Memorandum / Note

Guidelines for the Design of the Plant Interlock System (PIS)

This document sets the guidelines to be taken into account by the I&C plant system designers for the development and implementation of the Plant Interlock Systems (PIS) under their responsibility.

<table>
<thead>
<tr>
<th>Name</th>
<th>Action</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>Soni J.</td>
<td>27 Oct 2017:signed</td>
</tr>
<tr>
<td>Co-Authors</td>
<td>Gaikwad Y.</td>
<td>27 Oct 2017:signed</td>
</tr>
<tr>
<td></td>
<td>Pedica R.</td>
<td>27 Oct 2017:signed</td>
</tr>
<tr>
<td>Reviewers</td>
<td>Ciusa G.</td>
<td>27 Oct 2017:recommended</td>
</tr>
<tr>
<td></td>
<td>Fernandez-hernando J.</td>
<td>27 Oct 2017:recommended</td>
</tr>
<tr>
<td></td>
<td>L.</td>
<td>27 Oct 2017:recommended</td>
</tr>
<tr>
<td></td>
<td>Liu Y.</td>
<td>27 Oct 2017:recommended</td>
</tr>
<tr>
<td></td>
<td>Petitpas P.</td>
<td>27 Oct 2017:recommended</td>
</tr>
<tr>
<td></td>
<td>Prieto diaz I.</td>
<td>27 Oct 2017:recommended</td>
</tr>
<tr>
<td>Approver</td>
<td>Wallander A.</td>
<td>27 Oct 2017:approved</td>
</tr>
</tbody>
</table>

Document Security: Internal Use
RO: Fernandez-hernando Juan luis

Read Access
LG: CODAC team, LG: Interlock Gang, AD: ITER, AD: Only-staff, AD: External Collaborators, AD: IO_Director-General, AD: EMAB, AD: Auditors, AD: ITER Management Assessor, project administrator, RO, AD: OBS - Control System Division (CSD) - EXT, AD: OBS - CODAC Section (CDC) - EXT, AD: OBS - CODAC Sect...
### Change Log

**Guidelines for the Design of the Plant Interlock System (PIS) (3PZ2D2)**

<table>
<thead>
<tr>
<th>Version</th>
<th>Latest Status</th>
<th>Issue Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0</td>
<td>In Work</td>
<td>03 Sep 2010</td>
<td></td>
</tr>
<tr>
<td>v1.1</td>
<td>Signed</td>
<td>03 Sep 2010</td>
<td>Formalities.</td>
</tr>
<tr>
<td>v1.2</td>
<td>Signed</td>
<td>24 Sep 2010</td>
<td>One more chapter added: classification of machine protection functions. Version sent to I&amp;C IPT on Machine Protection</td>
</tr>
<tr>
<td>v2.0</td>
<td>Signed</td>
<td>10 Jan 2011</td>
<td>Version for PCDH v6 external review</td>
</tr>
<tr>
<td>v2.1</td>
<td>Signed</td>
<td>10 Jan 2011</td>
<td>Minor modifications (version, date)</td>
</tr>
<tr>
<td>v2.2</td>
<td>In Work</td>
<td>09 Feb 2011</td>
<td>Comments from IO and DAs reviewers included.</td>
</tr>
<tr>
<td>v2.3</td>
<td>In Work</td>
<td>09 Feb 2011</td>
<td>Comments from I&amp;C IPT reviewers included</td>
</tr>
<tr>
<td>v2.4</td>
<td>Approved</td>
<td>09 Feb 2011</td>
<td>Formal corrections.</td>
</tr>
<tr>
<td>v3.0</td>
<td>Approved</td>
<td>24 Jan 2013</td>
<td>Version for PCDH v7</td>
</tr>
<tr>
<td>v4.0</td>
<td>Approved</td>
<td>28 May 2014</td>
<td>New version before the iFDR and after results from R&amp;D contract and prototypes.</td>
</tr>
</tbody>
</table>
| v5.0    | Approved      | 27 Oct 2017| - Design guidelines for software architecture of Fast and Slow PIS is added  
|         |               |            | - Detail about the various configurations of Fast PIS hardware architecture is added  
|         |               |            | - Powering detail of Fast PIS architecture is added  
|         |               |            | - Cabling detail of Fast PIS I/O modules is added.  
|         |               |            | - Detail of Hardwired architecture (DLIB/BLIB) removed as this is falls under the CIS responsibility  
|         |               |            | - Chapter 10 Verification and Validation will be moved to another documents (Management of local interlock function)  
|         |               |            | - Some figures of slow architectures are updated /added  
|         |               |            | - ICS architecture updated and some changes made in document orientation |
Table of Contents

1 Introduction ..................................................................................................................................5
  1.1 PCDH context .....................................................................................................................5
  1.2 Document Scope ..............................................................................................................5
  1.3 Acronyms ...........................................................................................................................6
  1.4 Related documents ............................................................................................................7
2 Principles ...................................................................................................................................8
  2.1 Terminology .......................................................................................................................8
  2.2 Interlock Function Scope .................................................................................................10
  2.3 Interlock Function Integrity Levels ..................................................................................11
  2.4 Interlock Function Response Time ................................................................................12
  2.5 ICS Architecture ............................................................................................................13
3 PIS Architecture ....................................................................................................................15
  3.1 PIS Slow Architecture .....................................................................................................17
      3.1.1 Hardware Architecture ..............................................................................................18
      3.1.2 Network Architecture ...............................................................................................22
      3.1.3 Software Architecture ...............................................................................................24
  3.2 Fast Architecture .............................................................................................................25
      3.2.1 Hardware Architecture ..............................................................................................25
      3.2.2 Network Architecture ...............................................................................................28
      3.2.1 Software Architecture ...............................................................................................29
4 Interfaces ....................................................................................................................................31
  4.1 Interface between different PIS in same plant system ...................................................31
      4.1.1 Slow Architecture ......................................................................................................31
      4.1.2 Fast Architecture ......................................................................................................31
  4.2 Interface between different PIS of different plant systems ....................................31
  4.3 Interface between PIS and CIS ......................................................................................31
      4.3.1 Slow Architecture ......................................................................................................32
      4.3.2 Fast architecture .........................................................................................................32
  4.4 Interface between PIS and PON (PSH & PSCC) ............................................................32
      4.4.1 Slow architecture ......................................................................................................33
      4.4.2 Fast architecture .........................................................................................................33
  4.5 Interface between PIS and PSS ......................................................................................33
5 Powering ....................................................................................................................................36
  5.1 Conceptual principles .......................................................................................................36
  5.2 Slow Architecture .............................................................................................................36
      5.2.1 Powering of Controllers .........................................................................................36
      5.2.2 Powering of Peripheral Racks / Components .........................................................37
  5.3 Fast Architecture .............................................................................................................38
  5.4 Networks Products ...........................................................................................................39
  5.5 Other Components ..........................................................................................................39
6 Signal Cabling ........................................................................................................................39
  6.1 Slow Architecture .............................................................................................................39
      6.1.1 Digital Modules ..........................................................................................................39
      6.1.2 Analog Modules .........................................................................................................39
6.2 Fast Architecture .................................................................39
   6.2.1 Input Modules ..............................................................39
   6.2.2 Output Modules ..........................................................39
   6.2.3 Diagnostic Modules ......................................................39
   6.2.4 Communication Modules .............................................39

7 Sensors & Actuators .............................................................39
   7.1 Redundancy of Investment Protection: Sensors and Actuators ..........39
   7.2 Sharing of Sensors between PIS, PSCC and PSS ....................39
   7.3 Sharing of Actuators between PIS, PSCC and PSS .................39

8 Hardware ..............................................................................39
   8.1 Catalogues for PIS hardware components ............................39
   8.2 Cubicles .........................................................................39
List of Figures

Figure 1 : PCDH Document Structure __________________________________________________________5
Figure 2 : Local Interlock function __________________________________________________________10
Figure 3 : Central Interlock function __________________________________________________________10
Figure 4 : Time to respond to abnormal situations _______________________________________________12
Figure 5 : ICS Architecture _________________________________________________________________13
Figure 6 : PIS Architecture _________________________________________________________________16
Figure 7 : PIS Architecture having multiple Slow PIS controller ___________________________________17
Figure 8 : Standalone Architecture (One peripheral Rack) _________________________________________19
Figure 9 : Standalone Architecture (Two or more peripheral Rack) __________________________________19
Figure 10 : Standalone Architecture __________________________________________________________20
Figure 11 : Fully Fault Tolerant Architecture ___________________________________________________21
Figure 12 : Fully Fault Tolerant Architecture with Redundant Peripheral Racks ________________________22
Figure 13 : Network Architecture for Slow PIS ___________________________________________________23
Figure 14 : Software Architecture for Slow PIS Controller ________________________________________24
Figure 15 : General architecture for local function _______________________________________________26
Figure 16 : Central functions architecture for events ______________________________________________27
Figure 17 : Central Functions architecture for actions _____________________________________________27
Figure 18 : Fast architecture example implementing both central and local function ____________________28
Figure 19 : Fast PIS software architecture _____________________________________________________29
Figure 20 : Connection between PIS and PSH&PSCC ____________________________________________32
Figure 21 : Powering CPU Rack of Standalone PIS Architecture ______________________________________37
Figure 22 : Powering CPU Racks of Fully Fault Tolerant Architecture _______________________________37
Figure 23 : Powering IM Module in Peripheral Rack of Standalone Architecture ________________________38
Figure 24 : Powering IM Modules in Peripheral Racks of Fully Fault Tolerant Architecture _____________38
Figure 25 : Powering Fast Architecture __________________________________________________________39
Figure 26 : Powering Network Products ______________________________________________________39
Figure 27 : Selecting Applications for Digital Modules ___________________________________________39
Figure 28 : Application 3 for Digital Input Module - Safety Mode 3IL-2 ________________________________39
Figure 29 : Application 4 for Digital Input Module - Safety mode 3IL-2 with high availability ____________39
Figure 30 : Application 5 for Digital Input Module - Safety mode 3IL-3 ________________________________39
Figure 31 : Application 6 for Digital Input Module - Safety mode 3IL-3 with high availability ____________39
Figure 32 : External sensor supply for Digital Inputs _______________________________________________39
Figure 33 : Application 5 for Digital Output Module - Safety mode 3IL-3 _______________________________39
Figure 34 : Application 6 for Digital Output Module - Safety mode 3IL-3 with high availability ____________39
Figure 35 : Selecting Applications for Analog Modules ___________________________________________39
Figure 36 : Two-wire transducer, internal sensor supply _____________________________________________39
Figure 37 : Four-wire transducer, internal sensor supply _____________________________________________39
Figure 38 : Two-wire transducer, internal sensor supply with Module Redundancy _____________________39
Figure 39 : Four-wire transducer, internal sensor supply with Module Redundancy _____________________39
Figure 40 : Input Modules Cabling Schema _______________________________________________________39
Figure 41 : NI 9477 Output module cabling Schema ________________________________________________39
Figure 42 : NI9264 Diagnostic Module Cabling Schema _____________________________________________39
Figure 43 : NI9476 Diagnostic Module Cabling Schema _____________________________________________39
Figure 44 : NI9426 Diagnostic Modules Cabling Schema ____________________________________________39
Figure 45 : NI9401 DI Diagnostic Module Cabling Schema ___________________________________________39
Figure 46 : NI9401 DO Diagnostic Modules Cabling Schema _________________________________________39
Figure 47 : SPI Communication Cabling Schema ___________________________________________________39
Figure 48 : Manchester Code event transmission cabling schema ____________________________________39
Figure 49 : Manchester Code action receiver cabling schema _________________________________________39
Figure 50 : Sharing Sensor (Through Signal Duplicator at field) ______________________________________39
Figure 51 : Sharing Sensor (Through Interface within Controllers) _________________________________39
Figure 52 : Sharing Actuators ________________________________________________________________39
List of Tables

