IDM UID
75ZVTY

VERSION CREATED ON / VERSION / STATUS
08 Dec 2017 / 6.0 / Approved

EXTERNAL REFERENCE / VERSION

Memorandum / Note

Management of Local Interlock Functions

This document explains the guidelines to be followed by the plant system and central interlock system responsible officers for the identification and classification of the local and central interlock functions acording to the approved MQP ITER Investment Protection Policy. The document is the first version of one of the PCDH Satellite Documents for the interlocks.

Approval Process			
	Name	*Action*	*Affiliation*
Author	**Prieto diaz I.**	**08 Dec 2017:signed**	**IO/DG/COO/SCOD/CSD/PCI**
Co-Authors			
Reviewers	**Ciusa G.** **Coatanea Gouachet M.** **Fernandez-hernando J. L.** **Liu Y.** **Pedica R.** **Petitpas P.** **Soni J.**	**14 Dec 2017:recommended** **13 Dec 2017:recommended** **11 Dec 2017:recommended** **11 Dec 2017:recommended** **15 Dec 2017:recommended** **12 Dec 2017:recommended** **08 Dec 2017:recommended**	**IO/DG/COO/SCOD/CSD/PCI** **IO/DG/COO/SCOD/CSD/PCI** **IO/DG/COO/SCOD/CSD/PCI** **IO/DG/COO/SCOD/CSD/PCI** **IO/DG/COO/SCOD/CSD/PCI** **IO/DG/COO/SCOD/CSD/PCI** **IO/DG/COO/SCOD/CSD/PCI**
Approver	**Wallander A.**	**22 Dec 2017:approved**	**IO/DG/COO/SCOD/CSD**
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, GG: TBM Committee, GG: TBM_IM_Teams, LG: FST/TBM staff, LG: TBP-WG-RWM-experts, LG: Allowed TBM-Frame Wr...**		

Change Log			
Management of Local Interlock Functions (75ZVTY)			
Version	***Latest Status***	***Issue Date***	***Description of Change***
v1.0	Signed	31 Jan 2012	
v2.0	Approved	01 Feb 2012	Comments from Izuru included. Version to be sent to Interlocks Integration Team
v3.0	Approved	24 Jan 2013	Version for PCDH v7
v4.0	Signed	28 May 2014	New version before the iFDR and after results from R&D contract and prototypes.
v4.1	Approved	10 Jun 2014	Comments from Izuru Yonekawa: 1. (Page 4/17); Please write simply as possible. Such as CIS do and not to do, PIS do and not to do. Second part is the mixture of CIS and PIS. The descripcion included in section 2 has been completed, providing more details about the functionality of the CIS and PIS. 2. (page 5/17); Need check PCDH rule. Whether this requirement is the rule or not the rule. It should be the rule. It has been added a reference to [R247] of the PCDH, to align the described requirement with the rules.
v5.0	Approved	16 Apr 2015	Section 4 - Inlcuded references from ITER Guide to Perform Hazard and Operability (2F6B9M) Section 5 - Included references to Review guidelines for Interlock Systems (PMUS5G) Section 5 - Updated specification of Local interlock functions Appendix 1 - Included references to reliability databases
v6.0	Approved	08 Dec 2017	Following sections has been added in this version: 1. figure 2, describing the flow diagram for identification and allocation of local interlock functions 2. Section 6, Verification and Validation 3. Appendix 1, example of list of Investment Protection Functions. Several minor modificaitons accoding to the feedback from Plant systems.

Table of Contents

1 Introduction

1.1 PCDH Context

The Plant Control Design Handbook (PCDH) [RD4] 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 systems into one integrated control system,
- Maintain all plant systems after delivery 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. This document is one of them.

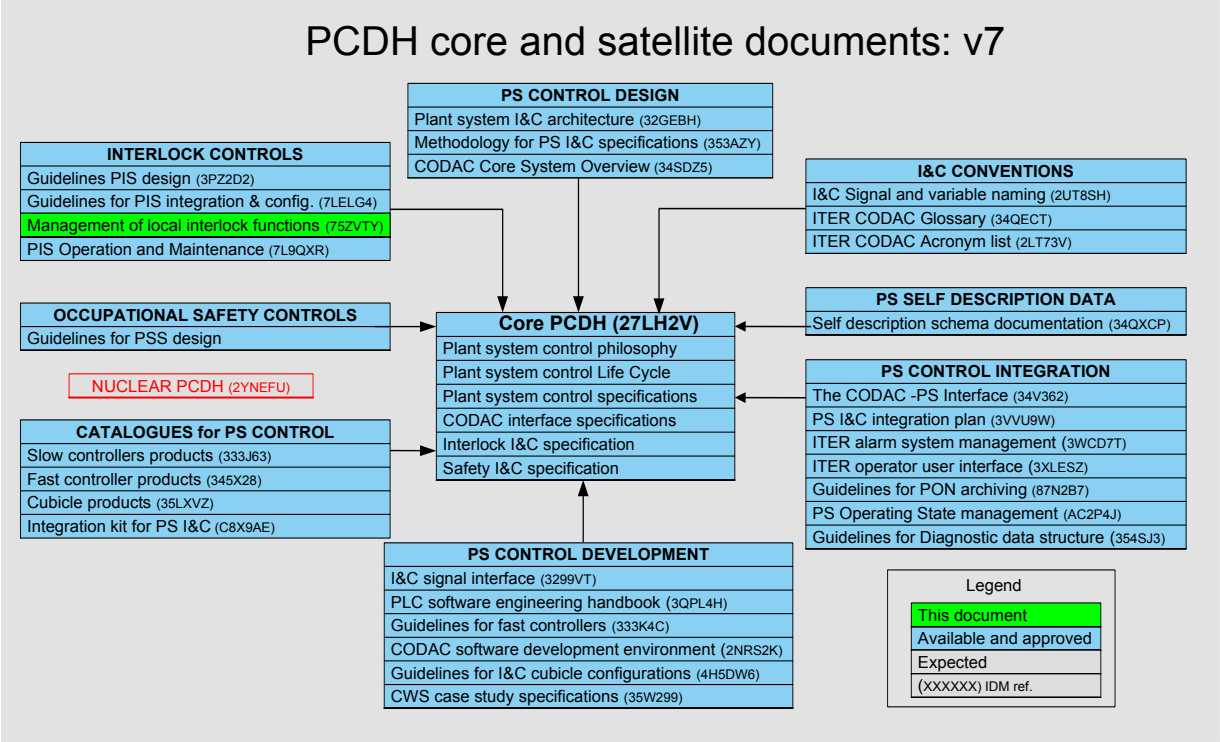

Figure 1: PCDH documents structure

1.2 Document Scope

This document provides the guidelines for the identification, classification and allocation of ITER machine protection functions. The functions are classified according to the likelihood of the risk occurring and it is according to the approved MQP ITER Investment Protection Policy [RD1].

Figure 2 provides in a graphical way how the interlock functions shall be identified and classified as per the guidelines included in this document. References to the section which describe each step in detail are included in brackets.

