comprises CODAC Networks, Central Interlock Network and Central Safety Networks.
- **CODAC Networks** – A set of networks providing the physical and logical interconnection between CODAC System and plant systems I&C. The functions of different CODAC networks include distribution of commands and data exchanges, time and events, plus means of fast synchronous communication.
- **Central Interlock Network –** Provides the physical interface between Central Interlock System and Plant Interlock System.
- **Central Safety Networks** – Provide the physical interface between Central Safety Systems and Plant Safety Systems.
- **Plant Control System** – Provides local data acquisition, control, monitoring, alarm handling, logging, event handling and data communication functions. Communicates with CODAC System using CODAC Networks. Comprises plant system host, plant system controller(s) and signal interface(s).
- **Plant System Host (PSH)** – Provides asynchronous communication from CODAC System to Plant Control System and vice versa. Provides command dispatching, state monitoring, data flow and configuration functions.
- **Plant System Controller** – Provides plant system specific data acquisition, control, monitoring, alarm handling, logging and event handling functions.
- **Signal Interface** – Provides signal conditioning, isolation and connection functions for sensors and actuators.
- **Plant Interlock System (PIS)** – Provides investment protection function for plant system. Interfaces to Central Interlock System for plant-wide investment protection functions. Comprises Plant Interlock System Controller and Signal Interface.
- **Plant Interlock System Controller** – Provides event detection, monitoring and logic for investment protection functions.
- **Plant Safety Systems (PSS)** – Provide safety functions for plant system. Interface to Central Safety Systems for plant-wide safety functions. Comprise plant safety system controllers and signal interfaces.
- **Plant Safety System Controller** – Provides event detection, monitoring and logic for safety functions.

2.3. Plant system I&C mandatory functional requirements

[R1] Plant system I&C shall perform control of the plant system under the authority of Central I&C systems during any operating state.

[R2] Plant system I&C shall comply with project-wide supervisory control functions and central data handling functions (i.e. archiving, monitoring, logging and visualization) provided by CODAC System.

[R3] Plant system I&C shall make available all data acquired from sensors/actuators, with a time stamp, to Central I&C Systems for analysis, archiving, logging, monitoring and visualization. The principle of “no hidden data” is applicable for all plant systems I&C; there shall be no permanent local storage of data.

[R4] Plant system I&C shall provide status information for common operating states, plant system operating states, alarm conditions, trip conditions and corrective actions, control system set points and power supply status information that is required to operate the plant system I&C from Main Control Room (MCR).

[R5] Plant system I&C shall be designed to be configurable from MCR using its self-description data.

[R10] Plant system I&C shall be operated centrally from MCR.

[R11] Permanent local control rooms are forbidden. There are two exceptions to this rule; remote handling and tritium plant.

[R12] Plant system I&C shall use Mini-CODAC as a tool for plant system software development support, integration, factory acceptance test and site acceptance test. Mini-CODAC will be complemented by certified tools for PIS and PSS.

[R15] Plant system I&C shall have built-in absolute-limit protection to prevent local control and central control errors. Time critical devices shall have built-in time-outs to ensure correct operation in case of Central I&C Systems failure.

3. PLANT SYSTEM I&C LIFE CYCLE

3.1. Introduction

This chapter specifies the plant system I&C life cycle and development process. For each phase in the life cycle the required inputs, the methodology and rules applicable and the resulting outputs (deliverables) are defined. Applying this development process will ensure that the plant system I&C is fully compliant with PCDH and reference documents as shown in section 1.4.2.

This chapter defines roles and responsibilities, but not the assignment of those to IO, DA or external party. The assignment of roles shall be defined in the particular procurement arrangement (PA).

3.2. Roles

- **Plant System Responsible Officer** – Provides input throughout the design process. He/she reviews the plant system I&C design as well as approves PS factory acceptance test and site acceptance test.
- **Plant System Central I&C Responsible Officer** – Develops, supports, maintains and enforces I&C development standards, development process and design conventions. He/she also provides PSH hardware and software to plant system I&C supplier. He/she reviews the plant system I&C design and participates to factory acceptance test and site acceptance test.
- **Procurement I&C Designer** – Designs the I&C system according to I&C specifications for a plant system at the procurement stage.
- **Procurement I&C Supplier** – Supplies any I&C equipment or component including spare units for a plant system procurement. The boundary of the supply is defined in the PA. Configuration of the PSH and Mini-CODAC – used as a local CODAC system – is a task of the plant system I&C supplier.
- **Plant System I&C Integrator** – Integrates all plant system I&Cs to ITER Central I&C Systems. He/she is in charge of the I&C part of the plant system integrated commissioning.
- **Plant System Operator** – Operates the plant system I&C. He/she works mainly in the MCR and uses control and monitoring tools delivered by the plant system I&C supplier. He/she has received the necessary training based on information provided by the plant system I&C supplier.
- **Plant System I&C Maintenance Operator** – Maintains the plant system I&C. He/she conducts preventive and routine maintenance as well as unplanned maintenance in case of breakdown. He/she manages spare units.

3.3. Lifecycle Phases

As a part of plant system procurement, the procurement process of plant system I&C shall comply with the general scheme and procedures used for the ITER project.

This scheme foresees a procurement process in three main phases as illustrated in Figure 3-1.

- A **design phase** in two steps - plant system I&C design followed by a project review as defined in Figure 3-1. The two steps are repeated for conceptual, preliminary and detailed design.
- A **manufacturing phase** in two steps – plant system I&C manufacture and factory acceptance test. Individual tests of I&C equipment shall be performed during manufacture.

- An **integration phase** in three steps – plant system I&C installation on ITER site followed by site acceptance test and integrated commissioning. Site acceptance test includes integration of plant system I&C subsystems and acceptance tests of the whole plant system I&C if applicable.

The procurement process is followed by:

- **Operation and maintenance phases** - These two phases are merged together as shown in Figure 3-1 as they are closely linked, they are not in the scope of PCDH.
- **Decommissioning phase** - completes the plant system I&C lifecycle, but is outside the scope of PCDH.

Each phase or step is characterized by its outputs, which are the deliverables at completion of the phase or the step. The outputs from one phase or step are used as inputs to the next phase or step together with I&C requirements and guidelines as provided in this document and other ITER handbooks.

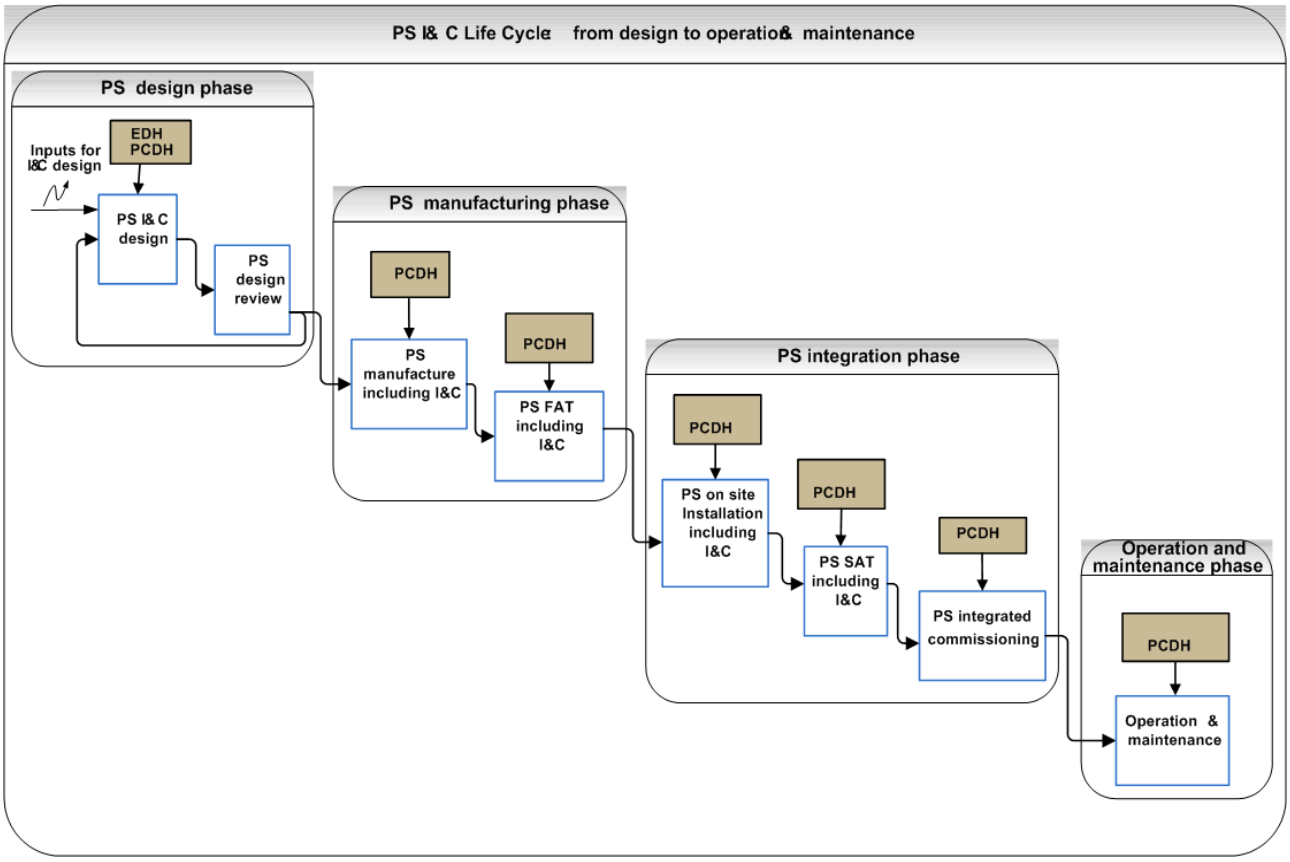

Figure 3-1: Plant system and procurement I&C life cycle from design to operation.

3.4. Plant System I&C Development

This section details the plant system I&C development process introduced, by defining the life cycle, in previous section. For each step the required inputs, applicable rules and methodology in order to generate the outputs required for the next step are defined.

The deliverables identified in this section as [DXX] are delivered at completion of each I&C life-cycle phase considered. They may be required depending on the PA configuration.

The [SD2] provides guidelines for the I&C life-cycle.

3.4.1. I&C Deliverables Management

[R18] Outputs or deliverables shall be identified and managed to ensure that IO and involved DAs know that they have the correct version and shall be advised of any changes and/or deficiencies. Each output shall be recorded with at least the output identifier/name, the type, the description, the current version and the status (not built, built, reviewed and approved).

[R20] All deliverables shall be traceable to their parent output as well as to their relevant specification and design item.

[R21] All deliverables in electronic format shall be backed up after the acceptance phase in order to secure a functional restore state.

[R22] All deliverables shall be kept updated along the whole lifecycle up to the SAT by the I&C supplier. All deliverables shall be approved by IO.

3.4.2. Deliverables for I&C technical specifications

Deliverables for I&C design:

At completion of the plant system I&C final design, the specifications issued of the plant system I&C shall include the following items:

[D1] Plant system I&C function and architecture. This includes a high level functional analysis (D1A), a detailed functional breakdown with functional links and the characterization of functions (D1B), and the physical architecture with separation of conventional, interlock and safety controls (D1C).

[D5] Plant system controller(s) computational and signal IO performance requirements. and physical configuration requirements.

[D6] List of physical input and output signals (I/O) of the I&C controllers and signal conditioning units. Documentation in Interface sheets.

[D7] List of the variables handled by the plant system I&C controllers. This includes plant internal variables as well as all variables exchanged via networks (grouped by network/function). Separate by type of controller (conventional, interlock, safety).

[D8] Physical configuration of plant I&C within I&C cubicles including intra-rack and external cabling connections (includes networks).

[D9] Detailed description of plant system state machines (PSOS) with all states, transitions, procedures and state variables. Documentation in standard prescribed graphical format.

Plant system I&C inputs recommended for I&C design:

The plant system responsible officer provides these inputs during the design process:

[I1] Plant system I&C operation and control philosophy. This includes operation concepts, high level operational procedures and plant system operating states (PSOS) with mapping to COS and GOS.

[I2] High level Plant system functional analysis.

[I3] Plant system PFDs, P&IDs mechanical and electrical drawings related to I&C conceptual design.

[I4] A list and short description of main plant system operating states for plant system operation.

[I5] Plant system risk analysis and I&C hardware and software RAMI requirements

[I6] System Interface Control Documents (S-ICDs) relevant for the plant system I&C.

[I7] List and specifications of the main protection functions to implement within the plant system or with respect to other plant systems. The specifications include a risk analysis to identify the interlock functions from amongst all of the protection functions.

[I8] List and specifications of the main safety functions and safety related measurements to be implemented within the plant system or with respect to other plant systems. Distinguish between nuclear, occupational, access, and safety relevant functions.

Rules and guidelines required for I&C design:

They are defined in the related sections of that document. Some topics may be further detailed; in such a case refer to the dedicated satellite document. See Figure 1-1 for available satellite documents.