Table 1 : Classification of ITER interlock functions .................................................. 11
Table 2 : Hardware integrity: architectural constrains on type B components (Refer Table 3
from IEC 61508-2). ......................................................................................... 11
Table 3 : Codes and standards for Plant Interlock System ............................................. 15
Table 4 : Selection of PIS Hardware Architecture ....................................................... 16
Table 5 : IO modules for the different Fast architecture standard configuration ............. 25
Table 6 : Wiring scheme of SM 336; F-AI 6 x 0/4 ... 20 mA HART ................................ 39
Table 7 : Applications and Wiring Schemes for Analog Input Modules .......................... 39
1 Introduction

1.1 PCDH context

The Plant Control Design Handbook (PCDH) [RD1] defines the methodology, standards, specifications and interfaces applicable to the whole life cycle of ITER plant instrumentation & control (I&C) systems. I&C standards are essential for ITER to:

- Integrate all plant I&C systems into one integrated control system.
- Maintain all plant I&C systems after delivery and acceptance.
- Contain cost by economy of scale.

PCDH comprises a core document which presents the plant system I&C life cycle and recaps the main rules to be applied to the plant system I&Cs for conventional controls, interlocks and safety controls. Some I&C topics are explained in greater detail in dedicated documents associated with PCDH as presented in Figure 1: PCDH Document Structure. This document is one of them.

![Figure 1: PCDH Document Structure](image)

1.2 Document Scope

This document provides the guidelines to be followed by the plant system I&C designers for the hardware and software design of the Plant Interlock System (PIS) which implements investment protection functions and interfaces with the Central Interlock System (CIS).

This document does not provide the guidelines to be followed by the plant system I&C designers for the configuration and integration of the PIS. These are described in [RD2] Guidelines for PIS integration and configuration (ITER_D_7LELG4).
1.3 Acronyms

Table 1 show the acronyms used in this document. The relevant acronyms have been extracted from the complete list in PCDH.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>3IL</td>
<td>ITER Interlock Integrity Level ‘tril’</td>
</tr>
<tr>
<td>CHD</td>
<td>CODAC &amp; IT, Heating &amp; Current Drive, Diagnostics</td>
</tr>
<tr>
<td>CIN</td>
<td>Central Interlock Network</td>
</tr>
<tr>
<td>CIS</td>
<td>Central Interlock System</td>
</tr>
<tr>
<td>CNP</td>
<td>Communication Network Panel</td>
</tr>
<tr>
<td>MC</td>
<td>Manchester Code</td>
</tr>
<tr>
<td>CODAC</td>
<td>Control, Data Access and Communication</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-The-Shelf</td>
</tr>
<tr>
<td>CP</td>
<td>Communication Processor</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CSS</td>
<td>Central Safety System</td>
</tr>
<tr>
<td>DLIB</td>
<td>Discharge Loop Interface Box</td>
</tr>
<tr>
<td>EDH</td>
<td>Electrical Design Handbook</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>I&amp;C</td>
<td>Instrumentation &amp; Control</td>
</tr>
<tr>
<td>ICS</td>
<td>Interlock Control System</td>
</tr>
<tr>
<td>IO</td>
<td>ITER Organization</td>
</tr>
<tr>
<td>PCDH</td>
<td>Plant Control Design Handbook</td>
</tr>
<tr>
<td>PIN</td>
<td>Plant Interlock Network</td>
</tr>
<tr>
<td>PIS</td>
<td>Plant Interlock System</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>PON</td>
<td>Plant Operation Network</td>
</tr>
<tr>
<td>PS</td>
<td>Plant System</td>
</tr>
<tr>
<td>PSCT</td>
<td>Plant System Conventional Control</td>
</tr>
<tr>
<td>PSH</td>
<td>Plant System Host</td>
</tr>
<tr>
<td>PSS</td>
<td>Plant Safety System</td>
</tr>
<tr>
<td>RO</td>
<td>Responsible Officer</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>TCN</td>
<td>Time Communication Network</td>
</tr>
<tr>
<td>WinCC-OA</td>
<td>WinCC Open Architecture</td>
</tr>
</tbody>
</table>

Table 1: List of acronyms

Convention:
As explained in the document “Management of Local Interlock Functions”, safety is a term that should not be used when describing the interlock system. Nevertheless, this term will be used in the expression “safety-related” as opposed to normal/standard.
1.4 Related documents

[RD1] Plant Control Design Handbook (PCDH) (ITER_D_27LH2V)
[RD2] Guidelines for PIS integration and configuration (ITER_D_7LELG4)
[RD3] Management of Local Interlock Functions (ITER_D_75ZVTY)
[RD4] PIS Operation and Maintenance (ITER_D_7L9QXR)
[RD5] Central Interlock System (PBS-46) - Design Description Document (DDD) (QCH3GJ v2.2)
[RD7] Catalogue for I&C products – Cubicles (ITER_D_35LXVZ)
[RD8] IO cable catalogue (ITER_D_355QX2)
[RD10] Guidelines for I&C cubicle configurations (ITER_D_4H5DW6)
[RD11] IO cabling rules (ITER_D_335VF9)
[RD12] I&C Interlock Control System – Overall Quality Plan (ITER_D_75GBSW)
[RD15] Signal and Plant System I&C Variable Naming Convention (ITER_D_2UT8SH)
[RD16] ITER Numbering System for Components and Parts (ITER_D_28QDBS)
[RD17] EDH Part 1: Introduction (ITER_D_2F7HD2)
[RD19] EDH Part 5: Earthing and Lightning Protection (ITER_D_4B7ZDG)
[RD20] Integration Kit for PS I&C (ITER_D_C8X9AE)
[RD21] 1-S3-04 Dependability (RAMI, SIL) (ITER_D_RYXCZJ)
[RD23] ATN-ITER-DLIB-D12 Operation and Maintenance Manual (UL34AH)

[RS2] IEC 61511 Functional safety – Safety instrumented systems for the process industry sector
2 Principles

2.1 Terminology

- **Central Interlock System (CIS)**
  The **Central Interlock System (CIS)** together with CODAC and the Central Safety System (CSS), forms the ITER I&C Central Systems. The CIS is in charge of implementing the central protection functions via the Plant Interlock Systems (PIS) and, if required, some direct actuators. It also provides access to the local interlock data of the different plant Interlock Systems.

- **Plant Interlock Systems (PIS)**
  The **Plant Interlock Systems (PIS)** are part of the plant systems I&C. Each PIS provides local protection by implementing the local interlock functions of the corresponding plant system. Also, most of the PIS participate in the central interlock functions coordinated by the CIS. All the sensors and actuators involved in machine protection in ITER are connected to at least one PIS in their plant system. The PIS constitutes the interface between the CIS and the plant systems. Only plant systems I&C participating in inter-plant interlocks or implementing local investment protection functions are integrated in the Interlock Control System (ICS) architecture.

- **Central Interlock Network (CIN)**
  The **Central Interlock Network (CIN)** provides communication between the Plant Interlock Systems and the Central Interlock System for inter-plant systems investment protection functions. Only plant system’s I&C participating in inter-plant system investment protection functions, or performing local investment protection functions, are connected to the CIS via CIN.

- **Plant Interlock Network (PIN)**
  The **Plant Interlock Network (PIN)** provides communication between the controllers involved in the investment protection functions inside same plant system over a network bus. For the plant systems with more than one PIS, the PIN will be used to inter connect them. The PIN in one Plant System shall not be shared with other Plant Systems.

- **Interlock Control System (ICS)**
  The **Interlock Control System (ICS)** is in charge of the supervision and control of all the ITER components involved in the instrumented protection of the ITER plant systems. It comprises the Central Interlock System (CIS), the different Plant Interlock Systems (PIS) and its networks (CIN and PIN). The ICS does not include the sensors and actuators of the plant systems but controls them through PIS.

- **Interlock Event**
  This is the plant system state or combination of states involving different plant systems that triggers an action of the corresponding PIS and/or the CIS.

- **Interlock Action**
  These are measures or sequences of measures carried out by the CIS and/or the PIS to mitigate the risks following an interlock event. These protection actions are managed by the PIS when the measures are restricted to the plant system that generated the interlock event and by the CIS when different plant systems are involved.
• **Interlock Function**
  This is the logical description of the interlock actions following an interlock event. These functions are
classified into two categories as explained in 2.2 Interlock Function Scope

• **Critical Interlock Data**
  There are interlock signals performing the machine protection functions transmitted via the CIN and
PIN. They are divided into:

  o **Critical Automatic Data:**
    Data that is exchanged between CIS modules and PIS modules and is directly involved in the central
    interlock functions (events, actions) is called critical automatic data. This data is generated from
    logical / functional behaviour in controllers.
    Following are the examples of critical automatic data
    - Interlock events (Boolean). Example: wrong plasma current.
    - Interlock actions (Boolean). Example: Disruption Mitigation System trigger.

  o **Critical Manual Data:**
    Data that is exchanged between CIS modules and PIS modules and directly involves manual actions/
    triggering is called critical manual data. This data is generated from supervisory module and is
    transferred to controllers for performing further logic.
    Critical manual data includes:
    ▪ Override
    ▪ Interlock Configuration Data (Threshold Values etc.)