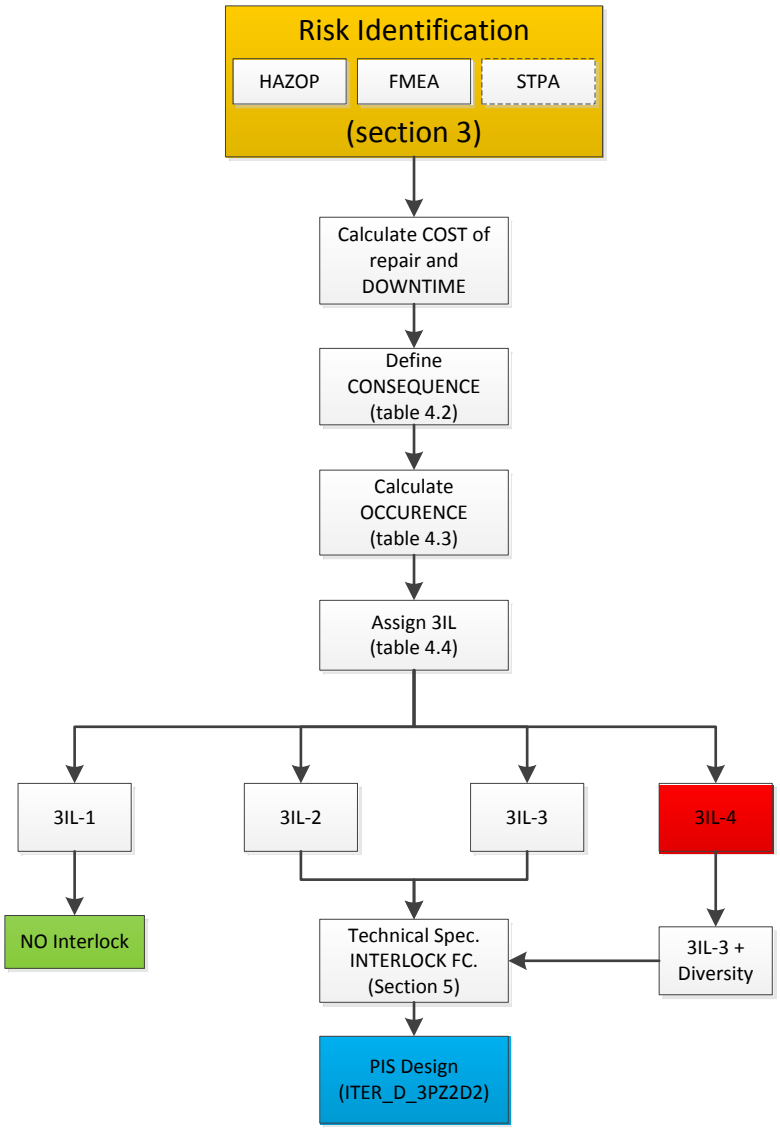

Figure 2: Flow diagram for identification and allocation of Local Interlock Functions

1.3 Acronyms

Acronym	Item
CIS	Central Interlock System
CIN	Central Interlock Network
CSS	Central Safety System
CODAC	Control, Data Access and Communication
FMECA	Failure Modes, Effects and Criticality Analysis
HAZOP	Hazard and Operability Analysis
HFT	Hardware Fault Tolerance
I&C	Instrumentation & Control
ICS	Interlock Control System
MQP	Management and Quality Program
PCDH	Plant Control Design Handbook
PE	Programmable Electronics
PIS	Plant Interlock System
P&ID	Process and Instrumentation Diagram
PS	Plant System
PSCC	Plant System Conventional Control
PSS	Plant Safety System
RAMI	Reliability, Availability, Maintainability and Inspectability Analysis
RPN	Risk Probability Number
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
3IL	ITER Interlock Integrity Level ‘tril’
STPA	System Theoretic Process Analysis.

Table 1-1: List of acronyms

1.4 Related Documents

[RD1] MQP Policy for ITER Investment Protection (ITER_D_3VUMVW)

[RD2] ITER RAMI ANALYSIS PROGRAM (ITER_D_28WBXD)

[RD3] Risk Management Plan (ITER_D_22F4LE)

[RD4] Plant Control Design Handbook (PCDH) (ITER_D_27LH2V)

[RD5] Template for RAMI Analysis Summary Reports (ITER_D_2N3SS9)

[RD6] ITER Guide to Perform Hazard and Operability (2F6B9M)

[RD7] IEC-61508 Functional safety of E/E/EP safety-related systems

[RD8] IEC 61511: Functional safety – Safety instrumented systems for the process industry sector.

[RD9] IEC 61882 Hazards and Operability Studies- Application Guide

[RD10] IEC60812 Analysis Techniques for System Reliability – Procedure for FMEA

[RD11] An STPA Primer - http://sunnyday.mit.edu/STPA-Primer-v0.pdf

[RD12] Selected component failure rate values from fusion safety assessment (INEEL/EXT-98-00892)

[RD13] Fusion Component Failure Rate Database - http://fus-se.frascati.enea.it/Home.htm

[RD14] ITER Control Breakdown Structure (CBS) (9TYFWC)

[RD15] ITER Numbering System for Components and Parts (28QDBS)

[RD16] Guidelines for the Design of the Plant Interlock System (PIS) (3PZ2D2)

[RD17] Guidelines for PIS configuration and integration (7LELG4)

[RD18] Implementation of High Integrity Operator Commands in the Interlock Control System (PKMDA8)

[RD19] Review guidelines for Interlock Systems (PMUS5G)

[RD20] STPA Preliminary analysis (SELWZL)

[RD21] List of PPTF IP functions (P9TBEJ)

[RD22] Failure Modes Effects and Diagnostics Analysis (FMEDA) Results for NI CompactRIO-based Fast Interlock System (N626Z4)

[RD23] ATN-ITER-DLIB-D3_IEC 61508 Compliance Plan v1.6 (T8G28H)

[RD24] F-LIC IEC 61508 Compliance Assessment Report (VMNWVN)

2 Introduction to ITER Investment Protection

The interlock system of ITER is only responsible for the protection of the investment; the environment and personal safety are beyond its scope. Hence, the interlock system including the CIS, PIS, networks, sensors, actuators and all other components involved in the investment protection of ITER are not concerned by the ITER licensing process.

As an essential component for the success of ITER, the interlock system will be designed, built and operated according to the highest quality standards. The international standard IEC-61508 has been chosen as the reference [RD7].

The standard introduces the notion of **Safety Integrity Level** (SIL). In order to avoid confusion with ITER terminology in which the term '**Safety**' is used only for environmental and personal safety, the term 'SIL' will be avoided in the interlock context. The term '**ITER Interlock Integrity Level**' or '**3IL**' (*tril*) is proposed to differentiate dependability levels for an interlock function.

The ICS is designed in a two layer architecture, as the best solution to follow the ITER procurement strategy and accommodate the interlock functions:

- The functionality of the Central Interlock System (CIS) is:
  - Receive the interlock events
  - Coordinate and transmit the interlock actions
  - Inform the operator about the status of all the ICS
  - Log all the critical data
  - Perform operator actions: permits and resets of central functions and override management.
- The PIS will be in charge of:
  - Detect the interlock events
  - Execute interlock actions
  - Inform the CIS about the local events/actions
  - Interface with CODAC for local operations

The CIS coordinates the central interlock functions via the Central Interlock Network (CIN) and performs them together with the PIS of the affected plant systems
The local interlock functions are executed by the PIS of the affected plant system using its own network, sensors and actuators. The CIS is only informed of the plant system change of state, as it is represented in Figure 3.