- General architecture, methods, standards for the whole plant system I&C: chapter 4
- Conventional controls: chapter 4
- Interface with CODAC systems: chapter 5.
- Specific rules and guidelines applicable to interlock controls: chapter 6.
- Specific rules and guidelines applicable to nuclear and occupational safety controls: chapter 7.

Methodology for defining the plant system I&C architecture

- A Functional Breakdown Structure (FBS) for each plant system is the first step. This PS FBS is used to determine the process functions of the plant system and to identify the I&C functions required to control the plant system.
- Then CAD drawings and text documents giving details for each I&C function are issued. The I&C functions and the data links between the I&C functions are characterized for required amount and performance.
- The third step is to distribute these I&C functions in controllers in a consistent way for operation and technology.
- The last step is to link the controllers with CODAC networks physically and functionally in order to get the I&C architecture of the plant system. The document “Methodology for plant system I&C design” [SD2] provides guidelines for this process and together with plant system I&C technical specifications.

3.4.3. Deliverables and requirements for I&C Manufacture

Plant system I&C manufacturing is assumed to be performed as part of an integrated process for the manufacture of the whole plant system. However, in some cases, for procurement sharing purposes, plant systems are split in several procurements distributed among ITER partners. In this case, the plant system I&C manufacturing phase must cope with such configurations in order to avoid any major issues during on-site integration at ITER.

The manufacturing phase should include a manufacture design and construction activity, in which there shall be check points. The final check point at completion of manufacture is followed by a Factory Acceptance Test (FAT) for each plant system procurement.

Deliverables for I&C manufacture:

Outputs requested at completion of the manufacturing phase are as follows:

Hardware:

[D18] I&C cubicles with internal wiring and all internal I&C equipment. Sensitive equipment shall be packed separately for shipping and shall be mounted and wired on site in order to provide cubicles with all internal I&C equipment ready to be installed on ITER site and connected to:

- CODAC System, CIS and CSS interfaces (see section 4.4.6).
- Main supply and earth.

[D19] I&C spare parts list with appropriate specifications of storage space and conditions.

Software:

[D72] Source code of any software developed for the plant system I&C for operation, factory acceptance test, site acceptance test, integrated commissioning and maintenance, in the scope of the PA. Configuration data for any plant system I&C controller to be downloaded.

[D20] Plant system I&C self-description data (see section 4.4.6).

[D26] Mini-CODAC: configuration developed in Mini-CODAC environment required for factory acceptance test, site acceptance test and integrated operation.

Manufacturing documents or data:

[D31] Detailed descriptions (text documents including structured lists in self-description data format) of:

- Process control for any plant system operation state.
- Process failure detection and strategy for process control.
- I/O treatments.
- Data exchanges required for slow and fast controls.
- Feedback controls.
- HMI, alarms and events.
- Software architecture for these items with identification of related software modules and data exchange links.

[D32] Full software and configuration documentation as generated by the ITER IO prescribed engineering tools.

[D34] Every document required for cubicle mounting, air conditioning, assembly, external and internal wiring, earthing and powering. Inventory of any equipment or component used for cubicle manufacturing (including I&C equipment), with supplier identification and a supplier procurement reference.

ITER on-site installation documents:

[D38] Cabling documents for cubicle connection with I/O cabinets, I&C Networks, earth and power supplies.

[D39] Procedure of installation, configuration, starting up and software and hardware completeness checks for the plant system I&C in particular for plant system specific components (non standard components).

Maintenance documents:

[D40] Original technical documentation for each piece of equipment or component (including software) used to manufacture the systems in an I&C cubicle.

[D41] Schematic diagrams of the full signal path from the sensors/actuators to the I/O boards of the controllers including powering and conditioning, with identification of test points for fault analysis or calibration and identification of the terminal blocks. Trouble shooting procedures and functions.

[D42] Calibration factors for each sensor-actuator-conditioner-I/O board and procedures for re-calibration of these components.

[D43] Technical documents, manuals and procedures required for maintenance of any I&C component.

[D44] Maintenance plan: detailed warranty and/or maintenance periods and their possible extensions, licensing requirements.

[D74] Tools required for maintenance of any I&C component.

Conformity reports:

[D48] Certificates of conformity for I&C procurement to any regulation applicable on ITER site and proof of compliance to ITER I&C standards.

Rules required for I&C manufacture:

These rules are to be found within this document in the relevant chapters.

3.4.4. Deliverables and requirements for I&C Factory Acceptance Tests

Plant system factory acceptance tests (FAT) are intended to check the conformity of the procured plant system to IO requirements including PCDH requirements. Plant system I&C FAT is a part of the plant system FAT. All I&C components in the procurement shall be powered and tested during FAT. The FAT scenario for I&C will be adjusted depending on configuration of the I&C procurement with the policy to test as much as possible as soon as possible.

[G1] The leading guideline of FAT scenario is to test I&C performance and functionality as much as reasonable achievable. The Mini-CODAC is used for FAT and it will be configured in order to match the FAT campaigns and scenarios.

[R23] For every test (unit testing; system and integration testing; acceptance testing) the version of the equipment being tested, the version of the test specifications being used and, for acceptance testing, the version of the design specification being tested against, shall be recorded.

[R24] The procurement I&C supplier shall provide all necessary hardware and software tools and configuration files for FAT.

[G2] It is recommended that compliance with I&C standards and design rules is checked throughout the manufacturing process in order that the FAT runs more smoothly.

Deliverables for I&C Factory Acceptance Tests:

The scenarios for FAT are detailed in [SD6].

The FAT scenario to be considered will depend on the procurement configuration. The following configurations have been considered:

- Configuration#1: the procurement only comprises equipment with sensors and actuators, without any I&C hardware.
- Configuration#2: procurement comprises equipment with I/Os chassis and boards, without CPU.
- Configuration#3: procurement comprises equipment with conventional and possibly interlock controllers (i.e. I/Os and CPUs), without PSH and mini-CODAC.
- Configuration#4: procurement comprises equipment, conventional and possibly interlock controllers and PSH + mini-CODAC.

[D50] A single report collecting all I&C FAT results related to I&C will be issued It must include tracing to all requirements fulfilled, not fulfilled and not testable. A template is provided in [SD6].

- **Rules required for I&C Factory Acceptance Tests:**

[R25] The results of FAT shall be recorded and retained in the lifetime records of the ITER plant. Any failures during FAT shall be investigated and the cause and rectification of the failure documented in the FAT report. A complete bug report (problems and fixes) must be provided and maintained during all life-cycle phases.

3.4.5. Deliverables and requirements for I&C Installation on ITER site

ITER site installation includes ITER site reception of I&C cubicles and equipment, damage checking at reception, installation of cubicles, mounting of I&C equipment within the cubicle, cubicle cabling and cubicle powering.

Deliverables for I&C installation:

[D60] I&C installation instruction document for hardware installation and software installation on ITER site. This document has to be delivered prior to the beginning of the hardware installation on site and has to be approved by PS I&C RO.

3.4.6. Deliverables and requirements for I&C Site Acceptance Test

The plant system site acceptance test (SAT) is intended to check conformity with IO requirements of the plant system procurement first as a stand-alone. Plant system I&C SAT is part of the plant system SAT. All I&C equipment shall be powered and tested during SAT.

Plant system I&C SAT is first a repeat of FAT for each procurement. In addition, the SAT will include a performance test of the whole plant system when possible. Attention shall be paid to checking of plant system interlock and safety functions as they may be integrated with the whole plant system I&C for the first time. During SAT, the plant system I&C is still not connected to Central I&C Systems: therefore SAT is performed with Mini-CODAC. Mini-CODAC may be complemented by specific tools for the PIS and PSS. Data links with Mini-CODAC not tested during FAT shall be tested during SAT. See [SD6] for details for FAT.

Deliverables for I&C SAT:

[D65] A single report collecting all SAT results related to I&C will be issued.

Rules required for I&C SAT:

[R30] The results of SAT shall be recorded and retained in the lifetime records of the ITER plant. Any failures during SAT shall be investigated and the cause and rectification of the failure documented in the SAT report.

[R371] SAT is performed with Mini-CODAC. Mini-CODAC may be complemented by specific tools for the PIS and PSS.

[R372] Data links with Mini-CODAC not tested during FAT shall be tested during SAT. See [SD6] for details for FAT.

[R373] For performance test purpose, the plant system I&C shall be tested under a scenario and acceptance criteria provided by the ITER plant system RO. This scenario shall include the individual tests of every plant system I&C function with the real process connected to the plant system I&C and the test of the plant system as a complete autonomous system, without any interaction with Central I&C Systems. This test of plant system performance is out of scope of PCDH.

3.4.7. I&C Integrated Commissioning

This phase is not in the scope of PCDH.

3.4.8. I&C Operation and Maintenance

This phase is not in the scope of PCDH.

3.4.9. Deliverables and requirements for I&C Obsolescence Management

It shall be possible to replace plant system I&C equipment to cope with I&C maintenance issues, plant system I&C upgrades, I&C hardware or software obsolescence, or as a result of it becoming increasingly expensive to operate and maintain.

Deliverables for I&C obsolescence management:

[D71] A proactive management plan for obsolescence describing the strategies for identification and mitigation of the effects of obsolescence throughout all stages of I&C life cycle. This management plan shall be produced during the design phase and maintained through all the phases.

Rules required for I&C obsolescence management:

[R291] The latest PCDH version available shall be applicable when the PA is signed.

[R37] IO is committed to support old versions of PCDH standards, including the obsolescence management of those standards.

[R38] Every new I&C equipment shall be documented in the same way as was required for the initial procurement.

[R40] Training for operation and maintenance teams shall be included in the process of replacement, if required.

[R41] The plant system ROs shall define requirements for their plant system I&C backup and storage by successive evolutions and the strategy to adopt in case of obsolescence.

3.4.10. I&C Decommissioning

This phase is not in the scope of this document.

3.4.11. Requirements for I&C Documentation

[R43] All documentation shall be in the English language.

[R44] All documentation shall be available in electronic format (PDF, Open Document XML format or Microsoft Word) and in an online version which is accessible using IO product lifecycle management system.

[R45] All documentation shall be under version control.

[R46] For every item (including 3rd party and COTS) the original documentation shall be delivered.

4. PLANT SYSTEM I&C SPECIFICATIONS

4.1. Introduction

This chapter specifies plant system I&C common to all ITER plant systems. It comprises plant system I&C architecture, software and hardware specifications.

4.2. Plant System I&C Architecture

The plant system I&C architecture shall be defined from a generic ITER plant system I&C template, which shall be extended and adjusted according to the need for the particular plant system under consideration. Figure 4-1 and Figure 4-2 give two examples of possible plant system I&C physical architectures.

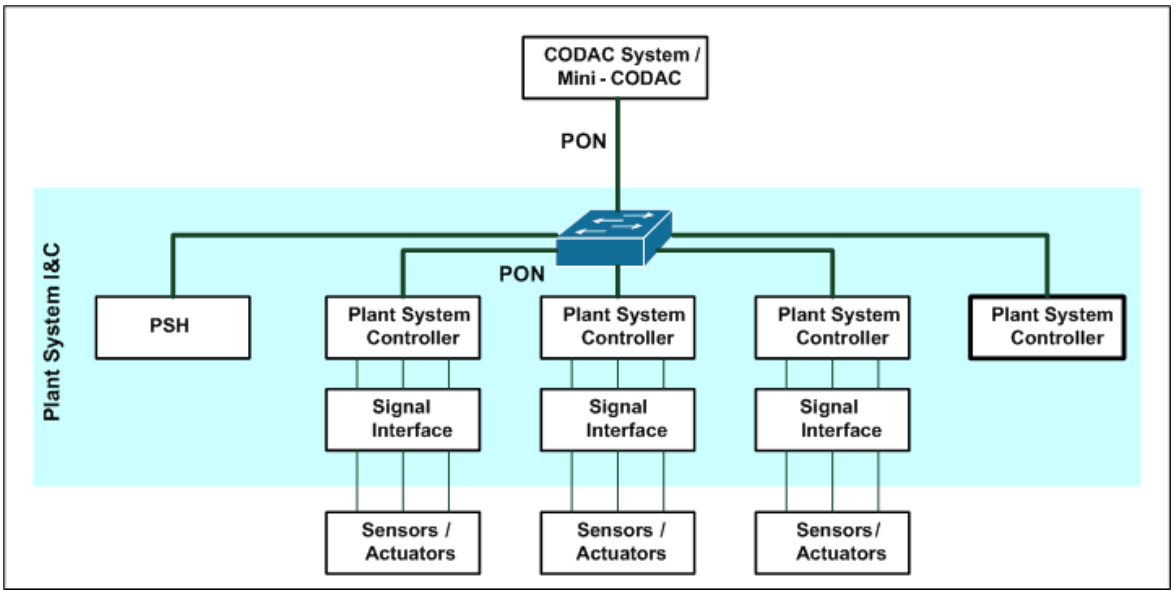

Figure 4-1: Plant system I&C physical architecture – example 1, tightly coupled system. Plant system has one supervising plant system controller (to the right). The supervising plant system controller coordinates three other plant system controllers which interface to the hardware**.**