• **Non-Critical Interlock Data**
  Information treated by the PIS and the CIS which, although needed, does not directly participate in the
interlock function. For instance, the reset (unlatch) of interlock functions, actuators and sensors, or
the analog values of the temperature, pressure etc.
For example, in case of cryogenics, temperature values are used to decide whether the magnets can
be powered or not, these values are used in PIS to generate the interlock event. However, only the
interlock event (critical data) signal is routed to the CIS via the CIN while the temperature values (non
critical data) are sent to CODAC via the non-secured network.
2.2 Interlock Function Scope

- **Local interlock function**
  This is a machine’s protection function in which the interlock event and the interlock action(s) occur in the same plant system. The CIS does not play an active role in the protection function and it has been only informed of the change of state of the plant system. An interlock function involving different PIS of the same plant system is considered to be a local function.

- **Central interlock function**
  This is a machine’s protection function involving two or more plant systems. The interlock events are generated by the PIS and transmitted via the CIN to the CIS, which takes an interlock decision and dispatches the required interlock actions to the PIS of the other plant systems involved.
2.3 Interlock Function Integrity Levels

The integrity level is a functional safety profile defined for each interlock function in order to set the requirements for the risk reduction factor proportionally to the consequences of an event. The methodology to classify the machine protection functions is addressed in the document [RD3] “Management of Local Interlock Functions”

Following an interlock event (a state or combination of states that triggers an action of the corresponding safety system), an interlock function represents the logical description of the interlock actions taken (interlock action being the measure or sequence of measures carried out by the CIS and/or PIS to mitigate the risks following an interlock event).

Based on Table 1 [Error! Reference source not found.], classification of ITER interlock functions the different interlock functions will have to demonstrate their compliance with the corresponding requirement (in general 3IL-2 or 3IL-3).

Table 1: Classification of ITER interlock functions

<table>
<thead>
<tr>
<th>3IL</th>
<th>I&amp;C Implementation</th>
<th>Average probability of a dangerous failure on demand of the interlock function operating in low demand mode of operation (PFD_{op})</th>
<th>Average frequency of a dangerous failure of the interlock function [h^-1] operating in high demand mode of operation or continuous mode of operation (PHI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3IL-1</td>
<td>Conventional Control (no interlock)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3IL-2</td>
<td>Low integrity interlock</td>
<td>( \geq 10^{-3} ) to ( &lt; 10^{-2} )</td>
<td>( \geq 10^{-7} ) to ( &lt; 10^{-6} )</td>
</tr>
<tr>
<td>3IL-3</td>
<td>High integrity interlock</td>
<td>( \geq 10^{-4} ) to ( &lt; 10^{-3} )</td>
<td>( \geq 10^{-8} ) to ( &lt; 10^{-7} )</td>
</tr>
<tr>
<td>3IL-4</td>
<td>High integrity interlock with diversity (e.g., PLC + hardwired I&amp;C)</td>
<td>( \geq 10^{-3} ) to ( &lt; 10^{-4} )</td>
<td>( \geq 10^{-7} ) to ( &lt; 10^{-8} )</td>
</tr>
</tbody>
</table>

The CIS and PIS architecture will be implemented over complex electronic devices, so it shall be classified as type B subsystem according to IEC 61508-2.

The architecture constrains will be given by Table 2: Hardware integrity: architectural constrains on type B components. The Safe Failure Fraction (SFF), in conjunction with the Hardware Fault Tolerance (HFT), provides a general framework for the architecture to be implemented in the design.

For example, a component with a SFF of 70% will require a HFT of 1 to accomplish a SIL2 architecture, this is a 1oo2, 2oo3, etc. The final integrity will be checked with the determination of the probability of failure per each function.

Table 2: Hardware integrity: architectural constrains on type B components (Refer Table 3 from IEC 61508-2).

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance (see note 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>(&lt; 60 % )</td>
<td>Not allowed</td>
</tr>
<tr>
<td>(60 % ) – (&lt; 90 % )</td>
<td>SIL1</td>
</tr>
<tr>
<td>(90 % ) – (&lt; 99 % )</td>
<td>SIL2</td>
</tr>
<tr>
<td>(\geq 99 % )</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

More details / guidelines for Interlock Functional Integrity Levels and calculations can be found at [RD3].
The interlock system must be capable of detecting the process’s hazard and responding in time to prevent the hazardous event.

The response time for local functions, involving only one controller, is the total time taken for performing the following actions:

1. Sense the out-of-control condition
2. Digitally filter the input signal
3. Input process scan time
4. Local controller program scan time
5. Output process scan time
6. Digitally filter the output signal
7. Fully actuate the output device

If several controllers are involved in the interlock function (central functions or local functions involving several controllers), the communication time and the program scan time for each controller must be added. Within how much time the interlock system has to respond depends on the process’s dynamics and the conditions initiating its actions. The process safety time, which is a parameter available for any given safeguard, starts when it is required to take action and ends at the point where the event can no longer be mitigated.

This safety time is defined as the time period between a failure occurring in the process or the basic process’s control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed.

Given the degree of uncertainty in the process’s safety time, the interlock system should be capable of completing its action within one-half of the safety time allocated for the process. The time to react is defined for each interlock function, which determines the technology to be used for the implementation of it. The time to react is the time elapsed between the fault detection and action taken by the controller.
- **Slow Controller profile**
  If the time to react is longer than 100ms for a local function and around 300ms for a central function, standard industrial control solutions like PLCs are used. For slow controller, Siemens Controllers are proposed to be used. Details of these modules can be found at [RD6].

- **Fast Controller profile**
  If the time to react of a local function is shorter than 100ms, or shorter than 300ms in case of a central function, the protection functions are implemented on a faster FPGA-based NI **CompactRIO (cRIO)** controller or a hardwired solution. Details of these modules can be found at [RD9].

### 2.5 ICS Architecture

The ICS is formed of the Central Interlock System and the different plant interlock systems belonging to their plant system. The ITER control system team is in charge of the design and implementation of the CIS through the PBS-46 (CIS) RO. The design and implementation of the PIS fall under the responsibility of Domestic Agency’s and IO’s responsible officers for the corresponding plant system.

As the person responsible of the central interlock system, the PBS-46 RO is also in charge of ensuring the proper integration of both architectures (central and local) via the guidelines mentioned in this document.

Below Figure 5 shows the ICS architecture schema.
Two-layer architecture has been adopted for the implementation of the ICS: the central interlock functions are coordinated by the CIS via the CIN and implemented together with the PIS of the affected plant systems. The local interlock functions, on the other hand, are implemented and coordinated by the PIS of the affected plant systems, using only its own sensors and actuators. The CIS is not directly involved in the performance of local protection functions and it is only informed about the change of state of the plant system.

In both CIS and PIS cases mainly two architectures are used:

a) Slow Architecture
   For the local and central functions with response time requirements slower than 100 ms and 300 ms respectively, Siemens PLC based architecture will be used.

b) Fast Architecture
   For the functions with faster time requirements, FPGA based NI cRIO technologies will be used. This fast architecture is not required for all plant systems.

Communication between the same architectures (like communication in between only Fast architectures or communication in between only slow architectures) with different plant systems is carried out through the CIN (ideally through CIS modules).

Communication in between the same architectures and in same plant systems is carried out by the PIN. Communication between the different architecture (like Slow Architecture & Fast Architecture or vice versa) is carried out by hardware interconnections only. This is applicable for interconnections in between same plant systems as well as different plant systems.

Third architecture (i.e. Hardware Architecture mainly DLIB and BLIB) is not applicable for PIS. It is used for performing the magnet fast discharge, directly coordinating different plant systems: a hardwired loop is used to connect the different systems. These loops belong to the CIS and the interface with the system is made via a Discharge Loop Interface Box (DLIB), providing electrical isolation and assuring segregation between the current loops and the user connected to the interface box. Use of this architecture is a very special case: if a plant system need to interface with this architecture, then the design of the PIS must be done in coordination with the CIS team. Further details about the architecture and the related components are provided in [RD23].
3 PIS Architecture

The Plant Interlock Systems shall be designed taking into account the following requirements:

- Interlock requirements specified in the Interlock function specifications (function description, safe state definition, requirements for proof-test intervals, response time requirements, ITER Interlock integrity level, maximum allowable spurious trip rate, requirements for overrides...), which are defined referring to [RD3] Management of Local Interlock Function.

Below Table 3 is referred from the PCDH document for giving brief information on codes and standards for Plant Interlock System.

<table>
<thead>
<tr>
<th>Interlock</th>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IEC 61069</td>
<td>Industrial-process measurement and control. Evaluation of system properties for the purpose of system assessment</td>
</tr>
<tr>
<td></td>
<td>IEC 61508</td>
<td>Functional safety of electrical/electronic programmable electronic safety related system</td>
</tr>
<tr>
<td></td>
<td>IEC 61511</td>
<td>Functional safety instrumented system for the process industry sector</td>
</tr>
</tbody>
</table>

Each Plant Interlock System is formed by one or more of the following architectures:

- Slow Architecture
  - Standalone Architecture
  - Fully Fault Tolerant Architecture
- Fast architecture
  - Double Decker Architectures

Below Figure 6 shows the architectures that are currently considered for the Plant Interlock Systems. Depending on the local and central functions that the plant system performs, one or several of these architectures may be implemented.
The choice of which PIS architecture to implement, depends on the local and central functional analysis, the allocation rules, the process time and the integrity level of the functions.

Additionally, for the slow architecture, depending on the availability or maintainability required by the system, it can be implemented using Single Controller (Standalone) architecture or a fully fault-tolerant architecture for a high availability requirement.

The following Table 4 resume the information to be considered in phase of the definition of the PIS hardware.