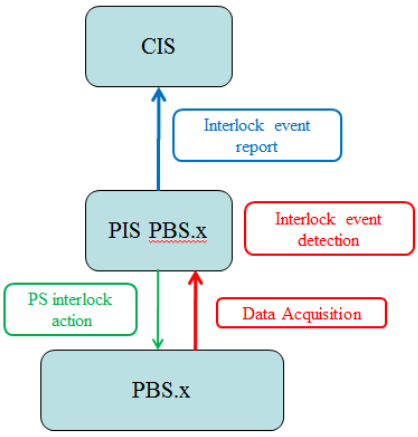

Figure 3: Local Interlock Function

3 Identification of hazards

As stated in the PCDH [RD4], one of the inputs for the design of the I&C in charge of the investment protection is the specification of the protection functions to be implemented within the plant system. The identification of the interlock functions will be based on structured methods that allow the design team to detect the potential problems that could lead to a risk for the system or the whole plant.

During the risk analysis, it can be possible to identify risks that concern both interlock (machine/systems) and safety (people/environment). In this case, it is necessary to specify both functions and follow the analysis/design process for both functions. In particular, the event likelihood, exposure, consequence of unmitigated event and mitigating actions which have an impact on the specification of the function may be different.

According to [R247] (PCDH [RD4]) and the internal protection requirement in [RD1], **each plant system must provide internal measures to detect the degradation of the utilities** required for the correct operation (e.g. Water Cooling System, Steady State Electrical Power Network, cryogenics, vacuum, etc.) and command the system to safe state. Additionally, the CIS will be informed of the event and coordinates the actions among the plant systems affected.

3.1 Methodologies

In this section three methods are presented to analyse the system under study and identify the potential risks.

HAZOP and FMECA methodologies are well stabilised industrial practices that provide a systematic approach. These studies can be initiated during the basic engineering phase of the systems, as they require that basic documentation, such P&IDs and control architectures, have been defined to be used as an input.

The third method is called STPA which is a new methodology that can be initiated during the conceptual phase of the development. This methodology is focused on the control architecture that will be implemented in the system, allowing the designer a systematic approach for specifying the investment protection requirements. STPA is not an industrial standard but it has a high potential for the identification of not evident cross relations in complex system. *The application of this methodology is recommend but it is not enforced at ITER.*

The HAZOP, FMECA and STPA methods study the system using different approaches, providing complementary results. For obtaining a complete evaluation of the hazards related to the system it is recommended to apply the three methodologies.

This section only provides guidance to understand the methodologies that can be used to identify the interlock functions at early stage of system design; it does not prevent to perform the RAMI analysis as described in [RD2].

3.1.1 HAZOP methodology

The HAZOP study is a structured and systematic evaluation of a system with the aim to identify and to arise current or potential problems that may end up presenting a risk for the system, personnel or even the whole plant.

This study will be carried out by a multidisciplinary team which provides expertise for defining the system functionality and how the deviations from normal operation may affect the global system. This group may include personnel from maintenance and operation section.

Additional information about the ITER HAZOP analysis can be found in [RD6].

3.1.1.1 Guide Words Technique

HAZOP will be based on a guide-words technique which is a deliberate search for deviations from the design intent. The whole system or subsystem will be divided into single components, called nodes, in such a way that the function and purpose of each part are clearly defined. Finally, this process will provide a worksheet with the combination of guide words and process parameters, as well as the causes, consequence and mitigation actions of each of these deviations.

The HAZOP team will study sequentially each node of the itemized system in order to detect the deviations from the design's intent which can lead the system to an adverse state. As a basis of the HAZOP study, the team should have process diagrams and studies, such as P&IDs, one-line diagrams or isometric diagrams in order to achieve the most comprehensive knowledge of the system and the interactions among its components.

Once the nodes have been properly defined, the team will run the "guide words" process. This will have the aim to identify unexpected and yet credible deviation from intended design by asking key questions. For that purpose, the IEC 61882 [RD9] proposes a group of pre-established guide words, which are listed in Table 3-1.

Guide Word	Meaning
No or not	Complete negation of the design intent
More	Quantitative increase
Less	Quantitative decrease
As well as	Qualitative modification/increase
Part of	Qualitative modification/decrease
Reverse	Logical opposite of the design intent
Other than	Complete substitution
Early	Relative to the clock time
Late	Relative to the clock time
Before	Relating to order or sequence
After	Relating to order or sequence

Table 3-1: Guide Word List

These guide words will apply to the parameters of the system or process. These parameters may be commonly classified into the next groups:

- Physical parameters related to input medium properties
- Physical parameters related to input medium conditions
- Physical parameters related to system dynamics

Typical process parameters include: Flow, Pressure, Temperature, Level, Viscosity, Reaction, Composition, Addition, Separation, Time, Power, Phase, Speed, Particle size, Measure Control, Data flow.

Table 3-2 provides an example of combination of guide words and process variables. The team in charge of the HAZOP is encouraged to define a relevant combination applicable to the system under analysis.

	GUIDE WORDS						
PROCESS VARIABLES	**No, Not, None**	**Less, Low, Short**	**More, High, Long**	**Part of**	**As Well As Also**	**Other Than**	**Reverse**
Flow	No flow	Low rate Low integrated flow	High rate High integrated flow	Missing feed, Condensation or adsorption	Additional feed, Evaporation or desorption	Wrong material	Backflow
Pressure	Open to atmosphere	Low pressure	High pressure				
Temperature		Low temperature	High temperature			Phase change	
Confinement	Rupture	Leaks		Single Barrier	Tritium Diffusion	Relief Path	In-leakage
Radiation		Low levels of radiation	High levels of radiation		Additional rad type	Other than expected rad type	
Shielding	No shielding	Less shielding				Wrong shielding material	
Reaction	No reaction	Slow reaction	Runaway reaction	Partial reaction	Side reaction	Wrong reaction	Decomposition
Concentration	Material not present	Low concentration	High concentration		Additional material present	Wrong material present	
Magnetism			High field				
Power	Long power failure	Short power failure	Power surge	Insufficient Power	Improper Ground	Wrong Power AC/DC	Reverse Polarity
Level/Capacity	Empty	Low level Underfilled	High level Overfilled			Wrong material	
Speed	Stopped	Too slow	Too fast	Out of sync		Disconnect (drive shaft or belt break)	Backward
Co-located systems and dependencies	Loss of dependent system	Reduction in dependent system	Excess from co-located system	Other systems competing for dependent system		Impact of co-located systems	
Vibration		Small	Large (EQ)	Intermitted (chronic affect)			
Access	Cannot access	Limited access	Entrapment			Unauthorized Access	
Procedure	Skipped step			Partially-completed step	Extra action(s) (shortcuts)	Wrong action	Out of order, Opposite

Table 3-2: Example of Deviations, extracted from [RD6]

Every deviation from the intended design will be caused by some reason that shall be revealed using this technique. It is recommended to start with the causes that may bring the worst consequences to the system or process. Generally, the causes may be summarized in the following three groups:

- Human Errors: Include all faults regarding any misbehaviour (deliberate or not) of designers, constructors, operators or any other actor that may lead to a hazard to the system or process
- Equipment Failures: include any malfunction of the components of the system or process that may be caused by inappropriate operation, ageing or random failures.
- External Events: Comprise all unexpected situations that may occur due to failures on the surrounding s of the system failure or exposure to nature effects such as weather, seismic activity, etc.

These consequences are defined as results of deviations from the intended design that may lead the system or process to undesirable conditions. Different consequences may originate from the same cause, and one consequence may have several causes.

The HAZOP Team shall consider all the concepts above mentioned and provide responses to reduce the occurrence or the consequences of the deviations, proposing functionalities to be implemented by the I&C systems:

- Identification of the deviations: Alarms, HMI, human detection
- Automatic actions to compensate the deviation: to be implemented in the Conventional control system
- Prevention of the deviation: Sensors to avoid exceeding safe operating limits
- Interlock functions to prevent a further escalation of the deviation.
- Interlock functions to relieve the process or system from the deviation

The HAZOP team may propose an additional set of actions required to eliminate or minimize the impact of the consequences over the system, such as design changes or preventive maintenance plans.