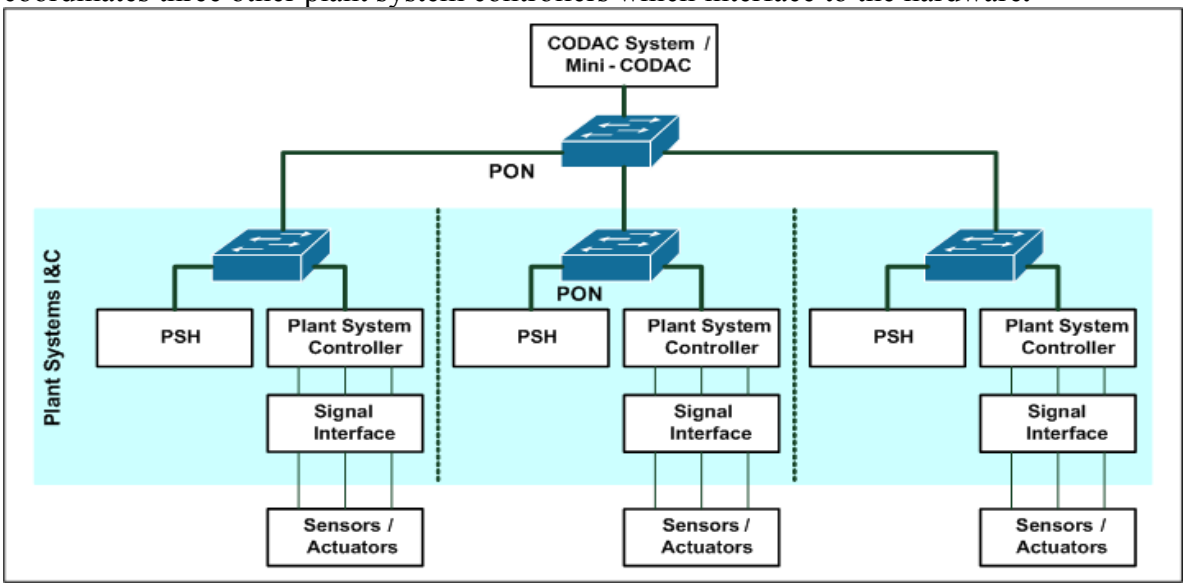

Figure 4-2: Plant systems I&C physical architecture – example 2, loosely coupled system. Plant system is decomposed in three plant systems I&C. Supervision is delegated to the CODAC system / Mini-CODAC.

A plant system, as defined by the ITER Plant Breakdown Structure (PBS) and/or PA, may be decomposed in multiple plant system I&C. A plant system I&C consists of one and only one plant system host, one or many OSI layer 2 switches and one or more plant system controller(s) interfacing to actuators and sensors via signal interface(s). Plant system I&C components communicate with the CODAC System / Mini-CODAC over the Plant Operation Network (PON). CODAC System / Mini-CODAC implements the human-machine interface. Plant system controllers may be organized in a functional hierarchical manner using one plant system controller supervising the others (Figure 4-1). Alternatively, the plant system can be broken up in multiple plant system I&C, each with one PSH, delegating the supervisory function to the CODAC System / Mini-CODAC (Figure 4-2). The former approach is preferred for closely coupled systems, while the latter is preferred for loosely coupled systems. The latter architecture has several advantages in modularity, testing and integration. Plant system I&C architecture is elaborated in supporting document [SD1] .

The following sections describe software components developed by IO and supplied to plant system I&C developers. These software components are delivered in a package called CODAC Core System and comprise the software for PSH, High Performance Network (see section 5) interfaces and Mini-CODAC with the tools required for PSH configuration and for development of applications in the Mini-CODAC environment. CODAC Core System is released at regular intervals, typically once per year, throughout the construction of ITER. IO is committed to provide all required support infrastructure, documentation, workshops, training etc. to promote this CODAC Core System approach to plant system I&C development.

4.2.1. Mini-CODAC

Mini-CODAC is a system supplied by IO in order to provide the plant system I&C with a subset of the CODAC system functions before the plant system is integrated into the CODAC system infrastructure on-site. The configuration of the Mini-CODAC is under the responsibility of the plant system I&C supplier [TBC]. Mini-CODAC is not a part of the plant system I&C and it is replaced by the CODAC system when the system is integrated on site.

The purpose of Mini-CODAC is to provide a software environment to prepare integration with the CODAC system and to provide a test tool for FAT and SAT. The subset of functions implemented by Mini-CODAC allows the development and test of the plant system I&C before integration.

The primary functions of Mini-CODAC are:

- Development and test of the HMI allowing commands to be issued to the plant system I&C and to visualize the plant system I&C state and status.
- Handling and visualization of the alarms generated by the plant system I&C.
- Handling and visualization of the logging messages generated by the plant system I&C.
- Storage of the data generated by the plant system I&C and access to this data.
- Development and management of test software.
- Development and testing of the supervisory functions to be integrated in the CODAC System.
- Generation for test purposes of software events transmitted to the plant system I&C from the CODAC System.
- Generation for test purposes of data flows transmitted to the plant system I&C from the CODAC System.
- Management and storage of the configuration data for the plant system I&C.
- Data visualization (real-time and history).

[R52] Mini-CODAC shall be used for FAT as a substitute for the CODAC System.

[R53] OSI layer 2 switch is the only plant system I&C component that has a physical interface with Mini-CODAC.

[R54] The physical interface of the plant operation network between Mini-CODAC and the plant system I&C shall be a conventional Gigabit Ethernet connection.

[R55] The functional interface of the plant system I&C shall be tested with the Mini-CODAC.

[R56] The software components delivered with the plant system I&C that will be integrated into the CODAC System shall be tested with Mini-CODAC.

4.2.2. Plant System Host

PSH is a standardized computer supplied by IO that is a component of the plant system I&C. PSH is connected to the Plant Operation Network. PSH is designed for implementing the standard functions for plant system I&C, not for plant-specific programming.

The primary functions of PSH are:

- Handle commands from the CODAC system / Mini-CODAC and dispatch commands to the plant system controllers.
- Monitor the plant system state and status and update this in the CODAC system / Mini-CODAC.
- Transfer alarms from the plant system I&C to the CODAC system / Mini-CODAC.
- Transfer logging messages from the plant system I&C to the CODAC system / Mini-CODAC
- Distribute software events from the CODAC system / Mini-CODAC to the plant system controllers and vice versa.
- Monitor its own state and update this state in the CODAC system / Mini-CODAC.
- Reconfigure the plant system I&C when in maintenance mode.

[R59] Each plant system I&C shall have one and only one PSH.

[R60] The PSH shall be connected to the OSI layer 2 switch.

[R61] The PSH shall be integrated into the plant system I&C.

[R62] 5U [TBC] in a 19” rack and 500W power supply shall be allocated for the PSH in one of the plant system I&C cubicles.

[R63] The interface between the PSH and the plant system controllers shall be Ethernet.

[R64] The PSH shall be configured by the plant system I&C designers using the software kit supplied by IO.

4.2.3. Plant System Controllers

Plant system controllers are local units in charge of implementing the functional and physical part of the control and data acquisition of the plant system. All plant system controllers include a processor and I/O interfaces, as required. I/O interfaces are either I/O embedded within the controller hardware system, or remote I/O, interfaced with a field bus.

Plant system controllers are split into two categories: slow controllers and fast controllers. Performance is a discriminating criterion but the main characteristic of the slow controllers is that they are only using COTS industrial components (Programmable Logic Controllers, PLC).

It is planned to have an overlap in the performance ranges of the two categories of controllers. It is assumed however, that only fast controllers implement control loops or data acquisition faster than 100 Hz.

It is recommended that the usage of slow controllers is maximized.

4.3. I&C Naming Conventions

See [SD3] for details on signal and variable naming conventions.

4.3.1. Components naming convention

[R65] A convention for uniquely identifying parts and components for ITER is defined in the ITER Numbering System for Parts/Components, see [RD3]. This naming convention is applicable to any component of the plant system I&C.

This reference consists of three identifiers separated by the separator (hyphen "-"):

- Plant Breakdown Structure (PBS) Identifier: PPPPPP;
- Component functional category designator: TTT;
- Sequential Number: NNNN.

Therefore, the format of any ITER component name is: **PPPPPP-TTT-NNNN.**

The PBS Identifier (PPPPPP) shall identify the plant system PBS level 3 to which the component belongs.

The Function Category Designator (TTT) shall designate the type of component and shall belong to the list of types defined in the ITER Function Category and Type of [RD17].

The Sequential Number (NNNN) shall be allocated by IO so that the complete identifier (PPPPPP-TTT-NNNN) is unique within the whole ITER plant.

4.3.2. Signals naming convention

[R69] Any I&C signal name is made of two identifiers separated by a colon ":". The first is the identifier of the component producing the signal; the second is the identifier of the signal within the component:

Signal Name = Component Identifier : Signal Identifier

[R66] The component naming convention, as defined in the previous section, applies to the component identifier.

[R67] The signal identifier shall satisfy the following naming convention: The signal identifier is made of three parts:

- The first part AAAA identifies the sensor/actuator class using the ISA-5.1-1984 (R1992) standard for instrumentation symbols and identification, see [SD3] for details.
- The second part RRRR is optional and used to identify several sensors/actuators of the same class within the component.
- The third part SSS is used to identify the signal type, see [SD3] for details.

The format of the suffix is then: AAAA[RRRR]-SSS, RRRR being an alpha-numeric string of maximum 4 characters and SSS an alphabetic string of 3 characters introduced by a hyphen character "-".

Therefore, the signal name format is: **PPPPPP-TTT-NNNN:AAAA[RRRR]-SSS**

4.3.3. Function identifier

A Functional Breakdown Structure (FBS) is defined for the whole ITER plant. See [RD20].

[R68] The plant system function identifier shall be based upon a Functional Breakdown Structure (FBS) and satisfy the following naming convention:

- Within each hierarchical FBS level, a plant system function is identified by an alpha-numeric string of maximum 4 characters: FFFF. This string identifier shall be unique within the considered FBS level, and mnemonic names are recommended (e.g. DIAG for PBS55, MAG for PBS11, CWS for PBS26.).
- The full plant system function name consists of all required function identifiers separated by the separator (hyphen "-").

Therefore the plant system function format is: **FFFF-FFFF-FFFF** for a level 3 function.

4.3.4. Variable naming convention

[R153] By analogy with the signals, the convention for naming variables is:

Variable Name = Function Identifier : Variable Identifier

[R154] The variable identifier is a free string of 16 characters maximum VV…VV, provided the full name including the function identifier is unique within the whole ITER plant.

Therefore, the variable name format is: **FFFF-…….FFFF: VV….VV**

For variables directly reflecting data from I&C signals, it is recommended but not mandatory that the variable Identifier VV….VV would satisfy the following naming convention:

- The variable Identifier is made of two parts separated by the separator (hyphen "-"):
- The first part is the component identifier without the PBS reference PPPPPP.
- The second part is the signal identifier without the SSS suffix for signal type.

Thus the complete variable identifier format would be: TTTNNNN-AAAA[RRRR] for variable reflecting signals.

4.4. Plant System I&C Software Specifications

4.4.1. Functional requirement

[R70] The plant system I&C shall implement the following functions:

- Process monitoring and experimental data processing
- Process control
- Alarms
- Error and trace logging
- System management
- Generation of data streams
- Configuration
- Management of events

Process monitoring and experimental data processing:

[R71] All information issued from the process shall be supplied with an identifier, a time stamp and a quality flag including error identification in case of error. Units and full name of the information may not be required in the dynamic data if defined in the associated static meta-data.

[G4] It is recommended that conversion from raw data to engineering data (scaling) is done as near as possible to the process.

[G5] It is recommended that time stamping is done as near as possible to the process.

[R73] Calibration factor and conversion formula shall be configurable.

[G12] Process information shall be transmitted as raw data and/or as engineering data whenever possible (not applicable to PSS).

Process Control:

The plant system receives low level commands as well as high-level commands from the CODAC system that shall end up as multiple commands towards the process. It is the responsibility of the plant system I&C to split the high level command into multiple unitary commands, to control their execution and to send back an execution status to the CODAC system. For state machines, the plant system I&C shall send an execution status for each transition back to the CODAC system.

[R77] The plant system I&C shall be able to autonomously maintain safe operation of the plant system in case of loss of central I&C systems or I&C networks.

[R78] The start-up strategy shall take into account the current state of the process and the presence/absence of the CODAC system (not applicable to PIS and PSS).

[R79] The plant system I&C shall be able to manage different control types such as the state machines, the high level commands issued by the CODAC system towards the process, the unitary commands for test purposes, the plant system local control loops and the configuration commands from the CODAC system.

[G6] Control loops shall be optimized in order to reduce the frequency of activation of the final control devices (not applicable to PSS).

Alarms:

The purpose of the alarm system is to provide information to the operators through a Mini-CODAC / CODAC system service for fault diagnosis and correction. A plant wide alarm handling policy will be put in place to handle the alarm situations and to undertake corrective action to allow normal and safe operation to continue.

