IDM UID
3VUMVW
VERSION CREATED ON / VERSION / STATUS
05 Feb 2025 / 5.0 / Approved
EXTERNAL REFERENCE / VERSION

Rules or Handbooks or Guidelines

ITER Investment Protection Handbook

This document defines the strategy and policies for ITER Investment Protection which is a function referring to any form of guarantee or insurance that investment will not be lostbecause of “any fault” in Structures/Systems/Components (SSCs) having a potential for causing damage to the ITER investment (cost and machine availability), directly by their own action, the action of other SSCs, events related to the operation of the plant, or the plasma itself which has to be considered as a complex system.

Approval Process			
	Name	*Action*	*Job Title / Affiliation*
Author	**Nunes I.**	**05 Feb 2025:signed**	**Commissioning & Operations Resp. Of...**
Co-Authors	**Lopez-Villanueva R.**	**15 Apr 2025:signed**	**Investment Protection Engineer**
Reviewers	**Boilson D.** **Grosset K.** **Udintsev V.** **Wallander A.**	**18 Mar 2025:recommended** **19 May 2025:recommended** **25 Feb 2025:recommended** **06 Feb 2025:reviewed**	**Program Manager** **Requirements Management Engineer** **Program Manager** **Deputy Program Manager**
Approver	**Bartels H.- W.**	**19 May 2025:approved**	**Head of Division**
Information Protection Level: Non-Public - Unclassified *RO: Grillot David*			
Read Access	**LG: IPA-Interim view access, AD: ITER, AD: External Collaborators, AD: IO_Director-General, AD: External Management Advisory Board, AD: EUROfusion-DEMO, AD: OBS - Integrated Commissioning Project (INP), AD: IDM_Controller, AD: OBS - Commissioning and Temporary Operation (CTO), AD: Nuclear Safety Ins...**		

#drn#

Change Log			
ITER Investment Protection Handbook (3VUMVW)			
Version	***Latest Status***	***Issue Date***	***Description of Change***
v1.0	Signed	24 Nov 2010	
v2.0	Signed	24 Feb 2011	The frequency of the failure modes has been added for the classification of the risk levels.
v2.1	Signed	24 Feb 2011	Change of the list of reviewers
v3.0	In Work	10 Oct 2011	The document Policy for ITER Investment Protection has been updated taking into account the comments of David regarding the MQP procedure. The MQP Policy template has been used, the procedures have been suppressed while keeping the Policy and the content has been simplified and shortened.
v3.1	In Work	10 Oct 2011	The two sections were merged.
v3.2	Signed	10 Oct 2011	The table of Contents field has been updated.
v3.3	Signed	12 Jan 2012	This new version has been prepared In order to take into account the comments of two reviewers (A. Vergara_CIS and K.W. Kang_PBS43). Three modifications have been made in this updated version: The names of risk categories (chapter 5) have been aligned to those of the standard IEC-61508 used for the design of the interlock system, ITER Interlock Integrity Levels have been added for the interlock functions while indicating an equivalence with the "Safety Integrity Levels" (SIL) defined in the standard IEC-61508 and the corresponding I&C architecture described in the PCDH, The power supplies chapter has been revised and completed to cover all the needs of the IP chain components. These changes have been agreed by the reviewers who made the comments during the review of previous versions. Only 1 reviewer is required by IDM for this new version.
v4.0	Signed	16 Jan 2012	This version is the same as the previous one v3.3 but the changes made between version 3.2 and version 3.3 being not compliant with minor change definition, a major upgrade version was required. See the change description on the version 3.3 below: The names of risk categories (chapter 5) have been aligned to those of the standard IEC-61508 used for the design of the interlock system, ITER Interlock Integrity Levels have been added for the interlock functions while indicating an equivalence with the "Safety Integrity Levels" (SIL) defined in the standard IEC-61508 and the corresponding I&C architecture described in the PCDH, The power supplies chapter has been revised and completed to cover all the needs of the IP chain components.
v4.1	Approved	20 Mar 2012	Minor changes in the Definition section and table 2 explanation.
v5.0	Approved	05 Feb 2025	This document replaces the previous policy and describes the process for risk assessment process for the definition of the protection functions required for the operation of ITER and the MPP process to follow during operation to include new, modify or commission the protection functions. It also defines the responsibilities for the various steps of both processes.

Table of Contents

1. Purpose

The purpose of this handbook is to provide a comprehensive framework for ensuring the Investment Protection (IP) function of ITER plant systems, as required to minimize the risk of damage, operational downtime, and loss of investment caused by failures, faults, or hazardous scenarios. This document establishes the principles, processes, and criteria for systematically identifying, evaluating, mitigating, and managing risks that could affect ITER's structures, systems, or components (SSC).

The Investment Protection function is achieved through a combination of interlock systems, passive barriers, and operational or administrative procedures to ensure a multi-layered defence-in-depth strategy. Specifically:

1. Plant Interlock System (PIS): Acts at the local system level to protect individual plant systems against failures, control system errors, or external triggers.
2. Central Interlock System (CIS): Ensures coordinated protection actions across multiple plant systems and integrates higher-level interlocks.
3. Advanced Protection System (APS): Provides advanced predictive and reactive protection functions for complex hazardous scenarios.