All this work will be presented in a worksheet such as Table 3-3.

Parameter	Guide word	Deviation	Possible causes	Consequences	Safeguards	Comments	Actions required

Table 3-3: HAZOP worksheet fields

A further explanation of the HAZOP Procedure is included in Figure 4, based on IEC 61882 [RD9].

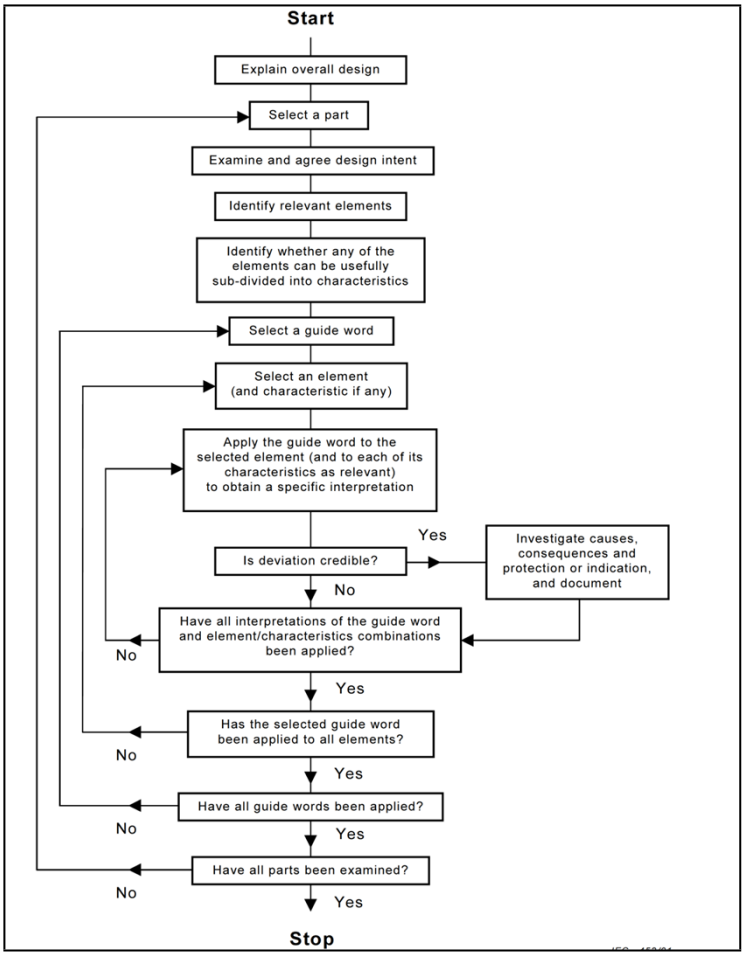

Figure 4: HAZOP Flow Chart

3.1.2 FMECA methodology

This section describes the methodology to be applied during the FMECA studies, defining all the considerations to be taken into account along the process.

FMECA is a systematic technique used to identify asses, prioritize and eliminate potential failures from the system, design or process before they may cause a damage to it.. The IEC 60812 [RD10] provides guidance in the application of the methodology.

A FMECA analysis consists of the following stages:

3.1.2.1 Identification of the component of the system

This step aims at identifying the components that belong to the system over a diagram (P&ID, one line diagram…), establishing the boundaries of the system and the interfaces among other systems of the plant.

This point shall also include all the functions of an item.

3.1.2.2 Identification of the failure modes

After the identification of the components within the scope of the study, the next point is the consideration of all modes of failure of the system. This involves the definition of the cause of a failure and its detection method, for each failure mode of each component.

3.1.2.3 Identification of the effects over the system

The study identifies the potential effects over the system regarding the potential failure modes.

The effects may affect as below stated:

- *Local Effects*: The nature of the effect only affects the component or item
- *Next Higher Level Effects*: The nature of the effect affects the immediately higher level assembly
- *End Effects*: The nature of the effect affects the top of the system

3.1.2.4 Evaluation of the potential effect risks

According to RPN Method, the risk associated to a failure mode is a function of the following three factors: Detection, Severity and Occurrence. The product of these factors represents the RPN value, so it takes into consideration the severity of each failure mode, its likelihood of occurrence and the likelihood of detection.

The expert shall establish a ranking for these three parameters, taking into account that this is only a subjective way to obtain a figure. This figure will provide a weighting to assume the corrective actions.

Finally, the initial RPN and the expected RPN are defined for each failure mode, assuming the effects of the corrective actions.

The ranking established for the RPN, according to [RD3], is the following:

Value	Description	Meaning
1	Weak <1h	Unavailable less than 1 hour
2	Moderate <1d	Unavailable between 1 hour and 1 day
3	Serious <1w	Unavailable between 1 day and 1 week
4	Severe <2m	Unavailable between 1 week and 2 months
5	Critical <1y	Unavailable between 2 months and 1 year
6	Catastrophic >1y	Unavailable more than 1 year

Table 3-4: Severity rating

Value	Description	Meaning	
1	Very Low	λ_{risk} < 5e-4/y	λ_{risk} < 5.7e-8/h
		MTBF > 2000 years	
2	Low	5e-4/y < λ_{risk} < 5e-3/y	5.7e-8/h < λ_{risk} < 5.7e-7/h
		200 years < MTBF < 2000 years	
3	Moderate	5^{e}-3/y < λ_{risk} < 5^{e}-2/y	5.7e-7/h < λ_{risk} < 5.7e-6/h
		20 years < MTBF < 200 years	
4	High	5e-2/y < λ_{risk} < 5e-1/y	5.7e-6/h < λ_{risk} < 5.7e-5/h
		2 years < MTBF < 20 years	
5	Very High	5e-1/y < λ_{risk} < 5/y	5.7e-5/h < λ_{risk} < 5.7e-4/h
		10 weeks < MTBF < 2 years	
6	Frequent	λ_{risk} > 5/y	λ_{risk} > 5.7e-4/h
		MTBF < 10 weeks	

Table 3-5: Occurrence rating

Value	Description	Meaning
1	Very Easy	Easy failure detection by human or system, or detection with high level coverage monitoring means (dedicated interlock/safety system, internal or external to the control system)
2	Easy	Automatic failure detection by control or monitoring system (medium coverage diagnostics)
3	Moderate	Failure detected by combined means of control or monitoring system (displays) and human intervention (within procedures)
4	Hard	Failure detected through external additional means (typically preventive maintenance operation)
5	Very Hard	No failure detection (cannot be detected)

Table 3-6: Detection rating

Nevertheless, the RPN Method presents several limitations that shall be considered:

- How the ranks of Detection, Severity and Occurrence have been defined depends on the particular application and the selected FMECA Standard
- Detection, Severity and Occurrence ranks may have different meanings for each FMECA
- RPN is only a “figure” which represents a comparative value. In some occasions, it is preferred to prioritize either by Occurrence / Severity Matrix (also known as Risk Matrix) or by Single Rating

3.1.2.5 FMECA Review

FMECA constitutes a continuous task that will be assessed along the lifetime of the project, receiving and introducing new inputs and data from the operation, maintenance and engineering departments, such as described in the flowchart below.