[R81] The plant system I&C shall maintain the status of all active alarms and shall transmit any change of this status (alarm raised, alarm cleared).

[R82] The alarm shall carry information to the CODAC system to enable alarm reduction (not applicable to PSS).

[R83] The alarms shall be raised in accordance with the operating states. This is needed to properly qualify alarms which are not significant in a given situation (not applicable to PSS).

[R84] An alarm shall contain:
- A timestamp;
- A severity;
- An alarm identifier [TBD];
- A process part identifier raising the alarm (source);
- A text describing the condition that caused the alarm to be raised.

The severity qualifier shall have one of the following values:

Minor:

The fault does not prevent the plant system from satisfying the current operational requirements, possibly with limitations. If not handled, the fault may evolve into a major alarm.

Major:

The fault prevents the plant system from satisfying the current operational requirements. If not handled, other faults may occur.

Error and trace logging:

The logging function consists of a set of messages and each message corresponds to the record of an event. These events could be normal events or abnormal events. Mini-CODAC / CODAC system will

supply a service to handle log messages.

[R85] A log message shall include:
- A time stamp;
- A process identifier according to the naming scheme;
- A text explaining the event;
- A message level (debug, info, warning, error).

[R86] The following log messages shall be recorded with their qualifiers in the logging system:
- All timing, PSH, plant system Controller, PLC or embedded system events or state changes;
- All operations related to data configuration (creation/modification/deletions of variables, threshold change);
- All transitions in operating states;
- All commands sent by central I&C systems;
- All binary state changes (e.g. valve opened or closed);
- All events concerning an analogue variable or a group of analogue variables (threshold overshooting, out of range, discrepancy);
- All variable validity changes;
- All actions done locally by operators (log on/off, local commands, variable tagging or forcing);
- All local alarm acknowledgements.

In the event of failure of any sensor or equipment or a software glitch, the error shall be detected and an error message shall be generated and communicated to the CODAC system.

System Management:

[R87] Remote control functions shall be available (reboot, configure, start, stop, switch to local / central control mode). These functions shall comply with the safety rules of the ITER site.

[R88] The plant system I&C shall be monitored in a homogeneous way in order to diagnose faults and facilitate fast recovery.

[R89] The monitoring function shall encompass monitoring of plant system I&C functions and equipment.

[R90] The plant system I&C shall be synchronized with ITER central time reference.

[R91] The equipment to be monitored shall include at least:
- Environment within cubicles;
- PSH hardware / software;
- Plant system controllers;
- I&C networks;
- CODAC system interface (in order to take local control of the plant system if there is a CODAC/CODAC network failure).

[R92] Any monitored equipment and function shall supply status information with one of the following exclusive values:
- Fully operational;
- Partly operational (which means with limitations with respect to design parameters – performance, RAMI, OLC, …);
- Not operational.

[R93] Information on equipment performance shall be monitored. Performance information such as field bus, CPU load, memory usage or network bandwidth utilisation shall be recorded for capacity planning.

[R94] The plant system I&C events shall be reported in the logging and also alarms. This information shall also be propagated to the CODAC system.

[R95] SNMP probes shall be used for I&C networks in order to have a common central monitoring tool (not applicable to PSS) [TBD].

[R96] Plant system monitoring shall include self tests and live tests.

Generate Data streams:

The archiving of process information and system information is done by the CODAC system.

[R97] The plant system shall be able to send acquired or computed information to the CODAC system in either raw data or in engineering units with conversion formula.

Configuration:

[R98] Any configuration of parameters shall be possible with minimum disturbance to the rest of the plant system I&C and underlying process.

4.4.2. Non-functional Requirements

General

[G7] It is recommended that all the software developed is designed to be data centric and not code centric for as far as practical. The settings which are expected to be changed, however rarely, in course of the plant system life time, should be made configurable without additional program recompilation and, preferably, without program restart.

Security

[R99] Access to the plant system I&C shall be through approved access points and shall be in agreement with the ITER site security requirements. This encompasses both the physical access and the access through networks.

[R100] Plant system I&C shall restrict access to authorized systems/people.

Performance

[R101] The availability of the plant systems I&C shall be compliant with the RAMI requirements of the plant system.

[R102] Each CPU's load ratio of the processor module shall be less than 50% on average in any 10s period.

[R103] Usage of main memory shall not exceed 50% in any period.

[R104] Network and bus loads shall not exceed 50% in any 10 seconds period and for Ethernet based on the CSMA/CD principle it shall not exceed 30%.

[R105] Additional reserve slots (not equipped) per backplane type shall be more than 20%.

[R106] Additional reserve I/O channels (not equipped) per type shall be more than 20%.

[R107] Additional reserve I/O channels (equipped) per type shall be more than 5%.

[R108] Duration for update of information from sensors to the Plant Operation Network shall be less than 1 sec (for PSS, this is only applicable to communication between PSS and CSS).

[R109] Duration for unitary commands from CODAC networks to actuators shall not exceed 1 sec.

[R110] Plant system I&C participating in the diagnostics or plasma feedback control shall have specific performance requirements (not applicable to PSS).

Availability

[G8] Hot swapping shall be used whenever it is required by the RAMI analysis of the plant system.

[G9] Redundancy shall be used whenever it is required by the RAMI analysis of the plant system.

I&C Self Diagnosis

[G10] Computers and equipment shall have provisions for self-diagnosis and provide a visual indication of the status on the local front panels and at the MCR. Computers and equipment should repeat self-checks at scheduled times.

4.4.3. Software Infrastructure

The software infrastructure for PSH and fast controllers is based on EPICS.

A software package, named CODAC core system, is distributed by IO for the development, test and operation of the plant system I&C. This package includes the required EPICS distribution.

Mini-CODAC and PSH are configured with the CODAC core system.

CODAC core system version 2 includes EPICS 3.14.12 or above.

[R155] CODAC core system version 2.0 or above shall be used on Mini-CODAC and PSH.

[R111] EPICS version R3.14.12 or above shall be used for PS fast controllers.

[R112] Communication with PS fast controllers shall use EPICS Channel Access.

4.4.4. Operating Systems

[R113] The Operating System of the PS fast controllers is Red Hat Linux 5.5 x86_64 or above, desktop with workstation option.

4.4.5. Programming languages and tools

Common to PS Slow and Fast Controllers

[R114] Computer Aided Design (CAD) tools shall be specified on the ITER project level as in Table 4-4-1.

Drawings	IO standard CAD tools
Mechanical drawings	CATIA V5
PFD drawings	SEE System Design
P&ID drawings	SEE System Design
Electrical drawings	SEE System Design
Functional analysis drawings	SEE System Design
Cubicle configuration drawings	SEE Electrical Expert

Table 4-4-1 CAD tools

[R115] The software versioning control tool shall be Subversion.

For PS Slow Controllers

[R297] The PLCs shall be programmed with the engineering software STEP7 v5.4 or above.

[SD10] provides guidelines for the user software engineering.

For fast controllers

The CODAC core system software includes the required environment to develop and test the fast controller software in a way that complies with the ITER requirements.

[R117] The Computer Aided Software Engineering tools are [TBD].

[R118] Fast controllers shall be programmed using the CODAC Core System distribution version 2.0 or above.

[R119] The FPGA technology, environment and tools are [TBD].

4.4.6. Self-Description Data

Plant system self-description data (SDD) is static configuration data which describes the plant system characteristics in a unified way in order to facilitate configuration of the central I&C systems' software for operation with the given plant system. SDD does not change during plant system operation. The data which has to be changed during operation shall not constitute a part of SDD but shall rather be made a part of PS run-time parameters. All the components of the PS I&C architecture shall be recorded in the SDD with their component naming and their characteristics.

SDD complement the software interface between central I&C systems and plant system I&C. It is created on a mini-CODAC system using the IO supplied tool, named SDD editor, which is part of the CODAC Core System, and it is stored into a database. The data created is then used to configure and program underlying PS I&C software and hardware.

[R120] The SDD consist of:

- Plant system I&C unique identification;
- Command list;
- Alarms list;
- Set-points list;
- Plant system I&C design limits;
- Physical (raw) signals list (I/O);
- Processed / converted signals list;
- Data streams list;
- Logging messages list;
- Definition of the plant system I&C state machine in accordance with the defined plant system operating states;
- Definitions of plant system I&C HMI;
- Plant system I&C constant values;
- Default values ("factory settings") for run-time configuration used for plant system I&C start-up;
- Identification of source codes and binary packages of the plant system I&C specific software;
- Documentation.

[R121] As a general principle, there shall be no hidden knowledge in the plant system I&C configuration. Whatever action is needed to configure the plant system I&C from scratch, it shall be an integral part of SDD (at least in the form of documentation).

The SDD is one of deliverables of I&C design and manufacturing phases. It is updated at the end of each phase of the lifecycle and uploaded to the ITER central SDD database. During the I&C operation and maintenance phase, the SDD master copy is kept in central I&C systems and may be modified through dedicated maintenance procedures. More information on the SDD lifecycle and contents is available in [SD4].

4.4.7. Operating States

ITER Plant operation is managed by system operating states, which are composed of three levels of hierarchy.

Global Operating States (GOS)

The GOS represent overall ITER plant system operating states defined by plant-wide operational activities associated with permission or prohibition of the plant operational activities. ITER GOS are defined in [RD18].

[S1] LTM – Long Term Maintenance;

[S2] STM – Short Term Maintenance;

[S3] TCS – Test and Conditioning State;

[S4] POS – Plasma Operation State.

Common Operating States (COS)

The common operating states are defined in [RD18]:

The COS is a state property that implements simple and synthetic state information common to all the PS so that they can be managed in a coherent way by CODAC system:

[S6] **Shutdown**

These states represent conditions in which a plant system I&C is declared as not operational. In these states the plant system I&C cannot present any active hazard to machine operation or control.

Absent – The plant system I&C is not present. It is either not installed, has been removed or disconnected from the machine and CODAC networks and cannot report any state;

Off – The plant system I&C is present, but it has informed the CODAC system that it is being switched off or rebooted and will not be able to report state;

Safe – The plant system I&C is in a well defined safe state. This may be trigged by the plant system safety system or at the instruction of the Central Safety System. (This state exists only where applicable);

[S10] **Not Ready**

These states indicate that the plant system I&C is operational but is not currently ready to start initializing.

Not Ready – The plant system I&C is operational but currently not ready to receive configuration, e.g. it may be performing system start-up tasks;

Local – The plant system I&C is undertaking some extended local preparation such as local control, conditioning or cleaning;

Fault – The plant system I&C has some internal fault, which must be corrected either manually or automatically;

[S8] **Ready**

Ready – The plant system I&C is ready to receive configuration and start initialising;

[S11] **Starting**

The plant system I&C has received a configuration command and will initialise itself. Under control of the CODAC system it will configure and prepare itself.

Initialising – The plant system I&C has received the command to initialise and configure itself according to a pre-defined set of parameters;

Initialised – The plant system I&C declares that it has initialised and configured itself according to the pre-defined set of parameters, and that it is ready to transfer to executing state;

Aborting – The plant system I&C has received a command to abort preparation and is executing any necessary actions under supervisory control. (This state exists only where applicable);

[S9] **Running**

The plant system I&C is executing. Pulsed systems are participating in a pulse sequence.

Executing – The plant system I&C in its running state, that is: normal operation for steady state systems;

Post-Checks – The plant system I&C has completed its execution. Pulsed systems are executing any necessary actions;

Terminating - The plant system I&C has received a command to terminate operations. Pulsed systems are executing any necessary actions;

[R122] Plant system I&C shall implement COS and PSOS.

4.4.8. Control mode

The control mode is a property that indicates whether or not the plant system is under (normal) **Central Control** via CODAC system from MCR or under **Local Control** using other interfaces. This property is managed by CODAC system and shall only be changed using formal operation procedures. Status of central control or local control shall be reported to the CODAC system.

Central Control:

Central control refers to the normal state in which the CODAC system is monitoring and supervising all plant systems.

[R123] Plant systems I&C shall always be in central control mode during normal operation.

[R124] Central control is always done through the CODAC system operator or plant system operator from the MCR.

Local Control:

Local control refers to control outside the MCR close to the plant system equipment. There are three cases of local control described below. The following apply to all cases.

[G11] Use of local control mode should be minimized as far as possible.

[R125] As far as possible, the monitoring of the plant system by the CODAC system shall be maintained when the plant system is in local control and the state of the plant system shall indicate the control mode to be local.

Mini-CODAC Control
Mini-CODAC control is only used during FAT and SAT. After integration, Mini-CODAC is replaced by CODAC system.

Local CODAC Terminal Control
This is the normal case for maintenance and troubleshooting. A CODAC terminal is connected to the network close to the plant equipment. Functionality is identical to central control.

Manual Control
Manual control refers to the ability of personnel local to the Plant System to control equipment of the Plant System independently of the Plant System I&C during maintenance of the equipment (e.g.,

using front panels).

4.4.9. Human Machine Interface

See [SD7] for details on human machine interface.