<table>
<thead>
<tr>
<th>Integrity</th>
<th>Performance</th>
<th>Availability</th>
<th>Technical Solution</th>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 3IL-3</td>
<td>&gt; 100ms</td>
<td>Standard</td>
<td>Siemens S7-400-F</td>
<td>Standalone</td>
</tr>
<tr>
<td>Up to 3IL-3</td>
<td>&gt; 100ms</td>
<td>High Availability</td>
<td>Siemens S7-400-FH</td>
<td>Fully Fault-Tolerant</td>
</tr>
<tr>
<td>Up to 3IL-3 Note 1</td>
<td>&lt; 100ms</td>
<td>Standard</td>
<td>NI Compact Rio</td>
<td>Double Decker</td>
</tr>
</tbody>
</table>

Note 1: Safe failure fraction of the fast controller is 85.47%.

It is possible to implement functions having a slow performance requirement in either a fast or slow architectures, while functions requiring fast performance can only be implemented in a fast architecture.

PIS may be used for exchange the non-critical data with other conventional controllers / PSH Host / CODAC in the same PBS via PON.

The local interlock functions are carried out by the PIS without any inputs from the other devices like conventional controllers / PSH Host/ CODAC in the same PBS.
In the same manner those devices (other conventional controllers / PSH Host / CODAC in the same PBS) are not affecting to the any central functions carried out by PIS to CIS. The PIS controls and monitors the machine protection sensors and actuators and provides the interface to the CIS via the central interlock networks. For technological or integrity reasons, some hardwired links may be considered for safety-related communication between the PIS slow controllers and the PIS fast controllers.

In the case of plant systems with I&C procured by different Domestic Agencies, or formed by components geographically separated; the protection functions may be shared among the different PIS controllers involved, the preferred solution is to have only one PIS controller in the plant system connected to the CIS via the CIN, which is referred as a “PIS concentrator” of the plant system.

The PIS concentrator architecture shall be selected to be at least the same of level of performance as the most powerful solution used in the plant interlock controllers connected to it. For example, if one of the plant interlock controller has a fully fault tolerant architecture, the PIS concentrator shall use the same solution. It is also possible to use one of the existing controllers as “PIS concentrator”, simplifying the interface with the CIS.

![Figure 7: PIS Architecture having multiple Slow PIS controller](image)

### 3.1 PIS Slow Architecture

The PIS slow architecture is intended to execute local interlock functions, whose time to react requirement slower than 100 ms.

The slow controller [RD6] is certified as suitable for its use as a SIL-3 controller and is used for the implementation of all 3IL-2 and 3IL-3 interlock functions.
This high level of integrity is achieved by means of self-diagnostics redundant code execution (internally in each CPU) and a fail-safe communications protocol.

### 3.1.1 Hardware Architecture

As per [RD1] PCDH [R254] slow controllers shall use the Siemens Simatic S7-400 FH range for both SIL-2 and SIL-3 PLCs. It is recommended to select the hardware components from the ITER catalogue [RD6].

The slow functions up to the 3IL-3 can be implemented using one of the following hardware architectures composed of SIMATIC S7 400FH PLCs, which are TÜV certified for applications up to SIL-3:

1. Standalone architecture, composed of a single S7-400F Systems
2. Fully fault-tolerant architecture, composed of redundant S7-400FH system for the slow functions that require a high availability, a very low spurious triggering rate or for plant systems that require maintenance without stopping the process.

#### 3.1.1.1 Standalone Architecture

This Architecture is recommended for the implementation of the Local Interlock functions up to 3IL-3 with standard requirement of availability.

The Standalone architecture is composed of a single CPU (S7-400F/FH) connected to I/O modules using the Profibus or Profinet protocol and implementing an additional safety layer provided by PROFIsafe.

The redundant inputs and outputs shall be connected to different I/O modules to increase the availability of the system. If the Pis include a large number of I/Os the redundant inputs and outputs shall be connected to different peripheral racks. Whenever possible, hot swapping shall be used.

The general configuration for this architecture shall consider:

- Redundant Power Supplies
- A Standalone CPU (S7-400 F/FH)
- Two Communication Processor

For interface with Sensors and actuators, the following configuration shall be considered additionally:

- **For Profibus configuration:** A ET200M rack with IM153-2 HF, IM/IM bus module,
- **For Profinet configuration:** A ET200M rack with IM153-4 HF, IM/IM bus module High Feature (PROFIsafe Compliant)
- Simatic S7- 300 Safety I/O Modules.
Figure 8: Standalone Architecture (One peripheral Rack)

Figure 9: Standalone Architecture (Two or more peripheral Rack)
3.1.1.2 Fully Fault-Tolerant Architecture

This Architecture is recommended for the implementation of the Interlock functions up to 3IL-3 with high requirement of availability, a very low spurious triggering rate or for plant systems that require maintenance without stopping the process.

The fully fault-tolerant architecture is composed of S7-400FH, used in a redundant configuration: both CPUs are connected redundantly to all I/O modules via Profibus protocol and implementing the additional safety layer PROFIsafe. A Profinet connection to the remote I/Os is not recommended for this architecture as it cannot provide the fully fault-tolerant configuration.

The redundant inputs and outputs shall be connected to different remote I/O modules. Whenever possible, hot swapping shall be used.

The Architecture shall be composed of a redundant S -7 400FH system and shall include the following components:
- Redundant Power Supplies for both CPU
- Redundant CPUs (S7-400 FH)
- Redundant Communication Processor (one for each CPU)

For interface with Sensors and actuators, the following configuration shall be considered additionally:
- A ET200M rack with 2xIM153-2 HF, IM/IM bus module
- Simatic S7-300 Safety I/O Modules.

There are two possibilities for the fully fault-tolerant architecture: the first option considers each CPU in separate locations and cubicles; in the second option, the two redundant CPUs are located in the same cubicle.

Note: CPU redundancy principle is hot-standby. The programs in both CPUs are identical and executed synchronously: only the active CPU commands the outputs.

Figure 11: Fully Fault Tolerant Architecture
3.1.2 Network Architecture

The slow architecture of the PIS shall be connected to the slow architecture of the CIS via a safety related communication over Ethernet (CIN) for the exchange of critical data directly involved in interlock functions.

The slow architecture also sends non-critical data to the CIS and receives manual data from CIS through CIN.

The slow architecture of one PIS shall be connected directly to the PSH and the plant system conventional controllers via Ethernet (PON) for the exchange of non-critical data with CODAC.

When required, one slow architecture of the PIS will communicate with the other slow architectures of the PIS inside the same plant system, using Plant Interlock Network (PIN). The PIN uses a safety-related communication for exchanging critical data directly involved in interlock functions or using standard communication for exchanging non-critical data not directly involved in interlock functions.

When required, the slow architecture of one PIS will be connected to the fast controllers of the same PIS, using redundant hardwired links, for the exchange of critical data directly involved in interlock functions.

The redundant communication cables shall be kept as separate as possible, although sharing the same cable tray is permitted.
Figure 13: Network Architecture for Slow PIS


3.1.3 Software Architecture

To standardised the PIS slow controller software architecture throughout all the suppliers of the PIS, the CIS team has designed a modular software architecture shown in the Figure 14. It is strongly recommended to implement PIS slow controller software using the same architecture.

![Figure 14: Software Architecture for Slow PIS Controller](image)

There are two areas in the PIS software architecture for the slow controller:

1. Safety Program
2. Standard Program

The safety program includes: logic for event detection, local protection functions, performance of actions, override implementation, accessing input and outputs from field and the communication on PIN or CIN.

The standard program includes: logic for conventional health monitoring, the non-critical communication to PON, the reset command from CODAC and the supervision and archiving data to the CIS etc.

For programming languages and tools [RD1] PCDH explains in [R252] the programming languages and tools for interlock I&C software shall comply with the assigned SIL level. The PLCs shall be programmed with the engineering software STEP7 and the additional packages: Continuous Functional Chart (CFC) language and certified F-Blocks (F-Library). Safety Matrix tool it is not recommended as it takes considerable time for execution in slow controllers, increasing the scan cycle of CPU.

To help the software developer for implementation of the recommended software architecture, the CIS team has developed the generic PIS PLC template project. This PIS PLC template project is ready to use and pre-configured as per the above software architecture design. Refer [RD2] Guidelines for PIS integration and configuration (ITER_D_7LELG4) for more detail about the PLC template, logic organization and implementation.
3.2 Fast Architecture

The PIS fast architecture is intended to execute the interlock functions with higher time to react constraints, established in between which have been defined to be $100 \mu s < t < 300$ ms.

3.2.1 Hardware Architecture

The Fast Hardware Architecture is composed of two National Instrument cRIO chassis in a double decker configuration, having a FPGA board and DIO modules dedicated to perform the protection functions; an Industrial PC completes the architecture and is dedicated to perform the interface between the FPGA boards and the network connections for logging and monitoring.

The fast controller architecture can implement interlock functions up to 3IL-3\textsuperscript{Note 1} according to evaluation done based on the reference IEC standards [RS1][RS2].

This architecture shall be used for local or central functions with response time requirements less than 100ms (typically in the order of 100 $\mu s$) and integrity level required up to 3IL-3.

In general the Fast architecture has the following features:

General configuration for the architecture includes:

- Two Redundant NI 9159 CompactRIO Chassis which having 14 C-series slots, MXI-Express (MXIe) connectivity and a Xilinx Virtex-5 LX 110 FPGA chip.
- Some NI C-Series I/O modules
- One Industrial Computer (Host PC) with a redundant power supply and 2x MXIe Card NI PCIe-8361

The Double-Decker system architecture is composed of two national Instrument Chassis working in parallel, implementing the protection functions through the application of a voting logic to the inputs and activating the related outputs. The architecture can be used with different configurations of input and output modules, depending on the requirements.

Given the fact that only a few PIS will require this type of architecture, each PIS may need a specific Input/Output modules configuration. Therefore it is strongly recommended to consult the CIS team for the design and configuration of a fast PIS architecture.

Some standard configurations have been developed in order to cope with the most common PIS configurations; they differ among them for the types of input, output, and diagnostic modules installed and give the overall structure for the design of a PIS that is able to perform central or local functions. These configurations are described in the Table 5.