This handbook aligns with IEC 61508 (Functional Safety of E/E/PE Systems) and IEC 61511 (Functional Safety in the Process Industry Sector), the latter, being particularly relevant for end-users and plant owners. The focus includes:

- Identification of protection functions, including active interlocks, passive safety barriers, and operator-driven administrative controls.
- Definition of the required 3IL for each protection function.
- Operation, maintenance, and change management processes to ensure the ongoing effectiveness of investment protection functions throughout their lifecycle.

This document serves as the foundational guide to:

- Define the risk assessment process for identifying hazardous scenarios.
- Establish risk acceptance criteria, categorization, and mitigation strategies.
- Allocate protection functions to interlock system layers (PIS, CIS, APS) or other passive/administrative measures to reduce risk to acceptable levels.
- Document roles, responsibilities, and processes for implementing and maintaining the Investment Protection strategy.
- Provide interfaces with complementary processes, including system design, operation, maintenance, and testing.

2. Scope

This handbook applies to the Investment Protection (IP) systems for ITER plant operations across all operational states and conditions. It focuses on ensuring the protection of plant systems from damage, loss of functionality, and downtime through coordinated mitigation strategies. The document addresses the identification and mitigation of hazardous scenarios, including internal events originating within a system, external incoming events from other systems, and external outgoing events impacting other systems.

The scope centres on the hierarchy of protection systems, specifically addressing the Investment Protection layer. At the local level, the Plant Interlock System (PIS) ensures the protection of individual plant systems, while the Central Interlock System (CIS) coordinates interlock actions across multiple systems. The Advanced Protection System (APS) complements these layers by providing predictive and reactive capabilities for complex scenarios. The handbook also recognizes

that some barriers may be achieved through passive safety mechanisms or operational and administrative procedures, complementing the active interlock functions.

This document defines the risk management process at critical stages, including hazard identification, risk evaluation, and the allocation of mitigation measures. It also clarifies the interfaces between Investment Protection functions and complementary systems, such as control systems, safety systems, and operational workflows.

Excluded from the scope are environmental protection, personal safety, fire safety, and protection against malevolent acts, which are managed through other ITER-specific systems and policies. Implementation-specific details, such as 3IL verification, testing, and proof testing for interlock systems, are covered in the ICS Management Plan.

Finally, the document establishes the foundational processes for reviewing and approving Investment Protection strategies, including the acceptance of residual risks through the Machine Protection Panel (MPP). It ensures alignment between system-specific investment protection plans and the overarching strategy for plant-wide risk mitigation.

3. Definitions & Acronyms

3.1 Definitions

Hazardous Event: An event that can cause harm

Hazardous Scenario: sequence of events and conditions leading to a Hazardous Situation.

Internal[1] Hazardous Situation (I-HS): Hazardous situations affecting one system, generated by failures or events within this system. No impact or loss of functionality on other systems or globally. An internal Hazardous Situation can be mitigated using interlock means on the scope of this system (Local Protection Functions), or using means provided by other systems (Central Protection Functions).

External[2] Incoming Hazardous Situation (EI-HS): Hazardous situation affecting this system, generated by failures or events of other systems (from external system to this system).

External[2] Outgoing Hazardous Situation (EO-HS): Hazardous situation impacting other systems generated by failures or events of this system (from this system to another system).

Local Protection: The internal investment protection is ensured by system design. This is an inherent protection, embedded in the component, subsystem or system itself.

Central Protection: Ensured by the Central Interlock System and the Advanced Protection System, in coordination with the local systems detection and/or actuation capabilities.

Plant Interlock System (PIS): Acts at individual plant system level, for example to protect the system against a failure, dysfunction of an input utility or control system error. The local protection is ensured by the Plant Interlock System. Actions of the Plant Interlock System are transmitted to the Central Interlock System.

Central Interlock System (CIS): The Central Interlock System ensures coordinated protection actions across several systems. These actions may be as a result of events coming from PIS, a scenario originated in the Advanced Protection System, or following failure of CODAC or the Plasma Control System. The CIS is responsible for the implementation of the Central Protection

[1] Internal to the system
[2] External to the system

Functions via the Plant Interlock Systems (PIS) (communicating through the Central Interlock Network (CIN) or directly hardwired links). It also centralizes the critical local interlock data of the different Plant Interlock Systems (threshold management, IP configuration parameters, protection function trigger status, etc.).

Advanced Protection System (APS): The APS complements the CIS in providing advanced functions with integrated algorithms concerning the evolution of some plasma and plant system conditions (e.g., calculation of coil forces) and in response to some plasma and plant system events. The APS identifies events that require mitigation, communicating the scenario to CIS for further coordination. The APS goal is to provide an intermediate level of investment protection. The APS is implemented with dedicated algorithms and strict change control procedures for each protection function to be sufficiently effective to maintain investment protection assurances during and between campaigns.

Interlock Control System: 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 Tokamak and its auxiliary systems. It is constituted by the Central Interlock System (CIS), the different Plant Interlock Systems (PIS) and its networks. The ICS does not include the sensors and actuators of the plant systems, but it is in charge of their control.