ITER Operator User Interface in the Main Control Room is based on the human-machine interface (HMI) running in the operator console and allowing the user to monitor, supervise and control the process.

The aim of the operator user interface is to facilitate effective operation and control of the plant systems. The primary aspects of this interface are graphics animated with feedback from the process which aids the operator in making operational decisions.

The focus here is on plant specific HMI for process control, even though the operator user interface will include other tools and facilities.

4.4.10. Alarm Handling

See [SD8] for details on alarm handling.

The fundamental purpose of alarm annunciation is to alert the operator to deviations from normal operating conditions, i.e. abnormal operating situations. The ultimate objective is to prevent, or at least minimize, physical and economic loss through operator intervention in response to the condition that generated the alarm. A key factor in operator response effectiveness is the speed and accuracy with which the operator can identify the alarms that require immediate action.

Alarm management is the application of human factors (or ergonomics) along with instrumentation engineering to manage the design of an alarm system to increase its usability and then its efficiency. Most often the major usability problem is that there are too many alarms presented during a plant system upset, commonly referred to as alarm flood.

With modern technology and industrial control systems such as EPICS, alarms are easy and cheap to configure and deploy, resulting in a combination of too much data combined with too little useful information.

The alarm philosophy is a guide that provides simple and practical guidance to plant system Instrumentation and Control (I&C) responsible officers and designers on how to design, develop, procure, operate and maintain an effective plant system alarm system.

Relevant rules apply for alarm handling:

[R361] The core principles underline this alarm philosophy are the following:

- Usability: the alarm system should be designed to meet user needs and operate within ergonomic requirements. This means that the support information alarm should:
  - Be relevant to the user's role at the time,
  - Indicate clearly what response is required,
  - Be presented at a rate that the user can deal with particularly when the plant system is upset or in an unusual condition,
  - Be easy to understand.
- Performance monitoring: the performance of the alarm system should be assessed during design and commissioning to ensure that it is usable and effective under all operating conditions. Regular auditing should be continued throughout the plant system life to confirm that good performance is maintained,
- Engineering: the design should follow structured methodology in which every alarm should be justified, documented and properly engineered. This initial investment in the

design should be sufficient to avoid the operational problems which result at the end in overall higher lifetime costs.

[R362] The purpose of ITER alarm system is to direct the operator's attention towards plant conditions requiring timely assessment or action. To achieve this goal, each alarm should be designed carefully according key principles:
- Each alarm should alert, inform and guide,
- Every alarm presented to the operator should be useful and relevant to the operator,
- Each alarm must have a defined operator action or response,
- The consequence if the alarm is not treated properly by the operator should be explicit,
- Appropriate time should be allowed for the operator to carry out a defined response,
- Each alarm must be rationalized prior to installation,
- Each alarm will be designed in accordance with given guidelines,
- Operator training is required for each alarm prior to installation,
- Alarm system performance must be monitored on a daily basis and corrective action taken when performance limits are not met,
- All additions, modifications, and deletions of alarms must follow a "management of change" procedure.

[R363] Number of configured alarms per operator shall be fewer than 100.

In steady operation, less than 1 per 10 minutes is recommended.

[R364] The number of alarms during the first 10 minutes of a major plant upset shall be less than ten.

[R365] The alarm priority distribution is MAJOR (20 %) and MINOR (80 %).

[R366] The average number of standing alarms shall be less than ten.

4.4.11. Plasma control data format

TBD

4.4.12. Plant system status format

TBD

4.5. Plant System I&C Hardware specifications

Each hardware component and instrument within the plant system I&C shall comply with these specifications.

4.5.1. Plant System Slow Controller

[R131] Slow Controllers shall use the ProfiNet field bus within their architecture up to the input/output card. The interface between PSH, PON and slow controllers shall be standard Ethernet.

[R132] Slow controllers shall use the Siemens Simatic S7-300 or S7-400 ranges.

[G52] It is recommended to select the equipment for the slow controllers the ITER catalogue [SD12].

[G50] Slow controller ordering shall be performed using the web tool mentioned in the ITER catalogue [SD12].

4.5.2. Plant System Fast Controller

[R133] Fast controllers shall be based on PCI Express I/O bus system.

To ensure interoperability it is recommended that Fast Controllers, I/O cards and field buses are selected from the ITER fast controller catalogue, as specified in [SD14]

4.5.3. I&C cubicles

[G51] To ensure compliance with volume allocation, monitoring and environmental constrains it is recommended that I&C cubicles are selected from the ITER catalogue for I&C cubicles and their components, as specified in [SD15]. The catalogue of standards applies on SCC and LCC or any combination.

[R157] The I&C cubicles shall be equipped with a monitoring system for doors, temperature and cooling monitoring and the monitoring system shall be interfaced to the plant system I&C.

[R161] The I&C cubicles shall comply with ITER EMC and radiation policy.

4.5.4. I&C signal cabling rules

[R159] The ITER cabling rules apply to signal cabling.

In addition, the [SD9] provides guidelines for signal cabling. The following rules apply for signal cabling:

[R312] A particular Plant System Equipment (PSE) signal shall not be connected to different plant system I&Cs. If requested by several plant system I&Cs, the corresponding data shall be transmitted through the CODAC networks.

[R313] Direct cabled connections of I&C signals from a plant system I&C to another plant system I&C inside the same plant system or between two different plant systems are not allowed.

[R314] If the PSE and the I&C cubicle connected to it are not in same building or are located in the same building but far away from each other, then an optical fibre device shall be used.

[R315] All the electrical cables used for transport of I&C signals will be single or multiple twisted pairs. Exceptions to this rule may apply for high frequency and high voltage analogue signals transmitted over a short distance. For such signals coaxial cables are recommended.

[G20] The full differential configuration is recommended for sensitive analogue signals within harsh environments.

4.5.5. Signal standards

This section gives the signal ranges which are used for the selection of the I/O boards of the I&C controllers in the ITER catalogues. These shall be considered as rules. Measurements/controls transmitted through field-buses from sensors/actuators are not considered in this section, since they have no impact on the selection of the controller hardware.

[R318] The ITER standards for I&C signals to be interfaced on ITER standard I&C controllers are as follow:

Analogue signals

Sensors

- Voltage range: 0V to +10V unipolar, -5V to +5V bipolar, -10V to +10V bipolar.
- Current range: 4mA to 20mA (16mA span). Signal polarity: positive with respect to signal common.

Actuators

- Output Current: 4mA to 20mA (16mA span). Signal polarity: positive with respect to signal common. Load resistance: 500 Ω max. Preferred 250 Ω.
- Output voltage: 0V to +10V unipolar or: -10V to +10V bipolar.

Digital signals

Sensors and actuators:

- Signal logic: positive for process control, negative for fail safe logics (interlocks and safety controls).
- Range: 24V DC referenced to plant system I&C cubicle earth. Maximum current depends on the galvanic isolation interface.

Temperature sensors

- Resistance thermometers: Pt100, 4 wires.
- Thermocouples: type K, type N.

A passive low-pass input filter is recommended for any temperature sensor.

Pneumatic signals

- Range: 0.2 to 1 bar for the current/pressure signal converters of pneumatic proportional control valves.
- 0 to 6-8 bars for the non-proportional control valves.

4.5.6. Bonding - powering of I&C cubicles

[R309] All I&C cubicles shall comply with ITER policy for maintenance procedures, powering and earthing cable identification.

[R310] The IEC 61000-5-2 technical standard is applicable for bonding of I&C components.

[R199] Plant system I&C shall use Class-II power supply interface defined in EDH, [RD4]. The I&C cubicles shall be powered by class II 230 V AC OL (Ordinary Load) single phase for conventional cubicles. The PIS and PSS will use Class II – IP or OL and may be backed up by Class IV, see chapter 6 and 7 of that document.

[R306] Use by temporary external equipment: **NO external equipment** should be plugged into the socket strips of the I&C cubicles. The exception to this is diagnostic and test equipment which may be connected for a limited time.

4.5.7. Environment, Location and Volume Management

The environment conditions are described in **Error! Reference source not found.** and in the building SRDs. CODAC space requirements are defined in [RD22]. The control room specifications are defined in [RD23].

[R178] The location of the instrumentation, cubicles and junction boxes shall depend on the functional requirements and shall be chosen so as to allow ease of access for initial installation and for later routine maintenance.

[R179] I&C equipment shall comply with the environment conditions of the location at which they will be installed. If not a suitable protection shall be defined for the I&C equipment. Such conditions concern magnetic fields, neutron flux, electromagnetic radiation, vibration coming from other equipment or seismic event, temperature and humidity.

[R180] Access to the instrumentation, cubicles and junction boxes shall be sufficient to allow installation of testing and calibration equipment.

5. INTERFACE SPECIFICATION BETWEEN PLANT SYSTEM I&C AND CENTRAL I&C SYSTEMS

5.1. Introduction

This chapter specifies I&C interface between central I&C systems and plant system I&C. Each plant system I&C shall follow the interface conditions described in this chapter. [SD5] provides software interfaces between CODAC system and plant systems I&C.

5.2. Functional Interface

The plant system I&C shall interface the following CODAC system functions:

- Plant system I&C supervisory control and monitoring;
- Management of operating states and parameters;
- Visualization;
- Alarm management;
- Events handling and synchronization;
- Logging;
- Plasma control (if applicable);
- Data archiving and retrieval;
- Configuration management.

Interfaces implemented by Plant System Host

[R184] The plant system I&C shall implement a functional interface to central CODAC systems compliant with the I&C requirements as expressed in the chapter 4 of that document

Interfaces implemented by CODAC Networks

[R193] The plant system I&C shall implement an interface (read and write data with sampling rates) to Synchronous Databus Network (see section 5.3.6) for plasma feedback control, if applicable.

[R194] The plant system I&C shall implement an interface to Time Communication Network (see section 5.3.7) if high accuracy synchronization is required.

[R196] The plant system I&C shall implement an interface to Audio-Video Network (see section 5.3.8) to communicate audio/video signals, if applicable.

Interface implemented by Central Interlock Network

[R197] The plant system I&C shall implement an interface (read and write data) to the central interlock system, if applicable.

Interface implemented by Central Safety Networks

[R198] The plant system I&C shall implement an interface (read and write data) to central safety systems, if applicable.

5.3. Physical Interface

5.3.1. Plant System Host

Plant system host is considered being a part of the plant system I&C (see chapter 4). There is one and only one PSH in a plant system I&C. PSH interfaces to the CODAC system.

5.3.2. Network Interface

Network interfaces provide the only physical interconnection between plant system I&C and central I&C systems. There are six networks (I&C Networks) (see Figure 5-1) defined for different purposes and with different performance. Networks are centrally managed by IO, including the assignment of network addresses.

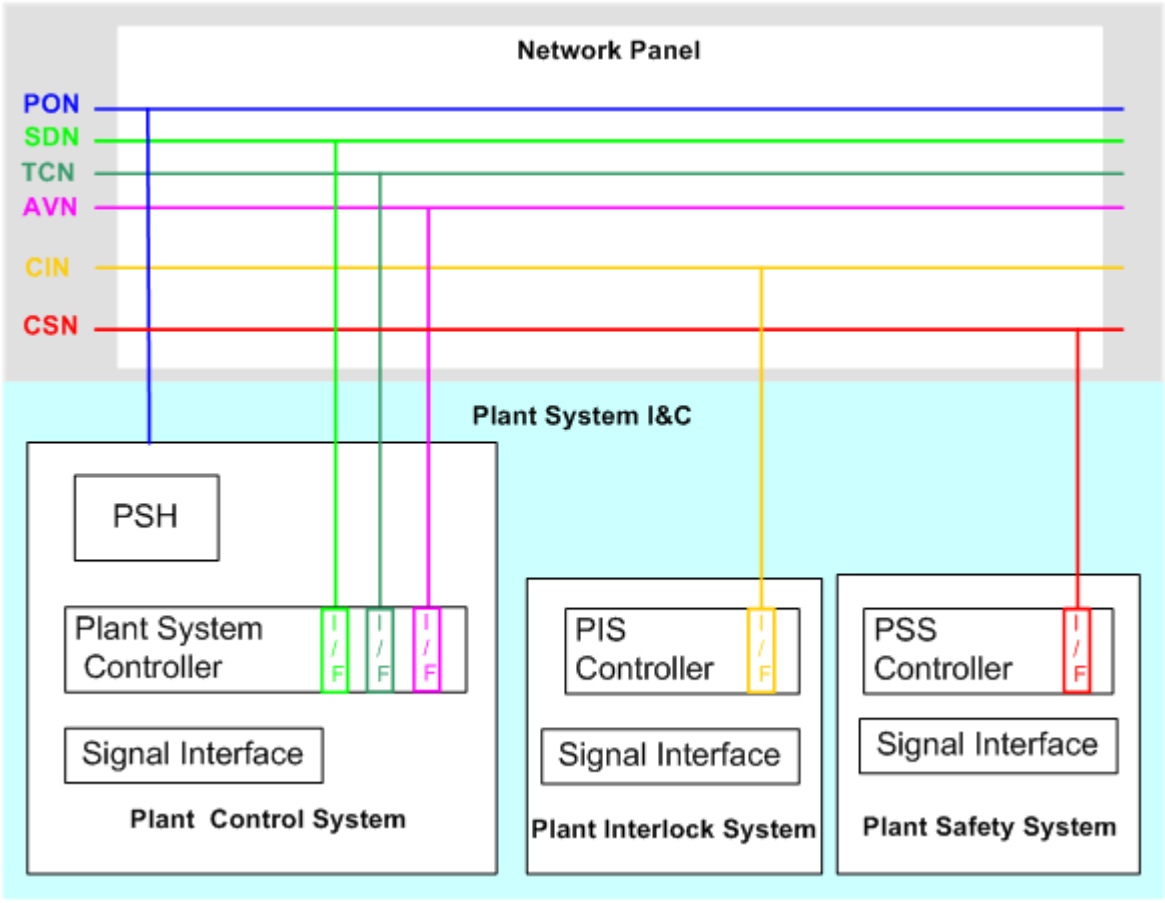

Figure 5-1: Network Interface between plant system I&C and central I&C systems

In accordance with the three tier separation concept I&C networks are divided into CODAC networks, the central interlock network (CIN) and central safety networks (CSN). CODAC networks, in turn, comprise the general purpose plant operation network (PON) and a set of specialized networks, called high performance networks. High performance networks include the Synchronous Databus Network (SDN), the Time Communication Network (TCN) and the Audio/Video Network (AVN).