If required, a specific configuration can be generated starting from one of the standard ones.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>FUNCTIONS</th>
<th>ANALOG INPUT</th>
<th>DIGITAL INPUT</th>
<th>DIGITAL OUTPUTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>System A</td>
<td>Local</td>
<td>3 AI</td>
<td>-</td>
<td>2DO 24V</td>
</tr>
<tr>
<td>System B</td>
<td>Local</td>
<td>-</td>
<td>3 DI 24V</td>
<td>2DO 24V</td>
</tr>
<tr>
<td>System C</td>
<td>Local</td>
<td>-</td>
<td>3DI TTL</td>
<td>2 DO TTL</td>
</tr>
<tr>
<td>System D</td>
<td>Central</td>
<td>-</td>
<td>3DI TTL</td>
<td>1 TTL MC (Event)</td>
</tr>
<tr>
<td>System E</td>
<td>Central</td>
<td>1 TTL MC (Action)</td>
<td>2 DO 24V</td>
<td></td>
</tr>
</tbody>
</table>
3.2.1.1 Local Functions Architecture

The general architecture of the three configurations for local functions is based on two National Instrument cRIO chassis in a double decker configuration, each one with three input modules, two output modules, one inter-chassis communication module and two diagnostic modules, with the voting logic implemented in the FPGA.

![Figure 15: General architecture for local function](image)

3.2.1.2 Central Functions Architecture

Two different architectures as shown in Figure 16 and Figure 17, can be configured to communicate an event to the CIS or to receive a mitigation action from the CIS, to implement a central interlock function. Both of them are based on two National Instrument cRIO chassis in a double decker configuration.

The architecture in Figure 16 is dedicated to the detection of an event and sends it to the CIS. In the architecture each chassis includes: three input modules, one output module (dedicated to the MC communication between the PIS and the CIS), one inter-chassis communication module and one diagnostic module, with the voting logic implemented in the FPGA.

The architecture in Figure 17 is dedicated to the reception and actuation of an action. In the architecture each chassis includes: one digital input module (dedicated to the MC communication between the CIS and the PIS), one inter-chassis communication module, one diagnostic module and two digital output modules.
Figure 16: Central functions architecture for events

Figure 17: Central Functions architecture for actions

In below Figure 18, an example of a hypothetical architecture implementing both central and local function is presented.
Figure 18: Fast architecture example implementing both central and local function

- The Host PC is an industrial computer that permits the interface between the chassis and the central architecture of CIS and CODAC. The Host PCs connected to the chassises via MXIe connections. In this Host PC several Ethernet ports shall be available for the following connections:
  - CIN-P: for data exchange between the Host PC and both the CIS modules and supervisor module
  - PON : for data exchange between the Host PC and CODAC
  - TCN : for the timing synchronization function of the fast PIS.

3.2.2 Network Architecture

The critical automatic data directly involved in the central interlock functions is exchanged between the PIS fast architecture and the CIS fast modules via redundant optical link; the Manchester Coding is used as line code for the transmission.

CIN-P connection between the Fast PIS host PC and the CIS supervisor module is used for the exchange of critical data (action, event, voter results) which has to be monitored and archived by the CIS Supervisor Module.

The Critical Manual data is exchanged between the fast PIS architecture and the Supervisor module by High Integrity Operator Commands protocol, via CIN-P.

The PIS fast controllers Host PC shall be connected to the CIS supervision and configuration tools (redundant CIS supervisor implementing WinCC-OA and CIS engineering workstation) through the CIN-P.
The non-critical data exchanged with CODAC, which takes place between the PIS Host PC and the PSH, is done through the PON connection.

An OPC UA server is installed on the PIS host PC in order to allow the subscription of the data to any OPC UA client (WinCC OA and CODAC).

3.2.1 Software Architecture

![Figure 19: Fast PIS software architecture](image)

The software architecture of the fast controller is strictly related to its hardware architecture. The fast PIS is composed of a National Instrument chassis mounting a FPGA board dedicated to perform the Interlock functions and the critical communication, and a host PC dedicated to the monitoring and archiving functions via network communication.

The logics directly involved in interlock functions (critical communications and function implementation) are implemented in the FPGA whereas the other blocks/modules (standard communication and monitoring) are developed in the Host PC. The Data is exchanged between the FPGA and the Host PC software layer using the DMA in the FPGA and implementing an exchange data buffer in the Host PC.
For programming languages and tools [RD1] PCDH explains in [R252] the programming languages and tools for interlock I&C software, which shall comply with the assigned SIL level. The following tools are used to develop the fast controller's software.

For the Host PC:
- RHEL (Red Hat Linux Operation System) 6.5, 64 bits or later
- IRIO library
- NI RIO library, open software edition
- OPC UA Server

For the Chassis:
- NI LabVIEW 2014 FPGA Module

The instructions for the correct configuration of the Fast architecture are described in “Guidelines for PIS configuration and integration” [RD2].
4 Interfaces

4.1 Interface between different PIS in same plant system

The number of PIS within the same plant system must be kept as low as possible and its increase can only be justified by procurement, geographical or operational reasons.

The PIS-to-PIS interface inside the same plant system shall be used to the exchange only critical interlock data (local events, actions).

Whenever possible only one PIS of the plant system should be interfaced with the CIS, as explained in Section 3.

4.1.1 Slow Architecture

When required, the interconnection between different slow PIS in the same plant system is performed through the PIN.

The critical automatic data directly involved in slow interlock functions shall be exchanged using the safety-related communication.

It is recommended to use Ethernet network for PIN to perform connections between different slow PIS of the same plant system and exchange non-critical data which are not directly involved in interlock functions.

4.1.2 Fast Architecture

In case of Fast interlock functions, the connection between fast PIS for the exchange of the critical interlock data involved in interlock functions must be performed using Manchester code communication over redundant optical links.

It is recommended to use redundant hardwired links for realizing a connection between slow PIS and fast PIS for exchanging critical interlock data directly involved in interlock functions.

4.2 Interface between different PIS of different plant systems

The direct connection between plant interlock systems belonging to different plant systems is, in principle, not allowed. The two PIS must use the CIS to exchange information.

Exceptions can be made for performance or integrity reasons (e.g. hardwired loops between plant systems). In such cases this connection between one or more PIS belonging to different plant systems is considered to be part of the CIN and therefore falls under CIS responsibility.

4.3 Interface between PIS and CIS

The connection between the PIS and the CIS is done via the Communication Network Panel (CNP) for the architecture based on controllers and via user interface boxes for the hardwired architecture.

The communication between PIS and CIS is made through the CIN, which is an Ethernet network divided into two interconnected branches called CIN-P1 and CIN-P2. This network is dedicated to the exchange of
interlock critical data and non-critical data and each PIS shall be connected to both CIN-P1 and CIN-P2 via the CNP.

The CNP are installed in strategic locations, close to plant system I&C cubicles. The plant system shall provide the single mode optic fibre connection up to the CNP. More details about this connection are available in the Component Technical Specification for Passive Network Components [RD14].

4.3.1 Slow Architecture

Each PIS should be able to communicate with slow CIS protection modules and the CIS supervision and configuration tools (redundant CIS supervisor module including WinCC-OA and CIS engineering workstation).

Each PIS shall be connected to CIN-P via the communication processors (CP) on LAN X2 port.

The safety-related communication between the PIS and the slow CIS protection modules uses the safety message frame (F_SEND/F_RCV) via S7 fault-tolerant connections between the F-CPUs.

Details on the connection with the redundant CIS supervisor are given in Guidelines for PIS integration and configuration [RD2].

4.3.2 Fast architecture

A fast architecture of the PIS may communicate directly with the CIS fast controllers via redundant optical point-to-point links using Manchester coding, taking advantage of the CIN infrastructure (CNP, Network Hutches) but avoiding network switches.

The PIS can communicate with the CIS supervision tools (redundant CIS supervisor module implementing WinCC-OA and CIS engineering workstation), via CIN-P using WinCC OA-CRIO interface, based on an OPC UA server located on the Host PC of the fast architecture.

More details about implementation of the interface are provided in "Guidelines for PIS integration and configuration [RD2]".

4.4 Interface between PIS and PON (PSH & PSCC)

![Diagram of Connection between PIS and PSH&PSCC](image)

**Figure 20**: Connection between PIS and PSH&PSCC
The PIS or different PIS inside a plant system transmit *non-critical data* to the PSH through PON, which makes it available to CODAC and therefore accessible from the control rooms and to PSCC, which requires for its normal operation.

The link between PIS and PSH must be bidirectional in order to transmit *non critical commands (reset) and reintegration* from CODAC to the PIS via the PSH and to make *non critical data* available to the control rooms.

The link between PIS and PSCC must be unidirectional, that is from PIS to PSCC.

### 4.4.1 Slow architecture

The connection is done through PON over Ethernet for the transmission of non-critical interlock data. Slow PIS shall be connected directly to PON using the Gigabit X1 port of the CPs. In case of slow PIS standalone architecture only single CP’s X1 port will be connected to the PON as shown in Figure 10.

![Figure 10](image-url)  # While in the case of fully fault tolerant PIS architecture both CP’s X1 port will be connected to the PON as shown in Figure 11: Fully Fault Tolerant Architecture.
Hardwired connections can be allowed for the PIS-PSCC connection, but a connection through PIN or CIN is not allowed. The CIN and PIN must be used for the transmission of critical interlock data.

The connection to PON is also used to provide time synchronization through the Network Time Protocol (NTP) to the systems which do not require a high accuracy of time synchronization (e.g. slow PIS).

4.4.2 Fast architecture

The PIS fast controllers are connected to PON via a Network Connection on the Host PC; the Host PC permits the subscription of the non-critical interlock variables to CODAC, using an OPC UA server. The Connection to TCN is used to provide the time synchronization to the Host PC in order to accurately timestamp the data.

4.5 Interface between PIS and PSS

The network connection between PIS and PSS is not allowed: hardwired circuits must be used to exchange information. These electrical circuits include electrical separations between the safety-class equipment (PSS) and the non-classified equipment (PIS), according to IEC 61513 and RCC-E D7540.
5 Powering

5.1 Conceptual principles

The Central Interlock System cubicles are powered by two independent sources:

1. Class II-IP power supply: uninterruptible, backed up by a battery set of 1 hour of autonomy, plus a diesel generator available for 24 hours.
2. Class IV power supply: is an alternative power supply, adopted in the event of class II inverter failure or fault in the class II power feeder.

The principle for the powering of the PIS should be the same as for the CIS; all the PIS cubicles and components must be redundantly powered.

By mutual agreement between the Steady State Electrical Power Supply Networks and the consumer, another Class II-IP power supply from another feeder can be used instead of Class IV power supply for particular PIS.

The route of the redundant powering cables should be kept as separate as possible, minimizing the use of the same cable tray.