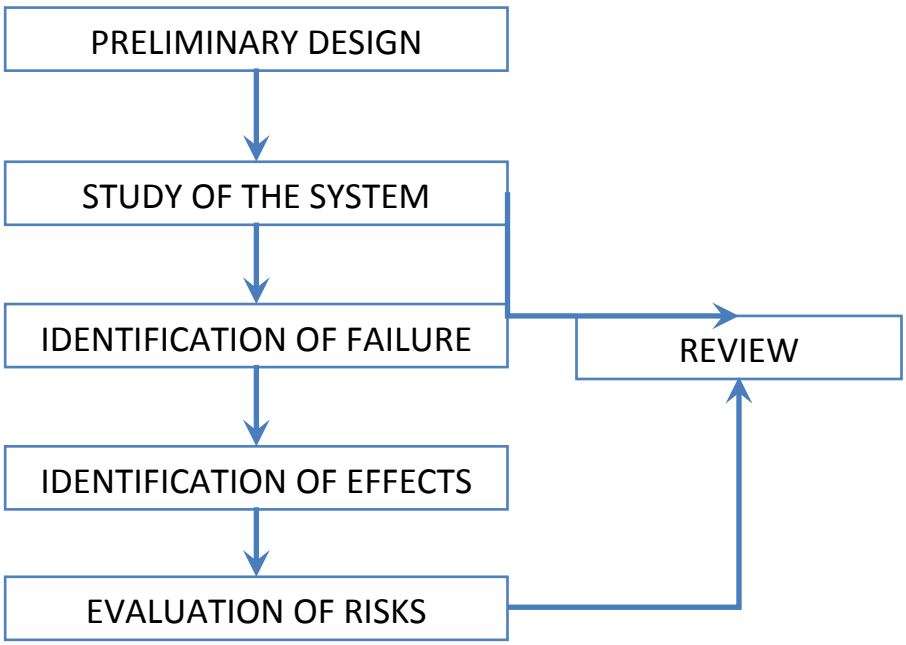

Figure 5: FMECA flow chart

3.1.3 STPA Methodology

System-Theoretic Process Analysis (STPA, [RD11]) is a method for performing a risk analysis, allowing to take into account the dependability requirements since the early stages of the design.

STPA consists in the definition of few general scenarios in which the system constraints could be violated (Accident), the set of conditions which could potentially lead to their occurrence (Hazard) and the corresponding requirements for the control structures which should handle this scenarios. As the knowledge of the system increases, requirements can be refined and control structures detailed accordingly.

The design of the protection systems is particularly suitable for STPA, as it has to be carried out while other systems are still under design. The choice of defining high-level control structures, which can be refined according to the updated design status of the different plant systems, is the best solution for assuring the required flexibility to cope with new hazards, which were not taken into account in the previous iterations.

An example of application of this methodology can be found on [RD20].

3.1.3.1 Identification of High Level Requirements

The process for the identification starts with the definition of the accidents and hazards of the system under study. For the purpose of the procedure described in this section, the following concepts shall be used:

- Accident: An accident is an undesired and unplanned event that results in a loss. In the case of the interlock system the accidents shall be defined as a reduction of the machine availability in the current operational campaign, according to Table 4-1
- Hazard: A system state or set of conditions that, together with a worst-case of environmental conditions, will lead to an accident (loss).

After the identification of the accidents and the related hazard, from the system point of view, they shall be translated into high level requirements.

It is recommended to summarize the analysis in one table, as per Table 3-7

Accident	Hazard	High level Requirements
A1	H1	
A2	H2	
…	….	

Table 3-7: Definition of Accident, Hazards and High Level requirements

3.1.3.2 Definition of the functional control structure

The deducted high level requirements can be fit in a generic control structure, with the components responsible to cope with listed hazards. The iteration of this method, refining the hazards definition and consequently the requirements for the control structure, yields to a more detailed schema. Figure 6 provides a representation of a generic control structure.

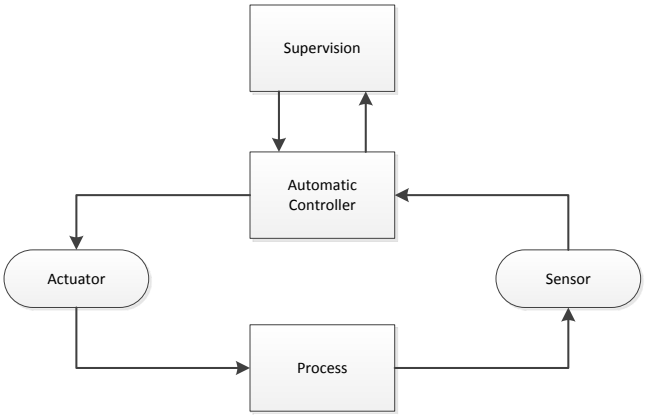

Figure 6: Generic Control Structure

3.1.3.3 Step 1: Identify Hazardous Control Actions.

An STPA considers Investment Protection as a control problem. The goal is to control the behaviour of the components and systems as a whole to ensure that the operational constraints are enforced in the system. The events are the result of the inadequate control, instead of preventing the failures the system shall enforce the constraints on system behaviour, based in four types of hazardous control actions that need to be eliminated or controlled to prevent accidents:

1 A control action required for the system protection is not provided or is not followed
2 An hazardous control action is provided
3 A potentially adequate control action is provided too late, too early, or out of sequence
4 A control action is stopped too soon or applied too long

Each item in the Table 3-8 should be evaluated to determine whether it is hazardous as defined by the system-level hazards. If this situation is a Investment Protection concern, then the hazard list can be updated to include the corresponding hazard.

Hazard:					
Element	Control Action	Providing causes hazard	Not providing causes hazard	Too early, too late, wrong order	Stopped too soon / Applied to long

Table 3-8: Identification of hazardous control actions

These hazardous control actions are used to create protection requirements and constraints on the behaviour of both the system and its components.

3.1.3.4 Step 2: Identify casual factors and control flaws.

The second step of the STPA examines each control loop in the control structure to identify potential causal factors for each hazardous control action, i.e., the scenarios for causing a hazard. While STPA Step One focused on the provided control actions Step Two expands the analysis to consider causal factors along the rest of the control loop

3.1.3.5 Generate System protection requirements

Once the second step of STPA has been applied to determine potential causes for each hazardous control action identified in STPA Step One, the causes should be eliminated or controlled in the design.

The protection functions will be defined according to the identified requirements.

4 Allocation of Interlock Function

4.1 Classification

After the completion of the risk analysis of a plant system, it is possible to estimate the probability of the risk's occurrence and its consequences if it is not mitigated. These values determine the 3IL required for the associated protection function (local or central).

The consequences of a non-mitigated risk are classified by [RD1] into four categories:

- Catastrophic
- Major
- Severe
- Minor

Table 4-1 and Table 4-2 quantify these four categories according to the special characteristics of the ITER Project. Unlike an industrial facility in which it is relatively easy to quantify the economic losses derived from a temporary shutdown, at ITER it is almost impossible to quantify the cost of one day without plasma: from a financial point of view stopping ITER for a period of time can save money since operational costs (e.g. electricity, helium, operator shifts, etc.) will be reduced, whereas the scientific cost could be enormous.

A simple (and wrong) approach to this problem is to divide the total cost of the ITER Project by its expected lifetime. However, the value of ITER operation will not be linked to the cost of the machine/system since the value of its goals is many orders of magnitude larger.

The solution is not to associate a cost with ITER downtime after an incident but to take into account both the cost of repair and the expected downtime. The combination of these two parameters will be used to evaluate the consequences of the incident.