There shall be no other external network connections to the Plant System I&C.

5.3.3. Network Hutch

A network hutch is a closed area equipped with heating, ventilation and air conditioning and suitable uninterruptible power housing a set of cubicles for CODAC, CIS and CSS, which accommodate the

active and passive components for central I&C networks. Most buildings on ITER site have one or several network hutches. The network hutch connects to the site network infrastructure and network panels.

5.3.4. Network Panel

A network panel is the passive wall mounted patch panel which is the physical termination point for CODAC and Central Interlock Networks. The CODAC and Central Interlock Network cables running from the nearest CODAC hutch will terminate in the network panel. There will be separate network panels for CODAC networks and Central Interlock Networks. Network panels are installed at strategic locations close to the plant system I&C cubicles in many buildings.

IO will provide the cables from plant system I&C cubicles to the network panel.

5.3.5. Plant Operation Network (PON)

The PON provides asynchronous interfaces between plant system I&C and the CODAC system.

[R201] Every plant system I&C shall be connected to PON.

5.3.6. Synchronous Databus Network (SDN)

The SDN provides the synchronous interface and events [TBC] required for fast plasma feedback control with sampling frequencies in the kHz range. Only plant system I&C participating in fast plasma feedback control shall be connected to the SDN. Plant system I&C may have multiple SDN network interfaces.

[R202] Only IO certified SDN interfaces shall be connected to SDN.

[R203] Specific hardware and software required by SDN interface will be supplied by IO.

[R204] The SDN interface is located in the plant system controller.

5.3.7. Time Communication Network (TCN)

The TCN provides project-wide time synchronization with an accuracy of 50 ns RMS [TBC]. The official ITER project time is UTC. Plant system I&C requiring high accuracy time synchronization shall be connected to TCN. Plant system I&C requiring less accuracy (10 ms RMS) can use network time protocol (NTP) over PON. Plant system I&C may have multiple TCN network interfaces. TCN may be used for pre-defined triggers [TBC]. TCN shall be based on the IEEE 1588 standard, as defined in [SD14].

[R205] Only IO certified TCN interfaces shall be connected to TCN.

[R206] Specific hardware and software required by the TCN interface will be supplied by IO.

[R207] The TCN Interface is located in the plant system controller.

5.3.8. Audio-Video Network (AVN)

The AVN provides communication for audio and video signals for scientific purpose (lossless transmission). Only plant system I&C generating audio and video signals shall be connected to AVN. Plant system I&C may have multiple AVN network interfaces.

[R211] Only IO certified AVN interfaces shall be connected to AVN.

[R212] Specific hardware and software required by the AVN interface will be supplied by IO.

[R213] The AVN Interface shall be located in the plant system controller.

5.3.9. Central Interlock Network (CIN)

The CIN provides communication between the plant interlock system and the central interlock system for inter-plant systems investment protection functions. Only plant system I&C participating in inter-plant system investment protection functions or having a local investment protection functions shall be connected to CIS via CIN.

[R214] PIS Controller shall interface to CIN if applicable.

5.3.10. Central Safety Networks (CSN)

The CSN provide communication between the plant safety system and central safety systems for inter-plant systems safety functions. Only plant system I&C participating in inter-plant system safety functions or having a local safety function shall be connected to the CSN.

[R215] PSS Controller shall interface to CSN if applicable.

6. INTERLOCK I&C SPECIFICATIONS

6.1. Introduction

This chapter complements Chapter 4 by stating the specific requirements for plant systems I&C which implement investment protection functions (interlocks) in the interlock system tier as described in Chapter 2. In order to discriminate among the various types of interlocking functions and to cover the wide range of possible application on ITER, this chapter, together with the interlock controls satellite documents, provides a set of guidelines and requirements:

- To guide in the identification and classification of the type of interlock functions (see also document Management of Local Interlock Functions, [SD22])
- To guide in the functional allocation to a set of standard conceptual architectures for the plant system interlock I&C (see document guidelines for the design of the PIS [SD16]).
- To confirm the requirements set in the previous chapters on the generic plant system I&C.
- To complement the generic plant system I&C requirements with additional requirements for the system specifications, for hardware components, for the software development and for the system interfaces. These are based on the results of the classification and the conceptual architecture assignment for the methodology to be used.

There are other actions for equipment protection naturally nested within the PS industrial controls and they are not discussed in this section. The recommendations provided in this section are based on the IEC 61508 standard.

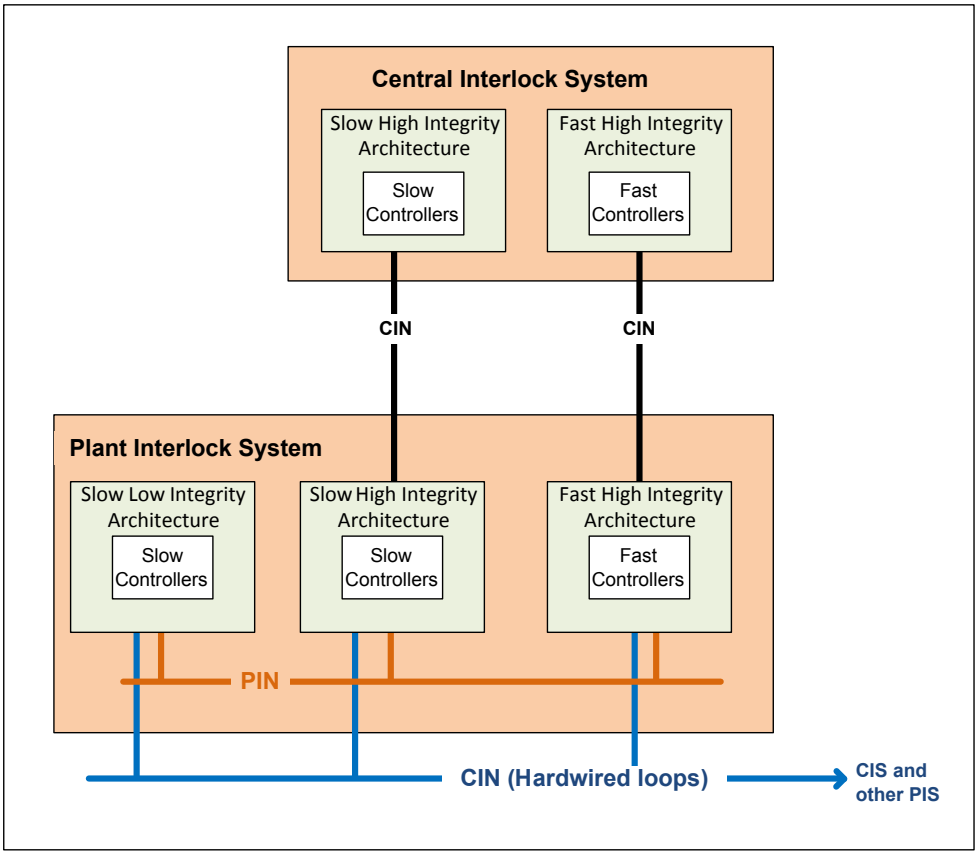

Figure 6-1: Standard Interlock I&C conceptual architectures

6.1.1. Identification and Classification of interlock functions

The aim of this section is to provide a set of guidelines to identify and classify the type of interlocking functions:

- With a description of the functions.
- With tables (IEC 61508) for a functional safety classification.
- With ranking of technical performance requirements.
- Considering environmental and physical constraints

[R216] Each function carried out by a plant system interlock I&C shall be defined, characterized and classified according to the guidelines given in this chapter and the associated related document or by an equivalent method.

[R217] Each function shall be described with at least the following fields:

- Protection/function name: define a name or unique identifier.
- Protection/function description: a textual summary description of the function.
- Sensors: indicate what type and number of measurements are required for the function
- Interlock logic: describe the interlock logic required for the function
- Actuators: indicate what type and number of actuators are required for the function
- Protection of machine: indicating which machine component is protected.
- Risk to protect: indicating which risk is being covered with this function.
- Risk description: a summary description of the risk being covered with this function.
- Risk class: Assign a class on the basis of the risk analysis.

[R218] Each interlock function shall be given a functional safety classification in the form of a safety integrity level (SIL) based on an established SIL assignment method (IEC 61508). In order to simplify the system as much as possible interlock functions are divided in: low integrity functions (SIL1 and SIL2) and high integrity functions (SIL3 and above)

[R219] The following technical performance requirements shall be identified for each function:

- RAMI parameters (Reliability, Availability, MTTR).
- Maximum execution time.

[R220] For each function, the list of environmental and/or physical constraints shall be identified:

- Space constraints.
- Ionizing radiation fields.
- Electromagnetic environment.
- ATEX requirements.

6.1.2. Rules for the requirement level allocation

The following recommendations are principally based on the standard IEC 61508 and standards IAEA NS G 1.1-3 and ISO 62061 / ISO 12100.

[R221] When a function is allocated to a level of requirements, then the whole equipment necessary to the achievement of this function shall observe the corresponding requirements.

[R222] If an equipment is involved in functions of different levels, then

- either the equipment shall be part of the highest level it contributes to
- or measures shall be taken to physically and electrically isolate the highest safety level part.

6.1.3. Instructions for the functionality guarantee

The following recommendations are based on the standards IEC 61508, IEC 61511 and IEC 61069.

Rules for the restriction of the complexity

[R223] The complexity of the I&C shall be restricted to the minimum required.

Containment of the most critical functions

[R224] The material organization of the I&C shall allow the containment of the most important functions for interlock within a perfectly identified physical entity.

Standardized architectures

A standardized architecture is defined for each integrity level (i.e. high and low)

[R225] I&C shall be built using standardized architectures that are made of standard equipment in order to meet the specified functional and reliability requirements.

[R226] This equipment (sensor, safety calculator, processing logic, network, actuator module…) shall be defined later in accordance with the functions to be performed. Slow Interlock PLCs have already been defined.

[G24] The standard equipment supports the basic mechanisms (failure processing, measurements safeguarding, availability checking…) and help them meeting the specified functional and reliability requirements.

Rules for the inviolability of the Interlock I&C

[R227] The plant system interlocks shall be implemented such that the risk of error during the following phases are reduced to a minimum:
- Routine operation
- Installation and commissioning;
- Periodic test operations;
- Corrective maintenance operations;
- Modifications of the installation.

[R228] The equipment shall be designed to restrict the interventions required on the equipment for maintenance or preventive tests to the minimum by anticipating at the design stage the necessary means and interfaces for the performance of these tests.

[G25] A modular structure of the Interlock I&C is recommended.

[R229] The equipment shall be fitted with specific access and intervention rules.

6.1.4. Instructions for reliability/availability guarantee

The recommendations provided in this section are based on the standards IEC 61508, IAEA NS G 1.1-3 and IEC 61069.

Rules relative to redundancy

[R230] The level of redundancy shall be set to reach the specified objectives for reliability and availability.

Rules relative to the achievement of quantitative objectives

Recommendations shall apply on a case by case basis as a function of the specified quantitative reliability objectives.

Behaviour incoherence

[R233] Incoherencies in behaviour (control or measurements conflicts) between redundant equipment shall be reported to the operators.

Rules relative to segregation

[R232] The structure of the I&C shall ensure that common modes are mastered.

[R235] If some equipment provides different level functions, some devices shall be implemented to avoid the highest level equipment being supplied with electric defects from the lowest level equipment.

[R236] The material segregation shall be associated with a functional segregation, in order to avoid supplying incorrect information from a lower to a higher level.