The powering of components not directly involved in the investment protection, such as cubicle monitoring systems shall not have any impact on components involved in the investment protection.

The following voltages shall be available in the interlock cubicles:

1. Class II-IP – 230Vac
2. Class IV – 230Vac
3. Class II-IP – 24Vdc
4. Class IV – 24Vdc

The power supplies shall be monitored so that a failure of one power supply can be reported and it can be repaired in order to restore the redundant configuration in the minimum period of time. In most cases, considering that Class II-IP 24Vdc and Class IV 24Vdc are linked to Class II-IP 230Vac and Class IV 230Vac, it will be necessary and sufficient to connect Class II-IP – 24Vdc and Class IV- 24Vdc with a NC relay or switch to a digital input module of the controllers already available in the PIS.

5.2 Slow Architecture

5.2.1 Powering of Controllers

Each CPU rack shall be powered by two redundant power supplies (PS 407 AC 120/230V DC 5V / 10A for redundant use). Each power supply module shall have two backup batteries in its battery compartment (Battery Lithium AA, 3.6V/2.3 Ah).
5.2.2 Powering of Peripheral Racks / Components

The powering of peripheral racks depends on the architecture and the number of redundant components and its cabling on the racks. It is recommended to have separate power supplies circuit breakers for the IM modules, digital I/O modules and the analog I/O modules. Please refer [RD10] Guidelines for I&C cubicle configurations (ITER_D_4H5DW6) for details of AC and DC power distributions.

The schema in describe the power supply redundancy concepts for the IM Module in single peripheral rack. In this schema, the PSa or PSb blocks are power supplies 230Vac/24Vdc, while the redundancy block is conceptual materials (for example: diodes or a SITOP Redundancy module) that enable a redundant 24Vdc supply to be implemented using two Power supplies.

Using two power supplies and one redundancy block per rack is just one of the possible solutions for creating redundant 24Vdc trains for peripheral racks; other solutions fulfilling the redundancy requirements can be implemented.

Please note that for powering multiple racks of PIS Standalone Architecture the same schema (as shown in Figure 23) can be use.
Figure 23: Powering IM Module in Peripheral Rack of Standalone Architecture

The schema in Figure 24 shows one of the solutions for powering the Interface Modules in peripheral racks of Fully Fault Tolerant PIS Architecture.
In the schema providing separate redundant power supplies to redundant IM modules increases the availability of the respective Rack.

Figure 24: Powering IM Modules in Peripheral Racks of Fully Fault Tolerant Architecture

By using the same schema (shown in Figure 24) multiple racks of Fully Fault Tolerant Architecture can be powered.

5.3 Fast Architecture

Powering of the Fast Architecture requires the powering of the Host PC and the two Chassis. The Host PC shall be powered by a redundant power supply for example MRG-5800V4V 9.0A @115V, 5A @230VAC redundant or similar.
The NI 9159 Chassis requires an external power supply that meets its supply voltage specifications. The NI 9159 chassis filters and regulates the supplied power and provides power for all of the I/O modules.
5.4 Networks Products

Each piece of network equipment (e.g. switches) involved in PIN or CIN shall be powered by two independent sources Class II-IP and Class IV.

5.5 Other Components

It is preferred that other cubicle components (e.g. cubicle monitoring system, fan) are redundantly powered but they can be powered by Class II-IP only.
6 Signal Cabling

The naming convention defined in Signal and Plant System I&C Variable Naming Convention [RD15] is applicable for the interlock signals.

When signal redundancy is required, the redundant cables shall be kept as separate as possible but they may be routed through the same cable tray.

6.1 Slow Architecture

Following are the recommendation for signal cabling for slow architecture

1. Signals shall be connected to I/O card through terminal blocks.
2. An external protective circuit shall be installed, in order to provide sufficient surge strength to an ET200M with fail-safe signal modules.
3. Marshalling Terminal Assembly as referenced in Catalogue for I&C products – Slow controllers shall be used.
4. It is possible to use pieces of equipment recommended in “Guidelines for I&C cubicles configuration” [RD10], if use of these equipment does not affect the PIS 3IL level.

In standalone S7 F/FH Systems, the fail-safe signal modules can be operated in an ET200M distributed I/O system. Safety-related communication between the safety program in the F-CPU and the fail-safe inputs and outputs takes place via the standard Profibus-DP or Profinet, with a superimposed PROFISAFE safety profile using the interface module IM153-2 HF or IM153-4.

In the case of fully fault-tolerant architecture, only the Profibus network shall be redundant: each redundant CPU is connected to all the peripheral racks using two interface modules (IM153-2) per rack. It is possible to use Optical Link Modules if there is a long distance on a Profibus I/O bus.

The connection between the PIS controllers and its remote peripherals is part of the PIN. The communication between controllers and remote peripherals shall use a safety-related protocol.

6.1.1 Digital Modules

As per following digital module shall be used in the applications:

1. Digital inputs module: SM 326; DI 24 x DC 24V
2. Digital outputs module: SM 326; F-DO 10 x DC 24V

As per [RD22], the applications shown in Figure 27 can be selected for corresponding configurations.

For Digital Input Modules:
Interlock functions shall use application 3 to 6, as per Figure 27. 3IL-2 functions shall consider application 3 and 4, while 3IL-3 functions require application 5 or 6, according to the availability requirement.

For Digital Output Modules:
Applications 1 and 2 are omitted because the module supports only safety mode. There is not much difference between Applications 3/4 and 5/6.
The Digital Output Module configurations for both 2IL-3 and 3IL-3 functions shall consider application 5 or 6 for high availability.
Examples of cabling can be found on [RD22] Siemens Fail-safe signal modules: Installation and Operating Manual, 07/2013, A5E00085586-11, for more details about settings for different modules.

6.1.1.1 Application 3 for Digital Input Module: Safety Mode 3IL-2

One sensor is connected via one channel for each process signal (1oo1 evaluation).

```
 SM 326;  
 DI 24 x DC 24V
```

Figure 28: Application 3 for Digital Input Module - Safety Mode 3IL-2

**WARNING**

To achieve the 3IL-2 functions using this wiring, you must use a suitably qualified sensor.
6.1.1.2 Application 4 for Digital Input Module: Safety mode 3IL-2 with high availability

Two redundant sensors are each connected via one channel to the two analog modules for each process signal (1oo1 evaluation).

![Diagram](image1.png)

Figure 29: Application 4 for Digital Input Module - Safety mode 3IL-2 with high availability

**WARNING**

To achieve the 3IL-2 functions using this wiring, you must use a suitably qualified sensor.

6.1.1.3 Application 5 for Digital Input Module: Safety mode 3IL-3

Two single-channel sensors are connected via two channels to each of two opposite inputs of the digital module for each process signal (1oo2 evaluation structure).

![Diagram](image2.png)

Figure 30: Application 5 for Digital Input Module - Safety mode 3IL-3

**WARNING**

To achieve the 3IL-3 functions using this wiring, you must use a suitably qualified sensor.
6.1.1.4 Application 6 for Digital Input Module: Safety mode 3IL-3 with high availability

Two redundant single-channel sensors are required per process signal. One sensor is connected via one channel to two opposite inputs of the digital module for each module (1oo2 evaluation).

![Application 6 for Digital Input Module - Safety mode 3IL-3 with high availability](image)

**WARNING**

To achieve the 3IL-3 functions using this wiring, you must use a suitably qualified sensor.

6.1.1.5 External Sensor Supply for Digital Inputs

It is **not** recommended to use an external sensor supply, but if it is required, the Figure 32 below shows how the sensors can be connected to an external sensor supply. All channels of a channel group must be connected to the same external sensor supply. In this case, some errors cannot be detected but these errors can be met by short-circuit proof routing of the sensor lines.

![External sensor supply for Digital Inputs](image)
6.1.1.6 Application 5 for Digital Output Module: Safety mode 3IL-3

Single-channel connection of one sensor for each process signal. The load voltage supply is wired to terminals 2L+/2M or 3L+/3M of the digital module.

**Note**

In case of SIL3: The signal at the output has to change daily or even more frequently. If this is not the case with the "0" signal, in parameter setting light test must be activated to meet this condition.

![Diagram of Application 5 for Digital Output Module - Safety mode 3IL-3](image)

**WARNING**

It is no longer possible to shut down an actuator if a short circuit is present between 2L+ and DO. To prevent short circuits between 2L+ and DO, the route of the cables used to connect the actuators shall be made in a short-circuit-proof manner.
6.1.1.7 Application 6 for Digital Output Module: Safety mode 3IL-3 with high availability

Each process signal requires one actuator which is controlled redundantly by the two digital modules. The load voltage supply is wired to terminals 2L+/2M or 3L+/3M of the digital module.

![Diagram of Digital Output Module](image)

**Figure 34**: Application 6 for Digital Output Module - Safety mode 3IL-3 with high availability

**Note**

Use the same reference potential for both modules.

**WARNING**

Prevent short circuits to L+ at the SM 326; F-DO 10 x DC 24V/2A PP with protected routing of the signal lines, otherwise the actuator will remain activated. In case of redundant wiring at the output, with configured redundancy operation, when a short circuit to L+ will happen the associated output will not be switched off.
6.1.2 Analog Modules

Analog input modules shall be SM 336; F-Al 6 x 0/4...20mA HART as per [RD6]. This module allows 0...20mA and 4...20mA configuration. For the interlock controls, the 4...20mA configuration is recommended.

Analog Output Module is not available to be used as a safety module from Siemens

The Figure 35 below helps to select an application based on availability and fail-safe operation requirements. Applications 1 and 2 are omitted because the module supports only safety mode.

![Figure 35: Selecting Applications for Analog Modules](image)

**WARNING**

The maximum Safety Integrity Level is determined by the sensor quality and the length of the proof-test interval according to the IEC 61508:2000 standard.

If there is a short circuit from L+ to Mn+, the input resistors will be destroyed. This problem can be avoided through a proper wiring and the use of the internal sensor supply. When an external sensor supply is used, other suitable measures are necessary to protect the input resistors (e.g. fuse on the module).

**Wiring Schemes**

Four wiring schemes (A - D or E- H) are available for each application, depending on the type of measurement
Recommendation: Internal sensor supply

This internal sensor supply of the module is monitored and its status is indicated by the Fn LED. The internal sensor supply of the associated channel is switched off in case of an overload of the analog input or short circuit to ground or during power-up in the event of short circuit to L+ to protect the input. A check is made approximately 1 minute later to determine if the error has gone. Because of these short circuit-proof and monitoring features of the internal sensor supply, it is strongly recommended to use the short circuit-proof internal sensor supplied by the module.