Category	Criteria
Catastrophic (Ca)	Disastrous threat to ITER's mission, abandonment of the project and goals
Major (Ma)	Loss of a full operational campaign, moderate threat to ITER's mission
Severe (Se)	Significant reduction of an operational campaign program
Minor (Mi)	No significant impact on the operational campaign program

Table 4-1: Qualitative Consequence categories

	Machine/System Unavailability						
Cost	< 1h	< 1 day	< 1 week	< 2 month	< 1 year	< 2 year	> 2 year
< 0.1 M€	Mi	Se	Se	Se	Ma	Ma	Ca
< 1 M€	Se	Se	Se	Se	Ma	Ma	Ca
< 10 M€	Se	Se	Se	Ma	Ma	Ma	Ca
< 50 M€	Ma	Ma	Ma	Ma	Ma	Ma	Ca
<500 M€	Ma	Ma	Ma	Ma	Ma	Ca	Ca
> 500 M€	Ca	Ca	Ca	Ca	Ca	Ca	Ca

Table 4-2: Quantitative consequence categories

The six frequency categories applicable to ITER Interlocks are listed in Table 4-3.

Category	Description	Yearly frequency level
Frequent	Event occurs very likely	> 5
Probable	Event is likely to occur	0.5 – 5
Occasional	Event possible and expected	0.05 – 0.5
Remote	Event possible but not expected	0.005 – 0.05
Improbable	Event unlikely to occur	0.0005 – 0.005
Negligible	Event extremely unlikely	< 0.0005

Table 4-3 Occurrence probability in events per year

Probability of occurrence for some specific fusion components can be found in [RD12] and [RD13]. *Appendix 1 lists additional sources of component failure rates.*

The required level of protection (3IL) for a certain risk can be obtained (according to IEC-61508) by combining the values given by Table 4-1, Table 4-2 and Table 4-3

Event Likelihood	Consequence			
	Catastrophic	Major	Severe	Minor
Frequent	3IL-4	3IL-3	3IL-3	3IL-1 (no interlock)
Probable	3IL-4	3IL-3	3IL-3	3IL-1 (no interlock)
Occasional	3IL-3	3IL-3	3IL-2	3IL-1 (no interlock)
Remote	3IL-3	3IL-2	3IL-2	3IL-1 (no interlock)
Improbable	3IL-3	3IL-2	3IL-1 (no interlock)	3IL-1 (no interlock)
Negligible	3IL-2	3IL-1 (no interlock)	3IL-1 (no interlock)	3IL-1 (no interlock)

Table 4-4 Minimum ITER Interlock Integrity Level required

Table 4-5 provides the equivalence between the 3IL and the SIL as per IEC 61508 [RD7] and the ITER I&C implementation for such requirement, as specified by [RD1].

Minimum Interlock Integrity Level	**Quality Class**	**Equivalent SIL**	**I&C Implementation**
3IL-4	QC-1	SIL-3	High Integrity Interlock with diversity (e.g. PLC + hardwired I&C)
3IL-3	QC-2	SIL-3	High Integrity Interlock
3IL-2	QC-3	SIL-2	Low Integrity Interlock
3IL-1 (no interlock)	QC-3	SIL-1	Conventional Control (no Interlock)

Table 4-5: Minimum 3IL required and equivalence with QC and SIL (IEC 61508)

If the analysis results in a 3IL-4 level being assigned to an investment protection instrumented function, consideration shall be given to change the process design in such a way that it becomes more inherently safe or adding additional layers of protection. These enhancements could possibly reduce 3IL requirements for the protection function.

Investment protection functions with a 3IL higher than level 4 shall be avoided where reasonably practicable given the difficulty of achieving and maintaining such high levels of performance throughout the overall life cycle. Where such systems are specified they will require high levels of competence from all actors involved throughout the life cycle.

4.2 Target integrity

To be compliant with the recommendations of IEC 61508, a system providing interlock functions should meet the following reliability design requirements:

- Qualitative requirements on fault behaviour, i.e. define a safe state in case of failure
- Quantitative requirements translated into probability of loss of function, i.e. probability of failure on demand (PFD) or probability of failure per hour (PFH)

Table 4-6 lists the 3IL levels and the corresponding failure probabilities (the same than for corresponding SIL levels) and the I&C architecture for its implementation as described in the PCDH [RD4].

3IL	I&C Implementation	Average probability of a dangerous failure on demand of the interlock function operating in low demand mode of operation (PFD_{avg})	Average frequency of a dangerous failure of the interlock function [h^{-1}] operating in high demand mode of operation or continuous mode of operation (PFH)
3IL-1	Conventional Control (no interlock)		
3IL-2	Low integrity interlock	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3IL-3	High integrity interlock	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
3IL-4	High integrity interlock with diversity	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$

Table 4-6: 3IL requirements

Note: The high demand mode is applicable if the number of demands is greater than one per year.

Examples of PFD /PFH calculation can be found on [RD22], [RD23] and [RD24].

4.3 Implementation

Local investment protection I&C functions will be implemented in the PIS architecture which is able to perform 3IL-2 and 3IL-3 interlock functions. Functions with 3IL-1 level can be implemented by the conventional I&C tier.

The IEC-61508 standard also introduces the notion of minimum **Hardware Fault Tolerance** (HFT). The hardware fault tolerance is the ability of a functional unit to continue to perform a required function in the presence of faults or errors. A hardware fault tolerance of 2 means that there are, for example, three devices and the architecture is such that the failure of two of the three components or subsystems does not prevent the protection action from occurring.

The minimum hardware fault tolerance required for PE logic solvers depends on the Safe Failure Fraction (SFF) of the PE logic solver, as per Table 4-7.

SFF	Hardware Fault Tolerance		
	0	1	2
< 60%	Not Allowed	3IL-1	3IL-2
60% - < 90%	3IL-1	3IL-2	3IL-3
90% - < 99%	3IL-2	3IL-3	
≥ 99%	3IL-3		

Table 4-7: HFT requirements of PE logic solvers

For sensors, final elements and non-PE logic solvers Table 4-8 represent the minimum hardware fault tolerance required takes into account the type of device, according to IEC 61511 [RD8]:

- Case 1: The dominant failure mode does not lead to the safe state and dangerous failures are not detected.
- Case 2: The dominant failure leads to safe state or dangerous failures are detected.
- Case 3: The hardware of the device is selected on the basis of prior use, the device allows adjustment of process-related parameters only, these adjustments are protected and the function has a 3IL requirement of less than 4.

3IL	Minimum Hardware Fault Tolerance		
	Case 1	Case 2	Case 3
3IL-1	1	0	0
3IL-2	2	1	0
3IL-3	3	2	1

Table 4-8: HFT requirements of sensors, final elements and non-PE logic solvers

5 Technical Specification of Local Interlock Functions

A technical specification of all the local interlock functions shall be provided per plant system, in order to design the Plant Interlock System and proceed with the design, configuration and final integration with the CIS.

The document that collects all local interlock function shall be provided by the Plant System's Responsible Officer or delegated, as part of the list of the main protection functions to implement within the plant system or with respect to other plant systems (Input I&C document I7 according to section 3.4.2 of the PCDH [RD4]).

Special attention has to be paid to the data involving the local interlock function, so that interlock events and actions are well defined, functional interfaces are clear and an integrity level target (3IL) is assigned for every member of the interlock chain from sensor to actuator. Finally, the implementation of the function is included (diagrams, architecture, redundancies) and other information such as ITER Operator required actions is provided.

Appendix 1 and [RD21] provides an example on how to list and summarize the required information for the classification of the Investment Protection functions.