[R238] The redundant process lines:
- Shall be located in different areas and take into account the risks of mechanical stress, fire or flooding;
- If not, shall be fitted with protective equipment to ensure that the redundant process lines shall not be affected by the same aggravating factors;
- Shall be fitted with devices that avoid spreading electrical defects among redundant equipment;
- Shall be fitted with ancillary systems (power supply, cooling device) which have compatible redundancy levels.

[R292] An incident shall not lead to the loss of several redundant process lines.

Rules for the detection of failures

[R240] The diagnostic coverage shall be defined in accordance with the safety failure fraction required for the safety integrity level of the equipment. (See IEC 61508-2 §7.4.3.1.4).

6.2. Interlock I&C Architecture

6.2.1. Principles

A two-layer architecture has been adopted as the best solution for implementing the interlock functions at ITER.

The central interlock functions are coordinated by the CIS via the Central Interlock Network (CIN) and implemented together with the PIS of the affected plant systems.

The local interlock functions are implemented and coordinated by the PIS of the plant system concerned using only its own network, sensors and actuators. The CIS is not directly involved in the performance of the local protection functions and it is only informed of the plant system change of state.

Ideally, one plant system contains ideally only one Plant Interlock System which is solely responsible in the plant system for implementing the local and central machine protection function. The PIS controls and monitors the machine protection sensors and actuators via the Plant Interlock Networks and it constitutes the interface to the CIS via the Central Interlock Networks.

The CODAC IO team, which is responsible for the central interlocks, is in charge of ensuring the proper integration of both architectures (central and local) by applying the rules and guidelines defined in the Plant Control Design Handbook.

6.2.2. Functional Interface

Interface between PIS and CIS

[R325] Each PIS sends to the CIS:
- Its own state (COS and plant system operating states)
- The PIS commands sent to the process
- The signals used by CIS or other PIS for making decisions
- The information to be displayed on CIS operator desks
- The information enabling PIS monitoring and PIS data archiving

[R326] The CIS sends to the PIS:
- Manual and automatic central commands related to this PIS
- The Global Operation State (GOS)

[R327] Interface between PIS and CIS relies on CIN.

[R328] CIN is built redundant.

Timing interface

[R329] All the PIS are synchronized on an ITER central clock.

Inter-PS interface

[R330] Inter-PS communication between PS flows through CIS using CIN. There may be some hardwired links between Plant Interlock Systems for performance reasons: they will be dealt as deviations as stated in chapter 8. In that case, only binary information will be exchanged and the connecting network will be considered part of the CIS.

6.2.3. CIS functions in Mini-CODAC

[R331] The requirements set in section 4.2.1 do not apply. Development in progress in this area [TBD]. The Mini-CODAC will integrate CIS functions.

[R332] The functional interface of the plant system I&C shall be tested with the Mini-CODAC.

6.2.4. Plant System Host

The requirements set in section 4.2.2 do not apply. Developments in progress in this area are [TBD].

6.2.5. Plant Interlock System Controllers

[R243] Plant Interlock System Controllers shall comply with the assigned SIL level.

[R333] The slow architecture is based on COTS industrial components (Programmable Logic Controllers, (PLC).

[G60] It is assumed, that fast controllers will implement local control loops faster than 100 ms and central control loops faster than 300 ms. It is planned to have an overlap in the performance ranges of the two categories of architectures. Some architectures may require the usage of both slow and fast controllers.

6.3. Interlock I&C Naming Conventions

6.3.1. Components naming convention

The requirements set in section 4.3.1 apply.

6.3.2. Signals naming convention

The requirements set in section 4.3.2 apply.

6.4. Interlock I&C Software Specifications

[R244] Interlock I&C software shall comply with the assigned SIL level.

[R245] The software specification shall describe in quantitative terms the performance criteria (accuracy), the time constraints (response time) and the dimensional constraints (size of memory), with the tolerances and the possible margins.

[R246] The derived functions introduced during the software development process shall be identified. The consequences of the errors of these software functions shall be studied at the system level. Derived functions shall be functions not expressed in the system specification but necessary for the functioning of the system (For example: functions of communication inherent to the internal architecture of the system, functions of system breakdown detection,)

The recommendations provided in this section are based on to the standards IEC 61508, IEC 60671, IAEA NS G 1.1-3, IEC 62138 and IEC 60987.

6.4.1. Functional requirements

In addition to the requirements set in section 4.4.1, the followings also apply.

[R247] The Interlock I&C shall implement the following functions:

- Detect anomalous situations on the basis of simple or complex algorithms from the measurement of field values, the operational status of the monitored equipment and of the overall machine.
- Generate protection events (events and inhibits).
- Command protection actuators operated on the basis of a set of conditions and events.

6.4.2. Non Functional requirements

In addition to the requirements set in section 4.4.2, the following also apply.

[R248] The performance shall be compatible with the SIL level required by the interlock functions.

[R249] The I&C self diagnostics (Diagnostic Coverage) shall be compatible with the SIL level required by the interlock functions.

6.4.3. Software Infrastructure

The requirements set in section 4.4.3 are not applicable.

[R250] The software infrastructure for interlock I&C software shall comply with the assigned SIL level.

6.4.4. Operating Systems

The requirements set in section 4.4.4 are not applicable.

[R251] The operating systems for interlock I&C software shall comply with the assigned SIL level.

6.4.5. Programming languages and tools

The requirements set in section 4.4.5 are not applicable.

[R252] The programming languages and tools for interlock I&C software shall comply with the assigned SIL level. For the PLCs, the safety matrix and Continuous Functional Chart (CFC) shall be used.

6.4.6. Self description data

The requirements set in section 4.4.6 apply.

[R334] Tools for configuring Plant System I&C functions shall comply with the assigned SIL level.

6.4.7. Operating States

The requirements set in section 4.4.7 apply.

[R335] The Interlocks can be enabled or disabled independently of the Plant System Operating States of the rest of the I&C and the ITER Global Operation State (GOS)

6.4.8. Control mode

The requirements set in section 4.4.8 are not applicable.

6.5. Interlock I&C Hardware Specifications

Each hardware component and instrument within the interlock I&C shall comply with these specifications.

The recommendations provided in this section are based on the standards IEC 61508, IEC 60987, IAEA NS G 1.1-3 and IEC 62138.

6.5.1. Plant Interlock System Slow Controller

The requirements set in section 4.5.1 are not applicable.

[R253] The plant interlock system slow controller shall comply with the assigned SIL level.

[R254] Slow controllers shall use the Siemens Simatic S7-400 FH range for both SIL-2 and SIL-3 PLCs.

[R255] SIL-2 and SIL-3 slow controls shall use the ProfiSafe profile on field buses.

It is recommended to select the equipment for the SIL-2 and SIL-3 slow controllers the ITER catalogue [SD12].

6.5.2. Plant System Fast Controller

The requirements set in section 4.5.2 are not applicable. Development is in progress in this area [TBD].

6.5.3. Plant Interlock System Network

[R257] The plant interlock system network shall comply with the assigned SIL level.

[R336] Communication within the PIS slow controllers uses the ProfiSafe field buses.

[G61] Whenever communication is required between slow and fast controllers, it shall preferably use **hardwired links with electrical insulation.**

6.5.4. I&C Cubicles

The requirements set in section 4.5.3 apply.

6.5.5. I&C signal cabling rules

The requirements set in section 4.5.4 apply.

6.5.6. Signal Interface

The requirements set in section 4.5.5 apply.

6.5.7. Bonding – powering of Interlock cubicles

The requirements set in section 4.5.6 apply.

6.5.8. Environment, Location and Volume Management

The requirements set in section 4.5.7 apply.

7. OCCUPATIONAL SAFETY I&C SPECIFICATION

7.1. Introduction

This chapter complements Chapter 4 by stating the specific requirements for plant systems I&C implementing safety functions in the safety system tier as described in Chapter 2.

Safety functions fall into 3 categories:

- The Nuclear Safety
- The Occupational Safety
- The Personal Access Safety

This chapter addresses Occupational Safety and Personal Access Safety and does not deal with Nuclear Safety functions; they are described in [SD21]. In order to discriminate among the various types of safety functions and to cover the wide range of possible applications at ITER, this chapter provides a set of guidelines and requirements:

- To guide in the identification and classification of the type of safety functions.
- To guide in the functional allocation of the plant system safety I&C (see Figure 7-1) to a set of standard conceptual architectures.
- To confirm the requirements set in the previous chapters on the generic plant system I&C.
- To complement the generic plant system I&C requirements with additional requirements for the system specifications, for hardware components, for the software development and for the system interfaces. These are based on the results of the classification and the conceptual architecture assignment for the methodology to be used.

The recommendations provided in this section are based on the standard IEC 61508.

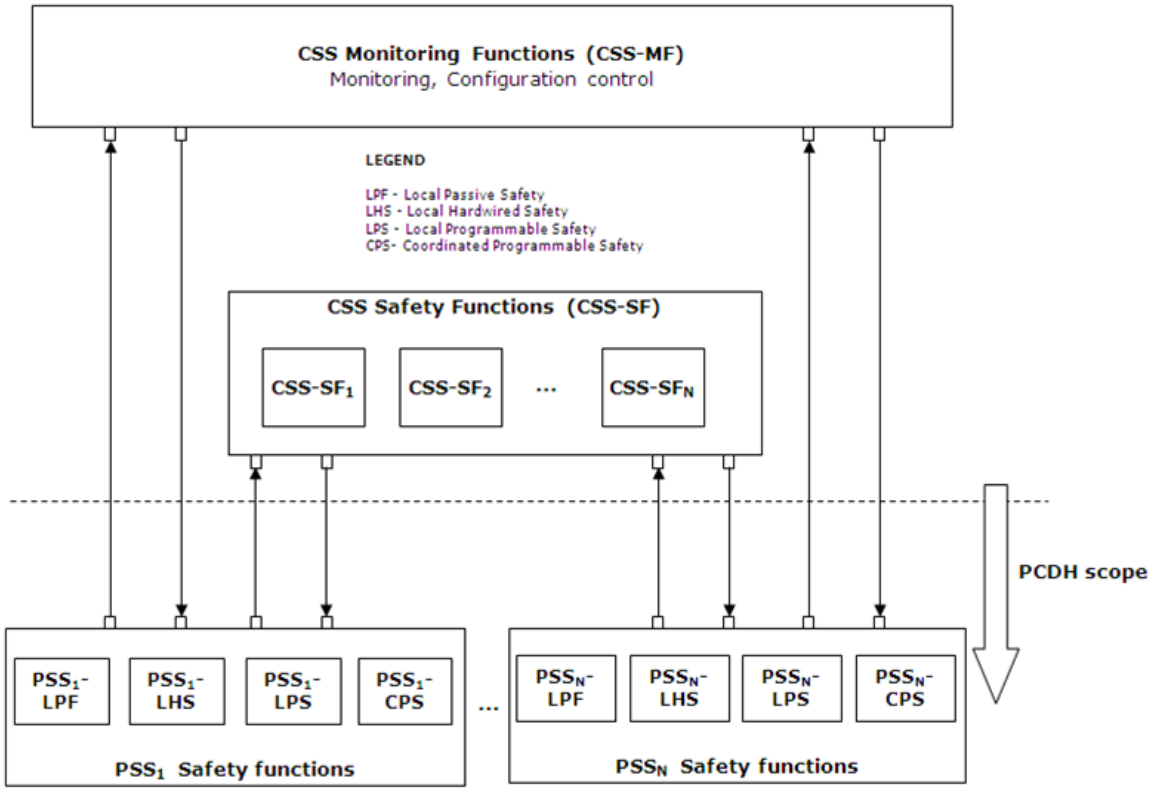

Figure 7-1 Standard Occupational Safety I&C conceptual architectures

7.1.1. Identification and Classification of Occupational Safety Functions

The aim of this section is to provide a set of guidelines to identify and classify the type of Safety functions:

- With a description of the functions.
- With functional Safety classification.
- With functional Safety allocation.
- With technical performance requirements.
- Considering environmental and physical constraints.

Each function carried out by a plant system Safety I&C shall be defined, characterized and classified according to the guidelines given in this chapter or by an equivalent method.

[R259] **Each function shall be described** with at least the following fields:

- Safety function name: define a name or unique identifier.
- Safety function description: a textual summary description of the function.
- Sensors: indicate what type and number of measurements are required for the function
- Safety logic: describe the logic required for the function
- Actuators: indicate what type and number of actuators are required for the function
- Risk to protect: indicating which risk is being covered with this function.
- Risk description: a summary description of the risk being covered with this function.
- Risk class: report the safety class assigned by the ITER Safety analysis (see below).

[R260] Each function shall be given a **safety classification** in the form of a Safety integrity level SIL1 to SIL3 (IEC 61508) based on one of the methods indicated in the standard or equivalent.

[R261] The following **technical performance requirements** shall be identified for each function:

- RAMI parameters (Reliability, Availability, Maintenability, Inspectability).
- Maximum execution time.

[R262] For each function, the list of **environmental and/or physical constraints** shall be identified:

- Space constraints.
- Radiation fields, integrated dose-rate.
- Magnetic fields
- Electromagnetic Interference.
- ATEX requirements.
- Ambient air conditions.