In the following subsections, only the examples of wiring schemes (1oo1) with internal sensor supply A, C, E and G are explained, as per Table 6.
6.1.2.1 Wiring scheme A: Two-wire transducer, internal sensor supply

Particularity:

- Short circuit between sensor supply voltage \( V_{sn} \) and \( M_n^+ \) is handled.
- It is possible to detect an under voltage at the transducer by reading back the sensor supply in the module.

![Wiring diagram](image)

Figure 36: Two-wire transducer, internal sensor supply
6.1.2.2 Wiring scheme C: Four wire transducer, internal sensor supply

Particularity:
- Short circuit between sensor supply voltage $V_{sn}$ and $M_{n+}$ is handled.
- It is possible to detect an under voltage at the transducer by reading back the sensor supply in the module.

![Diagram of four-wire transducer, internal sensor supply]

**Figure 37 : Four-wire transducer, internal sensor supply**
6.1.2.3 Wiring scheme E: Two-wire transducer, internal sensor supply with module redundancy

Particularity:

- Short circuit between sensor supply voltage V_sn and M_{n+} is handled.
- It is possible to detect an under voltage at the transducer by reading back the sensor supply in the module.
- It is necessary to incorporate the external elements into the application-specific safety examination. This means external elements (e.g., Zener diodes) are needed to achieve the respective Safety Integrity Level.

Note

1L+ and 2L+ can be fed from one power supply.

Figure 38: Two-wire transducer, internal sensor supply with Module Redundancy
6.1.2.4 Wiring scheme G: Four-wire transducer, internal sensor supply with module redundancy

Particularity:
- Short circuit between sensor supply voltage Vsn and Mn+ is handled.
- It is possible to detect an under voltage at the transducer by reading back the sensor supply in the module.
- It is necessary to incorporate the external elements into the application-specific safety examination. This means external elements (e.g., Zener diodes) are needed to achieve the respective Safety Integrity Level.

Note
1L+ and 2L+ can be fed from one power supply.

---

![Figure 39: Four-wire transducer, internal sensor supply with Module Redundancy](image)

6.1.2.5 Applications and wiring schemes

In the following Table 7, applications and associated wiring schemes for analog input module are mentioned:
The respective applications and associated wiring scheme can be selected from above Table 7. More details about wiring of each application can be found on reference document [RD22].
6.2 Fast Architecture

Following are the requirements for signal cabling for fast architectures:

1. Signals are connected to I/O card through terminal blocks.
2. Install an external protective circuit, in order to provide sufficient surge strength to an NI 9159 Chassis.
3. Marshalling Terminal Assembly referenced in Catalogue for I&C products – Fast controllers is used.

6.2.1 Input Modules

- Following input modules shall be use in fast PIS application:
  - NI 9401 8-Ch, 5 V/TTL High-Speed Bidirectional Digital Input/Output (DIO) Module
  - NI 9205 32-Ch, ±200 mV to ±10 V, 16-Bit, 250 kS/s Analog Input (AI) Module
  - NI 9425 32-Ch, 24 V, 7 μs, Sinking Digital Input (DI) Module

In below Figure 40: Input Modules Cabling Schema is shown how to connect NI 9205 modules; the same schema is applicable for NI 9401 (DIO) and NI 9425 DI modules.

In the schema (Figure 40: Input Modules Cabling Schema), each sensor is connected to one of the input pins of the Input modules in each chassis, therefore a trio of sensors (Sensor1, Sensor2, Sensor3) is connected to each \( n \) channel of the input module according to the following rule (were \( n \) increases as the number of triple-sensors increase):

- Sensor1 to Chassis1 Module1 and Chassis2 Module1
- Sensor2 to Chassis1 Module2 and Chassis2 Module2
- Sensor3 to Chassis1 Module3 and Chassis2 Module3

The port <0> of each Input module is reserved for checking its integrity. This is done by measuring pre-set input signals generated with the diagnostic modules.

Figure 40: Input Modules Cabling Schema
6.2.2 Output Modules

The following digital output modules shall be used in the fast PIS applications:

- NI 9401 8-Ch, 5 V/TTL High-Speed Bidirectional Digital Input/Output
- NI 9477 32-Ch, 24 V, 8 μs, 5 to 60 V, Sinking Digital Output (DO)
- NI 9476 32-Ch, 24 V, 500 μs, Sourcing DO Module

The above listed modules can be used as a DO module to interface to a digital actuator. The interconnection rule is the same as the input modules: the DO0 of each module is reserved for checking the integrity of the module itself and the remaining channels according to the following rule, which defines how to connect a double actuator (Actuator 1, Actuator 2) to a couple of NI 9159 chassis with two Digital output modules installed in slot 7 and 8 of each chassis:

- Actuator1 to Chassis1 Module7 and Chassis2 Module7
- Actuator2 to Chassis1 Module8 and Chassis2 Module8

![Figure 41: NI 9477 Output module cabling Schema](image)

6.2.3 Diagnostic Modules

The following modules shall be used as the diagnostic module in fast PIS applications:

- NI 9264 16-Ch, ±10 V, 16-Bit, 25 kS/s Analog Output (AO) Module
- NI 9476 32-Ch, 24 V, 500 μs, Sourcing DO Module
- NI 9426 32-Ch, 24 V, 7 μs, Sourcing DI Module
- NI 9401 8-Ch, 5 V/TTL High-Speed Bidirectional Digital Input/Output (DIO) Module

The NI 9264 Analog output module is used to implement the diagnostic of the NI 9205 Analog input modules. The AO channels of NI 9264 must be connected to the AI0 channel of each AI module in ascendant order. This means that AO0 of NI 9264 must be connected to Module1 AI0, AO1 to Module2 AI0 and so on. In the following Figure 42, it is shown how each AI module’s channel is connected to the AO module channels in RSE mode and wired to the corresponding analog signal channel and the ground connection.
The NI 9476 32-channel 24 V sourcing DO module is used to implement the diagnostic of the NI 9425 DI modules. The DO channels of NI 9476 must be connected to the DI0 channel of each DI module in ascendant order. This means that DO0 must be connected to Module1 DI0, DO1 to Module2 DI0, and so on.

In the below Figure 43, Each DI module’s channel DI0 is connected to one of the channels of the DO module; the digital ground is wired between the modules.

The NI 9426 (DI) module is used to implement the diagnostic of the NI 9477 sinking DO modules. One DO channel of each NI 9477 must be connected to a DI of the NI 9426 module in ascendant order. This means that Module6-DI0 must be connected to Module7-DO0, Module6-DI1 to Module8-DI0, and so on.
The NI 9401 with its channels configured as DO can be used to implement the diagnostic of the DI Modules NI 9401. Every DO channel must be connected to a DI module in ascendant order. This means that DO0 must be connected to Module1-DI0, DO1 to Module2-DI0, and so on.

The NI 9401 is also used to implement the diagnostic of the NI 9401 DO modules. In this case the module must be configured for DIs. Every DO channel must be connected to a DI module in ascendant order. This means that Module6-DI0 must be connected to Module7-DO0, Module6-DI1 to Module8-DI0, and so on.
6.2.1 Communication Modules

The NI 9401 Module can be also used to implement the Inter-chassis communication via SPI protocol or Manchester coded communication, in order to send and receive actions and events form the CIS Fast Modules. Below are explained the different cases.

6.2.1.1 SPI Communication between Chassis: Signal Interconnection

The NI 9401 is used to implement communication between the two chassis using the SPI protocol. Two bidirectional SPI communications are implemented in each chassis, but one is used only to receive (slave) and other only to transmit (master). To implement this communication, half of the channels of the module are configured as DO and the other half as DI as per Figure 47.
6.2.1.2 Communication between PIS and CIS: NI 9401 as Manchester Code transmitter (Events)

The NI 9401 is used to make the PIS communicate with the CIS using a Manchester Coded signalling. One unidirectional MC communication is implemented in each chassis, to transmit the chassis data. To implement this communication, only one channel of the module is configured as DO (refer to Figure 48).
6.2.1.3 Communication between CIS and PIS: NI 9401 as Manchester Code receiver (Actions)

The NI 9401 is used to make the CIS communicate with the PIS using a Manchester Coded signalling. Additionally, two bidirectional MC communications are implemented in each chassis, one to receive and the other to transmit data between chassis. To implement this communication, half of the channels of the module are configured as DO and the other half as DI (refer to Figure 49).

Figure 49: Manchester Code action receiver cabling schema
7 Sensors & Actuators

7.1 Redundancy of Investment Protection: Sensors and Actuators

Sensors and actuators must have their dominant failure mode yielding to a safe state, or their dangerous failures must be detected (Safe Failure Fraction SFF > 60% as per IEC 61508-2).

To establish whether the dominant failure mode brings to a safe state, it is necessary to consider each of the following aspects:

1. The process connection of the device
2. The use of diagnostic information of the device to validate the process signal
3. The use of inherent fail-safe behaviour of the device (for example, live zero signal, loss of power results in a safe state).

Whenever it is possible, sensors and actuators involved in 3IL-2 functions should be SIL-2 or SIL-3 certified components.

Whenever it is possible, sensors and actuators involved in 3IL-3 functions or in hardwired loops should be SIL-3 certified components or at least SIL-2 certified components able to achieve SIL-3 when used in a redundant configuration.

In a SIL rated safety loop there are occasions in which a SIL certified instrument is not available and it is thought desirable to use an instrument or a component which is well known to the user, and has not been assessed under the IEC 61508 group of standards e.g. by an FMEDA. The Functional Safety standards allow the use of such equipment only on the basis that they should be “proven in use” (IEC 61508) or has a history of “prior use” (IEC 61511). This means that a documented assessment has shown that there is an appropriate evidence, based on the previous use of the component, that the component is suitable for being used in a safety instrumented system (refer to IEC 61511-2 Section 11.5.3).

It is the end user who must ensure that the Safety Instrumented System (SIS) meets the requirements of the standard. One can do that by assessing the SIS them self or by devolving the assessment to a supplier or a system integrator. However, the user retains overall responsibility.