Additionally, each local interlock function shall be specified according to section 10 of IEC 61511-part 1 [RD8]. Table 5-1 proposes a format for the technical specification of the local interlock functions, summarizing the main pieces of information required:

Function	Title	
	Description	
	PBS	
	PS I&C / PA	
	CBS	
	Consequence	
	Occurrence	
	3IL Level	
	Time Requirement	
Sensor	Functional Reference	
	Description	
	Voting Scheme	
	PFH / 3IL Budget	
Controller	Functional Reference	
	Description	
	CBS Function	
	Technology	□ Slow F □Slow FH □Fast
	PFH / 3IL Budget	
Actuator	Functional Reference	
	Description	
	Safe State	
	Voting Scheme	
	PFH / 3IL Budget	
Operation	Function Reset	□Automatic □ Manual
	Predefined thresholds	
	OVERRIDES (From CIS)	
	Input Masking	
	Function Disable	□ Yes □No
	Output Forcing	
Links	Functional Breakdown	
	RAMI Analysis	
	3IL Assessment	
	IDS with PBS 46	
	Architecture	
	Cause & Effect Matrix	
	Datasheets	
Comments		

Table 5-1: Local Interlock Function Specification Template

5.1 Function

The title of the function shall be self-descriptive, in order to provide an easy understanding of the functionality of the specific function. The function is described more in detail in the field "description", which provides a textual summary indicating which machine component is protecting and what is the risk covered by this function.

The next three fields provides the identification of the function with the ITER project, by means of the PBS, Procurement Agreement identification and CBS up to level 3 according to [RD14].

The consequences, occurrence and 3IL of the function shall be stated according to the result of the 3IL assessment performed to the system, as described in section 4 of this document

The last field of the function block specifies the required response time for the function to bring the process to a safe state within the process protection time. If the required performance for the function has not been assessed yet, a qualitative approach can be used. 100 ms is the boundary between fast and slow local functions, so if the mitigation action is required to be faster than 100ms the function should be classified as "fast".

5.2 Sensors and actuators

The functional reference of the sensors or actuators is detailed in the first field of the description, in the form of PPPPPP-TTT-NNNN as per. [RD15]

A brief description of the sensor or the actuators shall be included, indicating the type of measurement carried out. Additional information such as thresholds or other relevant information related to the sensors or actuators shall be included if available.

For the actuators, a definition of the safe state of the process shall be included, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated.

The voting schema (1oo1, 1oo2, 2oo2, 2oo3, 2oo4, etc.) shall be also indicated.

The last parameter to be included is the integrity level of the sensors; the PFH value provided by the manufacturer shall be indicated. In the case of the parameter is not available an estimation of the 3IL budget should be indicated. For 3IL-3 function the total budget is 1E-7 and for 3IL-2 functions is 1E-6.

Example: if according to the SIL certification of a sensor, the PFH value of a 2oo3 voting schema is equal to 2.5E-8 the 3IL budget for a 3IL-3 function will be equal to 25%, and for a 3IL-2 function will be 2.5%.

The PFD (Probability of failure on Demand) values can be used if the function is requested to be trigger less than once per year.

5.3 Controllers

In addition to the fields described in section 5.2, the CBS identification of the function shall be indicated.

The configuration of the controller is selected from the following options:

- Slow F: Single CPU
- Slow FH: Fully fault tolerant
- Fast: Fast interlock controller

For additional details refer to Guidelines for the Design of the Plant Interlock System (PIS) (3PZ2D2)

5.4 Operation

Any requirement related to the procedures for starting up and resetting shall be indidcated. If a reset of the function is required before the normal operation can continue and the type of reset (manual or automatic) shall be indicated.

The threshold of an interlock function can be adjusted during normal operation according to a predefined list of values (up to 16). This field is intended to be used to specify these values.

All overrides applied in the interlock system will be managed by the CIS. There are three different possibilities to apply an override:

- Masking of inputs
- Forcing of outputs
- Disabling of functions.

A written procedure for each override shall be provided to describe how the bypasses will be administrated, controlled and cleared. For additional details about the implementation of this operation mechanisms refer to section 5.1.3 of [RD17] and to [RD18]

5.5 Links

This section of the technical specification is intended to summarize all the required links that support the function, such as:

- Functional Breakdown Analysis
- Rami analysis: like HAZOP or FMECA analysis performed to the system
- 3IL assessment: to classify the interlock functions.
- Interface Data Sheet with PBS 46, providing the signal list between the PIS and the CIS.
- The PS I&C architecture
- Cause & Effect matrix or logic diagrams to support the implementation of the interlock functions.
- Datasheets of the components

5.6 Comments

If additional remarks shall be included, and they do not fit in any of the above mentioned fields, it can be included here.

6 Verification and Validation

Each interlock function shall be implemented as specified taking into account the identified requirements and constraints. Not only a verification of compliance with its specifications, requirements and recommendations shall be performed, but also validation that these enable allows achieving a sufficient functional safety, correctly documented.

The main objectives of the verification & validation activities related IEC 61508 [RD7] requirements are to:

- Demonstrate, for each phase of the overall, E/E/PES and software lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.
- Test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.
- Integrate and test the Interlock systems.
- Ensure that the design and implementation of the Interlock systems meets the specified Investment Protection functions and ITER Interlock Integrity (3IL) requirements.
- Plan the validation of the Interlock systems.
- Validate that the Interlock systems meet, in all respects, the requirements for Investment Protection in terms of the required functions and the integrity level.

Each plant system supplier is fully responsible for the 3IL level of its local interlock functions throughout their lifecycle, as defined in the applicable standards [RD7] and [RD8] and that the system will complete its actions (in the worst case response time) within one-half of its allocated process safety time (Refer to section .2.4 of [RD16]).

PBS.46 is responsible of the central interlock functions but plant systems suppliers provide part of them and they must ensure that the ICS requirements can be met, especially the integrity level and response time.

As PIS event detection and PIS risk mitigation can proceed in parallel, the time to react allocated for a central function can be divided in 3 parts.

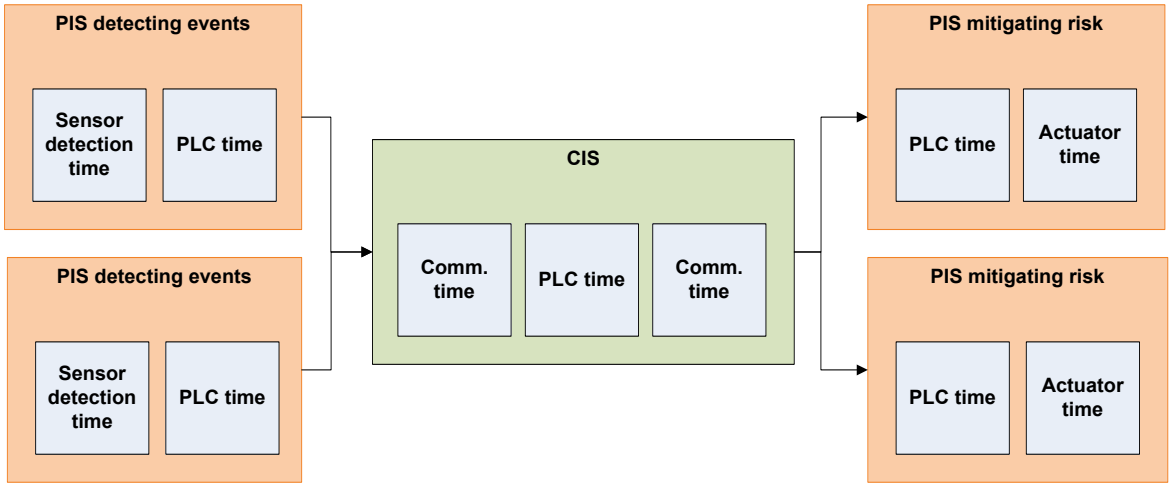

Figure 6-1: PIS validation of central function

As all the PIS event detection and all the PIS risk mitigation must be taken into account when calculating the 3IL level of a central function, the 3IL level allocated for a central level has to be divided into as many parts as there are in the PS involved in the function.