[R293] The Occupational Safety Plant Safety System (PSS-OS) shall provide I&C Safety functions for the protection of the people and the environment against all conventional hazards (toxicological, physical, electrical, cryogenic or other..), which it may produce in normal and abnormal circumstances.

[R294] The Plant Safety functions shall provide locally visual and audible warnings and alarms in the event of a hazard.

[R295] The Plant Safety functions shall communicate all hazards, warnings and alarms to the Central Safety System.

7.1.2. Rules for the requirement level allocation

[R263] All Safety functions, systems and equipment shall be designed on the basis of their SIL classifications (1, 2 or 3 considering the instructions of the IEC 61508 part-2).

[R265] When a function is allocated to a level of requirements, then all equipment necessary for the achievement of this function shall observe the corresponding requirements.

[R266] If equipment is involved in functions of different levels, then
- either the equipment shall be part of the highest level it contributes to,
- or measures shall be taken to physically and electrically isolate the highest Safety level part.

7.2. Occupational Safety I&C Architecture

The Safety I&C architecture for occupational safety shall be defined from a generic ITER plant system I&C template as indicated in section 4.2, which will be extended and adjusted according to the need for the particular plant system under consideration. In addition, the final I&C architecture shall consider the given set of standard conceptual architectures for the plant system Safety I&C for the Safety functional allocation.

These standard conceptual architectures are defined as follows (see Figure 7.1):

- **Type LPF** – Local Passive Safety function:
  These protections require no external equipment to carry out the Safety function (e.g., a spring loaded valve or a rupture disk).They are considered inside the safety I&C function when they are instrumented.
- **Type LHS** – Local Hardwired Safety function:
  These types of systems are very simple and are implemented using off-the-shelf non-programmable devices to carry out the Safety function within the same plant system (e.g., a machine emergency stop).
- **Type LPS** – Local Programmable Safety function:
  These types of systems are implemented using off-the-shelf programmable logic devices to carry out the Safety function within the same plant system (e.g., leak detection and isolation).
- **Type CPS** – Coordinated Programmable Safety functions:
  These types of systems participate in the implementation of Safety functions coordinated by the CSS that span across multiple plant systems. These types of systems are implemented using off-the-shelf programmable logic devices to carry out a part of the Safety function using external sensor/actuators connected via the CSS.

There might also be cases where the status of the LPF, the LPS and LHS are taken into account for the implementation of Safety functions coordinated by the CSS which span across multiple plant systems.

[R267] The plant system Safety I&C functions shall be allocated using the set of standard conceptual architectures given in this chapter.

[R268] Each plant system Safety I&C shall be represented by a composition of the set of standard conceptual architectures given in this chapter.

To avoid common mode failure communication redundant communication links between occupational safety I&C systems should be routed, as far as possible, via separated cable trays.

[R269] Occupational Safety part of the system must be separated from the nuclear safety part, and fulfil IEC 60709 and ITER requirements for separation of SIC functions. Occupational safety systems must be independent from conventional systems (independent cubicles, networks…). Cohabitation in same cubicles of OS and SR cat-C systems will be allowed

7.2.1. PSS functions testing

The requirements set in section 4.2.1 about interface with mini CODAC are not applicable and superseded by this section.

[R270] The different PSS-OS are not able to be interfaced with the mini-CODAC.

7.2.2. Plant System Host

The requirements set in section 4.2.2 are not applicable.

7.2.3. Plant Safety System Controllers

Section 4.2.3 is applicable with the restriction that only slow controllers are used.

7.3. Safety I&C Naming Conventions

7.3.1. Components naming convention

The requirements set in section 4.3.1 apply.

7.3.2. Signals naming convention

The requirements set in section 4.3.2 apply.

7.4. Occupational Safety I&C Software Specifications

[R272] The software specification shall describe in quantitative terms the performance criteria (accuracy), the time constraints (response time) and the dimensional constraints (size of memory), with the tolerances and the possible margins.

[R273] The derived functions introduced during the software development process shall be identified. The consequences of the errors of these software functions shall be studied at the system level. Derived functions shall be functions not expressed in the system specification but necessary for the functioning of the system (for example: functions of communication inherent to the internal architecture of the system, functions of system breakdown detection,…)

7.4.1. Functional requirements

The requirements and recommendations defined in section 4.4.1 apply, with the following additions and restrictions.

The PSS-OS shall implement the following functions:

- Perform occupational safety functions
- Safety input monitoring
- Maintenance & diagnostic
- Alarms
- Archiving
- System management

[R277] Once Occupational risk is eliminated, the operator has to reset the function to re-authorize the use of the actuator. **It is not possible to reset if the risk is not eliminated.**

Safety input monitoring:

All requirements apply to safety data.

Maintenance & diagnostic:

[R341] PSS-OS shall integrate system diagnostic functions with auto-diagnostic capabilities.

[R342] PSS-OS shall integrate signal diagnostic functions.

[R343] PSS-OS shall integrate maintenance override functions.

Alarms:

All requirements apply to safety data In addition:

[R344] PSS-OS communicate all safety events to the Central Safety System.

Archiving:

[R345] The logging data shall include:

- Safety physical parameter threshold exceeded.
- Sensors failure (open loop, short circuit)
- Maintenance override
- Redundant signals deviation
- Operator safety commands and reset
- Safety function activation & bypass
- Actuators failure (discrepancy command/status)
- I&C system failure (communication failure, hardware auto-diagnostic)
- I&C cubicle failure (high temperature, fan depowered, power supply failure…)

System management

Requirements defined in section 4.4.1 apply except R90: the Occupational Safety system will have its own time reference managed by CSS and sent to PSS, but limited to the safety system, and in compliance with IEC 61508.

[R346] System management shall be performed with safety dedicated safety engineering tools.

7.4.2. Non Functional requirements

The requirements and recommendations defined in section 4.4.2 apply, with the following additions and restrictions: R110 since diagnostic or plasma control are out of Occupational Safety scope.

[R347] The performance shall be compliant with the SIL level (IEC 61508) required by the Safety functions

[R348] The I&C self-diagnostics (Diagnostic Coverage) shall be compatible with the SIL level.

7.4.3. Software Infrastructure

The requirements set in section 4.4.3 are not applicable and superseded by the followings:

[R349] The software infrastructure for Occupational Safety I&C software shall be based on Siemens COTS operating systems and applications that comply with the assigned SIL level, up to SIL-3 (61508).

7.4.4. Operating Systems

The requirements set in section 4.4.4 are not applicable.

7.4.5. Programming languages and tools

Common and slow controllers requirements set in section 4.4.5 are applicable with following additional requirement:

[R350] Programming tools shall use Siemens dedicated engineering tools like Safety Matrix.

7.4.6. Operating States

The requirements set in section 4.4.7 apply with the restriction that:

[R351] Occupational Safety functions should be operational in all ITER operational states and could be disabled only when the absence of risk can be demonstrated.

7.4.7. Control mode

The requirements set in section 4.4.8 are not applicable.

7.5. Occupational Safety I&C Hardware Specification

Each hardware component and instrument within the Safety I&C shall comply with these specifications.

7.5.1. Plant System Slow Controller

The requirements set in section 4.5.1 are not applicable and are superseded by this section.

[R352] PSS-OS controllers shall use the Siemens Simatic S7-400 FH range for both SIL-3 PLCs. (IEC 61508).

[R354] PSS-OS controllers shall use the ProfiSafe on Profinet.

It is recommended to select the equipment for the SIL-2 and SIL-3 slow controllers the ITER catalogue [SD12].

7.5.2. Plant System Fast Controller

There are no Occupational Safety fast controllers.

7.5.3. I&C Cubicles

The requirements set in section 4.5.3 apply.

7.5.4. I&C signal cabling rules

The requirements set in section 4.5.4 apply.

[R357] The PBS in charge of the plant system shall perform the Cabling between PSS, process and up to the CODAC hutch.

7.5.5. Signal Interface

The requirements of section 4.5.5 apply, provided they comply with the IEC 61508 part-2.

7.5.6. Bonding – Powering of Safety cubicles

The requirements set in section 4.5.6 apply for bonding to earth..

[R356] PSS-OS cubicles shall be powered by two independent Class II-IP power supply and Class IV power supply.

7.5.7. Environment, Location and Volume Management

The requirements of section 4.5.7 apply provided they comply with the IEC 61508 part-2 and the following additional requirements:

[R358] Occupational Safety system components shall be accredited for to the identified environment al constraints and be installed in locations where environmental conditions are covered by this accreditation of the equipment. Even if the qualification process is less formal than the one for nuclear safety systems, the spirit is the same.

[R359] Where increased environmental hazards are imposed on I&C equipment by the Plant System design, it will be treated as an exception. PS-RO will define specific shielding and / or specific conditions and qualification criteria. In this case, the PS-RO is responsible for the qualification of the I&C equipment required for accomplishing Occupational Safety Functions.

7.6. Occupational Safety I&C lifecycle, and quality requirements

[R360] The plant safety system I&C lifecycle and development processes will follow the requirements of IEC 61508; and comply as far as possible with the plant system I&C lifecycle described in chapter 3.

7.7. Access safety

PSS may have to implement the local part of Local Access Safety I&C functions. The objective of those functions is to ensure the safety of the people, in some specific areas that generate safety risks and where “mechanical means” (key exchange systems, padlocks…) are not sufficient or suited:

- In the event of a door opening, stop plant system equipment to remove the source of safety risks,
- In very specific cases, ban access to an area, if there is a risk that people will not be protected from this hazard.

The Access Safety functions related to occupational risks are implemented in the Occupational Safety system using the same requirements. This section does not deal with Access Safety functions related to nuclear risks.

Example of access safety functions:

- Stopping hazardous Plant System Equipment in case of intrusion.
- Banning access on detection of a risk.
- Controlling safety airlocks.
- Interlocking safety access with same or other PSS.

8. DEVIATIONS POLICY

8.1. Deviations and Non-Conformances

[R281] Requests for deviations from and non-conformance with the requirements of the ITER Plant Control Design Handbook shall be made to the IO in writing following the procedures detailed in [RD6], [RD19] and [RD7]. The decision on the acceptance of the non-conformance report shall be made by the plant system central I&C responsible officer of the IO.

[R282] Any I&C equipment which is non-complaint to the PCDH requirements shall be subject to the Non-Conformance Report Process described in the ITER Deviations and Non-Conformances [RD7]. Every non-conformance shall be accompanied by an obsolescence management plan as suggested by IEC 62402.

[R283] The plant system responsible officer (and plant system I&C supplier, if appropriate) has to provide and pay for special integration and additional maintenance including spare parts for non-standard equipment.

8.1.1. Request for deviation and Report of Non-conformance

[R284] A deviation request shall include an alternative proposal including a justification of why I&C specifications in this document or procurement document were not followed, and a list of attachments which support the justification.

[R285] A non-conformance report shall include the original requirement, a description of the non-conformance, proposed remedial action, and a list of attachments which support the proposed remedial action.

8.1.2. Modifications to technical specifications

[R286] If the plant system responsible officer (and plant system I&C supplier, if appropriate) discovers that he had misinterpreted these technical specifications after signing the PA, this shall not be accepted as an excuse for deviations from it.

[R287] During execution of the procurement, all deviations from the technical specifications shall be reviewed and finally approved by IO.

[R288] IO shall consider the proposal on an expedited basis.

[R289] IO reserves rights to reject or accept such proposals.

[R290] IO reserves rights to modify these technical specifications during the execution of the procurement. The consequence of such modifications shall be mutually agreed between plant system I&C supplier and IO.

[G33] The plant system I&C supplier may suggest employing upgraded technology with respect to the technical specifications; these suggestions shall be reviewed by IO or by IO nominated parties; IO reserves rights to accept or reject the employment of upgraded technology.

9. APPENDICES

9.1. APPENDIX-A: Codes and Standards

Plant Control System	
Standard	**Title**
ISA-5.1-1984 (R1992)	Standard for Instrumentation Symbols and Identification
IEC 61158	Digital data communications for measurement and control
IEC 61000	Electromagnetic compatibility Requirement (includes IEC 61000-5-2)
IEC 62402	Obsolescence management
IEEE 802.3	Standards for Ethernet based LANs
IEEE 61850	Standards applicable to Power Station I&C components

Table 9-1-1: Codes and standards for Plant Control System.

Interlock	
Standard	**Title**
IAEA NS G 1.3	Instrumentation and control systems important to safety in nuclear power plants
IEC 60709	Suitable physical separation between systems
IEC 61069	Industrial-process measurement and control. Evaluation of system properties for the purpose of system assessment.
IEC 61508	Functional safety of electrical/electronic programmable electronic safety related system
IEC 61511	Functional safety instrumented system for the process industry sector
IEC/ISO 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

Table 9-1-2: Codes and standards for Plant Interlock System

Safety (Occupational and Access)	
Standard	**Title**
IEC 60709	Suitable physical separation between systems
IEC 61508	Functional safety of electrical/electronic programmable electronic safety related system

Table 9-1-3: Codes and standards for Plant Safety Systems.