The requirements of IEC 61508 and IEC 61511 for “proven in use” are very demanding. The user is required to have appropriate evidence that the components and subsystems are suitable for being used in the SIS. This means that, as a minimum, the user must have:

- A formal system for gathering reliability data that differentiates between safe and dangerous failures
- Means of assessing the recorded data to determine the safety integrity of the device / equipment, and its suitability for the intended use.
- Evidence that the application is clearly comparable
- Recorded historical evidence of device hours in use
- Evidence of the manufacturer’s management, quality and configuration manufacturing systems
- Device firmware revision records
- Proof that reliability data records are updated and reviewed regularly

Users are cautioned to closely scrutinise the relevant clauses of both standards before embarking on this solution

To limit the common mode failures, the choice of redundant instruments should be diversified (use of different technologies or different constructors).
The maximum Safety Integrity Level is determined by the sensor quality and the length of the proof-test interval according to the IEC 61508:2000 standard. If the sensor quality does not meet Safety Integrity Level requirements, always wire redundant sensors and connect them via two channels.

Sensors and actuators involved in 3IL-2 functions shall use 2 components with a 1oo2 voting or, where there is a high risk of spurious tripping or a low acceptable spurious trip rate, 3 components with a 2oo3 voting.

Sensors and actuators involved in 3IL-3 functions shall use 2 certified or “proven in use” components with a 1oo2 voting or, where there is a high risk of spurious tripping or a low acceptable spurious trip rate, 3 certified or “proven in use” components with a 2oo3 voting.

Whenever it is not possible to use certified or “proven in use” sensors or actuators, the sensors involved in 3IL-3 functions must use 3 components with a 1oo3 voting or 4 components with a 2oo4 voting. The choice of 2oo4 voting has to be made in case there is a high risk of spurious tripping, or a low acceptable spurious trip rate, or in case an assessment of the equipment according to the [RS1] IEC 61508 methodology is required.

In standalone architecture for slow controllers, the redundant sensors and actuators shall be connected to different modules. If the amount of I/O requires additional peripheral racks, the connection to I/O modules should be extended by using the separate ET200 modules.

Digital inputs modules of the slow architectures require for being reliably detected by the fail-safe a minimum duration of sensor’s signals of 30ms.

The fail-safe digital output modules belonging to the slow architectures perform a cyclic test of the outputs. The module briefly disables the active outputs and enables the inactive outputs. The test pulses have duration shorter than 1ms. High-speed actuators may briefly drop out or be activated during this test: if the process does not tolerate this action, actuators with sufficient lag (>1ms) must be used; if it is not possible, this issue can be solved by duplicating the outputs (refer to 6.1.1.7)

Below is summary for selecting the sensors and actuators plus the corresponding voting:

- **3IL – 2 functions:**
  - SIL 2 or SIL 3 sensors / actuators
  - Proven in use (IEC 61508-2 section 7.4.10)
    - HFT = 1 → 1oo2 / 2oo3 voting

- **3IL-3 functions**
  - SIL 3 sensor / actuators
  - 1oo2 / 2oo3 voting SIL 2 sensors / actuators
  - Proven in use (IEC 61508-2 section 7.4.10)
    - HFT = 1 → 1oo2 / 2oo3 voting
  - If not certified or proven in use elements must have a dominant failure mode to safe state.
    - Perform an assessment according to IEC 61508 methodology
    - HFT= 2 → 1oo3 / 2oo4 voting

- **Failsafe Inputs / outputs cards in slow controllers:**
  - Digital input detection > 30 ms
  - Digital outputs: Cyclic deactivation during 1ms
  - Solution duplication of the outputs (refer to 6.1.1.7)
7.2 Sharing of Sensors between PIS, PSCC and PSS

If a sensor has to be shared between the PIS and the Plant Safety System (PSS) or between the PIS and the plant system conventional control (PSCC) the preferred solution is to duplicate it (together with its redundancy) and to totally separate the systems, by linking one sensor to the PIS and the other to the PSS or the PSCC. Indeed, all the components involved in an interlock function shall comply with the interlock requirements and all the components involved in a safety function shall comply with the safety requirements.

When the sensor cannot be duplicated and needs to be shared between PIS, PSS and PSCC, the preferred solution is to share the sensor between PIS and PSS and to keep totally separated the PSCC. This allows the conventional control to be considered as a first protection layer for the process.

When the sensor cannot be duplicated and needs to be shared, two solutions are proposed:

- **Solution 1**: The sensor is shared, but the signal processing is performed separately by each system (using a signal duplicator, which makes the sharing of sensors transparent for each system). Example: Information from the Infra-Red cameras is treated with *intelligent* image processing in the diagnostics but with a reliable low-definition processor at the interlock level.

![Figure 50: Sharing Sensor (Through Signal Duplicator at field)](image)

- **Solution 2**: The most critical system (i.e. the PSS for the PSS-PIS sharing and the PIS for the PIS-PSCC sharing) takes control of the sensor and shares its information via the PSS-PIS (secured) interfaces or PIS-PSCC (non-secured).

  Example: A quench detector connected to the interlock system whose state is sent to the conventional control of the magnet I&C.
If the second solution is chosen, it is necessary to specify the safe-state for the case in which a communication failure between systems occurs (as it will be specified for PIS-CIS communication).

Whichever solution is chosen, the shared components shall comply with the requirements of each system.

Probability of failure for each solution (PFHs is the sensor part of the PFH of the function as defined above):

Solution 1:

\[ \text{PFHs} = \text{PFH (sensor)} + \text{PFH (signal duplicator)} \] for each system.

Solution 2:

\[ \text{PFHs} = \text{PFH (sensor)} \] for the most critical system

\[ \text{PFHs} = \text{PFH (sensor)} + \text{PFH (most critical system)} + \text{PFH (communication between system)} \] for the other system

If it is possible to implement a signal duplicator with a low probability of failure and which reacts quickly (compared to the sensor detection time), the solution 1 is preferred.

### 7.3 Sharing of Actuators between PIS, PSCC and PSS

If an actuator has to be shared between the PIS and the Plant Safety System (PSS) or between the PIS and the plant system conventional control (PSCC) the preferred solution is to duplicate it (together with its redundancy) and to totally separate the systems, by linking one actuator to the PIS and the other to the PSS or the PSCC. Indeed, all the components involved in an interlock function shall comply with the interlock requirements and all the components involved in a safety function shall comply with the safety requirements.

When the actuator cannot be duplicated and needs to be shared between PIS, PSS and PSCC, the preferred solution is to share the actuator between PIS and PSS and to keep totally separated the PSCC. This allows the conventional control to be considered as a first protection layer for the process.
When the actuator cannot be duplicated and needs to be shared, the proposed solution is:

- **Solution:** The actuator is shared but the command is performed separately by each system. The actuator respects the fail-safe principle, any system commanding the actuator in a safe position has the priority.

**Example:** A valve can be finely regulated by the conventional control but can also be reliably set in two single states (open-closed) by the interlock (the regulation loop controlled by the conventional system is opened by a safety relay, which is controlled by interlock system: when the loop is opened, the valve goes to a safe position).

![Figure 52: Sharing Actuators](image)

The shared components shall comply with the requirements of each system.
8 Hardware

Each piece of PIS equipment shall be compliant with its environmental constraints.

The recommendations of the providers (e.g., Siemens, National Instrument...) and IO cabling rules [RD11] shall be followed.

As far as possible, the cable paths prepared by Cable Trays (PBS-44) should be followed. If a path needs to be changed for any reason, then the proposed new cable path must be approved by PBS-44.

The naming convention defined in ITER Numbering System for Components and Parts [RD16] is applicable for the interlock components.

8.1 Catalogues for PIS hardware components

The slow architectures for the interlock systems are based on Siemens S7-400 FH PLCs. The components must be chosen from ITER’s “Catalogue of I&C products for Slow controllers” [RD6].

The fast controllers for the interlock systems are based on National Instruments’ FPGA-based system called CompactRIO. The components must be chosen from ITER’s “Catalogue of I&C products for Fast controllers” [RD9].

The network switches recommended for the interlock systems are Hirschmann products: MACH1040 or MACH104. The references of these switches are available in the Integration kit for PS I&C [RD20].

The cubicles hosting the interlock equipment have to be chosen from ITER’s “Catalogue of I&C products for Cubicles” [RD7].

The cables must be chosen from ITER’s “Catalogue for Cables” [RD8].

The equipment should be chosen to achieve the reliability and availability (MTBF criteria) demanded for the ICS. The sensor and actuators shall also comply with the integrity requirements of the functions (PFD/PFH criteria).

As far as possible, the PIS hardware components should be the COTS equipment; this is recommended for the standardization of the ITER interlock components, in order to simplify the reliability, adaptability, maintainability and integration with the ICS.

The user interface boxes (DLIB and BLIB) used for the hardwired architecture will be provided by PBS.46; each user interface box consists of a 19” rack mounted board, having a height of 2U. For more details about the hardware please refer to the [RD23] and the PBS 46 RO can also be contacted.

In addition to the requirements set in the “Plant Control Design Handbook” [RD1], the plant systems’ suppliers shall provide also some spare parts and tools, in order to replace the faulty equipment within the maximum time to repair (one shift).

8.2 Cubicles

The components belonging to the Plant Interlock System are hosted in designated IP cubicles, which will not be shared with the conventional control or the plant safety systems.
For maintenance purposes, the cubicles shall be installed as far as possible and in areas which are accessible during plasma operation; all electrical components (e.g. power supplies, circuit breakers etc...) have to be fully accessible and easily removable, in order to be replaced even if the cubicle is still powered.

The interlock cubicles located in buildings with seismic class SC1, or located in rooms with SIC cubicles, are classified SC2; other cubicles are classified NSC.

The number of interlock cubicles shall be kept as small as possible. Each architecture shall be fully implemented in a single cubicle (LCC+SCC). If several cubicles are required, it is preferred to separate the slow architectures from the fast architecture.

It is recommended that the “guidelines for I&C cubicle configurations” [RD10] are followed.

The requirements for earthing, electromagnetic compatibility and the cable entries (on top or on bottom) described in “EDH Part 1: Introduction” [RD17], in “EDH Part 4: Electromagnetic Compatibility (EMC)” [RD18] and in “EDH Part 5: Earthing and Lightning Protection” [RD19] are applicable to the PIS cubicles.

A cubicle monitoring system is included in each I&C cubicle: details about this system can be found in [RD13].