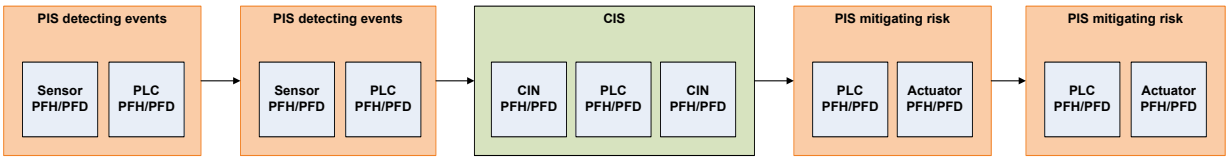

Figure 6-2: 3IL validation of central function

Considering the integrity, the CIS will probably participate in 15% of the 3IL-3 functions and so 1.5% of the 3IL-2 functions.

Each plant system must provide the documentation concerning its part of the interlock function (functions specification, functional analysis, justification of “proven in use” components, IEC 61508 assessment, calculations for SIL compliance, FAT report, response time validation in the worst case, SAT report, datasheets, user/maintenance manual and procedures…) as described in Plant Control Design Handbook [RD4].

[RD19] provides a complete guideline about the Interlock I&C system compliance with the project life cycle.

Appendix 1: List of Investment Protection Functions

Example of [RD21]List of PPTF IP functions (P9TBEJ)

Risk description				Unmitigated risk								Mitigation					
Name of Function	Effect	Hazardous event description	Hazardous event consequence	Machine unavailability		Failure cost		Risk categorisation (table 4-2)	Failure rate /year (table 4.3)		Integrity level (table 4.4)	Detection of the event	Protection action	Response time required	Conventional control or interlocks (table4.5)	Mitigation	Function specification
				Description	S	Description	Cost		Description	λ							
Protection of the Vacuum System against an overpressure	In case of overpressure inside the Test Tank (leakage), the vacuum system may be damaged by a sudden pressure rise (up to 1.5 bars). The function shall detect a rise of pressure and isolate the Vacuum System from the Test Tank.	Water leak in PP during baking	Vacuum System damaged	No	< 1h	PBS 58: turbomolecular pumps	<0.1 M€	Minor	Remote	1.E-02	3IL-1	PBS 58	PBS 58	Above 100ms	Conventional control	Isolate the vacuum system (valves)	Conventional control
Protection of the test stand and PP against a too high temperature during baking	A too high temperature in the PP could damage some components. This function shall cut the electrical heater if the temperature would raise above the threshold of 250°C.	High temperature (> 250°C) generated by the PPTF heater	Damage the PP	PPTF: No PP: No	< 1h	PBS 58: instrumentation damaged PP: no (TBC)	<0.1 M€	Minor	Improbable	1.E-03	3IL-1	PBS 58	PBS 58	Above 100ms	Conventional control	In case T > 250°C, the test stand heater must be shut down	Conventional control
Cooling parameters are not good during IC antenna RF power test	During a functional test in the PPTF the cooling is managed by PBS 58. In case these parameters go out of safe IC H&CD operation range then the action is to stop/inhibit RF power of IC H&CD. See Central Interlock System Strategy for ITER Heating and Fuelling Protection: Machine Protection Functions (JKYRME v1.5) section 4.11	The IC antenna injects RF power during functionnal tests which dissipates in the PP and the TT shell.	The PPTF cooling may not be sufficient or enough localized. If the temperature in any of the PP or TT shell raises too much it may dammage some PP components or weaken the TT structure.	PPTF: 2 months PP: 2 months	< 2 months	PPTF: no impact PP: 1 M€	<1 M€	Severe	Remote	1.E-02	3IL-2	PBS 58	PBS 51	Above 100ms	Low-Integrity Interlock	The operating temperature is 100°C	Detailed I&C Interlock Function Specification for "Cooling parameters are not good during functional test" (PSQSM3)
Protection of the IC antenna in case of loss in vacuum in PPTF test tank	If RF power is on and the pressure inside the Test Tank is too high (limit to be defined by PBS 51), RF power must be stopped. See Central Interlock System Strategy for ITER Heating and Fuelling Protection: Machine Protection Functions (JKYRME v1.5) section 4.12	Loss of TT vacuum, P > 10-2 Pa Note: to keep a suuficient safety margin, the function will be triggered for P > 10-3 Pa	Damage the IC antena	PPTF: no impact PP: 2 months	< 2 months	PPTF: no impact PP: 1 M€	<1 M€	Severe	Improbable	1.E-03	3IL-2	PBS 58	PBS 51	Above 100ms	Low-Integrity Interlock	In case in TT P > 10-3 Pa by PBS 51: RF power must be cut off	Detailed I&C Interlock Function Specification for "Protection of the IC antenna in case of loss in vacuum in PPTF test tank" (PREF64)
Protection of CHWS-H2 against a leak in the PPTF Heat Exchanger	Transfer of water from the PPTF pressurizer to the CHWS-H2 pressurizer	Water leak in the PPTF heat exchanger	Rise of pressure/volume in CHWS-H2, which is protected by relief valves	No	< 1h	Flooding of max 5 m3	<0.1 M€	Minor	Improbable	1.E-03	3IL-1	PBS 58	PBS 58	Above 100ms	Conventional control	In case P (PPTF secondary loop) > 1 Mpa: Isolate the Heat Exchanger	Conventional control

Appendix 2: Databases of Component Failure rate

The following component failure rate databases can support the frequency estimation:

1. INEEL/EXT-98-00892
   Selected component failure rate values from fusion safety assessment tasks.
2. Fusion Component Failure Rate Database
   https://user.iter.org/?uid=EFPDV9
3. FEVE.
   This database collects data from European Air Liquide plants operated by "Large Industry department" of the Air Liquide Group. Most of these plants are Air Separation Units (ASU). Data has been collected since 1994.
4. OREDA 2002, 2009 (Offshore REliability DAta).
   This data has been collected from offshore units. We consider that offshore conditions are more severe than onshore ones. These data are organized by nature of failure such that one can easily identify, for instance, how many failures are due to instrumentation and how many are due to the equipment itself.
5. EIReDA (European Industry Reliability Data Bank, 1998).
   The data bank comprises estimates of reliability parameters, failure rates and probabilities of failure, for equipment as pumps, tanks, valves, motors, sensors, etc. Estimates were based on operation and failure data collected from 1978 to 1995 in nuclear power plants operated by Electricité de France.
6. CCPS - Center for Chemical Process Safety
   Guidelines for Process Equipment Reliability Data, 1989.
7. IEEE (Institute of Electrical and Electronics Engineers) database.
8. EXIDA database
   http://www.exida.com/SAEL
9. IAEA-TECDOC-478
   Component Reliability Data for Use in Probabilistic Safety Assessment
10. IAEA-TECDOC-930
    Generic Component Reliability Data for Research Reactor PSA
11. SRS-332 Bellcore/Telcordia Reliability Prediction in Lambda Predict