3.2 Acronyms

3IL	ITER Interlock Integrity Level related to risk mitigation inherent to an investment protection function
C-IPF	Central Investment Protection Function
CLOT	Cost of Loss of Operational Time
CoR	Cost of Repair
EI-HS	External (to system) Incoming Hazardous Situation
EO-HS	External Outgoing (from system) Hazardous Situation
EVL	Expected Value Loss
GOI	General Operating Instruction
HS	Hazardous Scenario
ICS	Interlock Control System
I-HS	Internal (to system) hazardous Situation
IP	Investment Protection
kIUA	kilo ITER Unit of Account
L-IPF	Local Investment Protection Function
MPP	Machine Protection Panel
RAC	Risk Acceptance Criteria
RRF	Risk Reduction Factor
SIL	Safety Integrity Level related to risk mitigation inherent to a safety function
TF-I	Transverse Function – Investment Protection
TFO	Transverse Function Officer

For a complete list of ITER abbreviations see: ITER_D_2MU6W5 - ITER Abbreviations

4. References

[1] Working Instruction for Operation Readiness Review (55E54L)
[2] Transverse Functions Management Process (ADJV67)
[3] ITER Guide to Perform Hazard and Operability (2F6B9M)
[4] IEC61882 Hazards and Operability Studies- Application Guide
[5] IEC60812 Analysis Techniques for System Reliability – Procedure for FMEA
[6] An STPA Primer - http://sunnyday.mit.edu/STPA-Primer-v0.pdf
[7] Center for Chemical Process Safety (CCPS). 2010 "Layer of Protection Analysis: Simplified Process Risk Assessment" DOI:10.1002/9780470935590
[8] Center for Chemical Process Safety (CCPS). 2014 "Guidelines for initiating events and independent protection layers in layer of protection analysis" DOI:10.1002/9781118948743
[9] Central Interlock System - DDD
[10] Management of Local Interlock Functions (75ZVTY)
[11] Plan Control Design Handbook (27LH2V)
[12] ITER RAMI analysis program(28WBXD)
[13] I&E Systems Pty Ltd. High demand and continuous mode safety functions compared with low demand mode. Available in https://www.iesystems.com.au/wp-content/uploads/2022/04/High-Demand-vs-Low-Demand.pdf)
[14] Jin, Hui & Mostia, Bill & Summers, Angela. (2016). High/Continuous Demand Hazardous Scenarios in LOPA. Available in https://sis-tech.com/wp-content/uploads/2016/07/02-Main-Article-Summer-Edition-2016.pdf
[15] IEC 61508 Functional safety of E/E/EP safety-related systems
[16] IEC 61511 Functional safety - Safety instrumented systems for the process industry sector
[17] Quality Classification Determination (24VQES)
[18] Review guidelines for Interlock Systems (PMUS5G)
[19] Template for MPP Record of Decisions (9PPW7N)
[20] Template for Investment Protection technical specification for Function (7SCZBZ)
[21] Template for Investment Protection technical specification for Event (7SCX4S)
[22] Template for Investment Protection technical specification for Action (7SCXPF)
[23] Template for the Investment Protection Plan (8NZC7P)
[24] ITER Operational States (54L85L)
[25] Concept of Operations L2 ()

5. Introduction

Risks are introduced by potential problem situations that have undesirable consequences in terms of cost, schedule, and technical performance. A hazardous scenario is the sequence of events leading from the initial cause to the undesirable consequence, i.e., a hazardous situation. The cause can be a single event, or an occurrence, which triggers a problem. The magnitude of a risk is measured in terms of its probability of occurrence and the severity of its consequences. Categories can be attributed to represent each probability and severity. The probability is then a measure of the likelihood of occurrence of the risk scenario, and the severity is a measure of the amount of damage or penalty to be expected. Information on the risks is often displayed in a risk diagram. In addition, a risk category is introduced to categorise risks and classify them as acceptable or unacceptable.

Risk reduction is achieved by lowering the magnitude of a risk, by lowering its probability and/or severity with the help of preventive and mitigation measures. Preventive measures aim to eliminate the cause of a problem situation, whilst mitigation measures aim to prevent the propagation of the cause to the consequence or reduce the severity.

The acceptance of risk mitigation is governed by the Machine Protection Panel (MPP) complemented by the Investment Protection Transverse Function (TF-I) driven by the TF-I officer (in this case, the MPP chair), which requires specifically that:

- The implementation of the TF requirements must be performed by the PBS teams
- Where layout requirements are defined by a TF, the PBS RO in collaboration with the Design Integration Section (IO/SID/CID/DIS) is in charge of implementing those requirements. The Transverse Function Officer (TFO), in close connection with DIS, defines the process of implementation or verification of those requirements.
- Specific checklist [6] is provided to check at the DIR [7] the proper implementation of those requirements
- The TFO is in charge of the verification of some TF requirements that must be implemented at ITER level, rather than being specific to particular equipment and subsystems

The risk management needs to be implemented throughout the entire project lifetime following the various steps as shown in Figure 1.

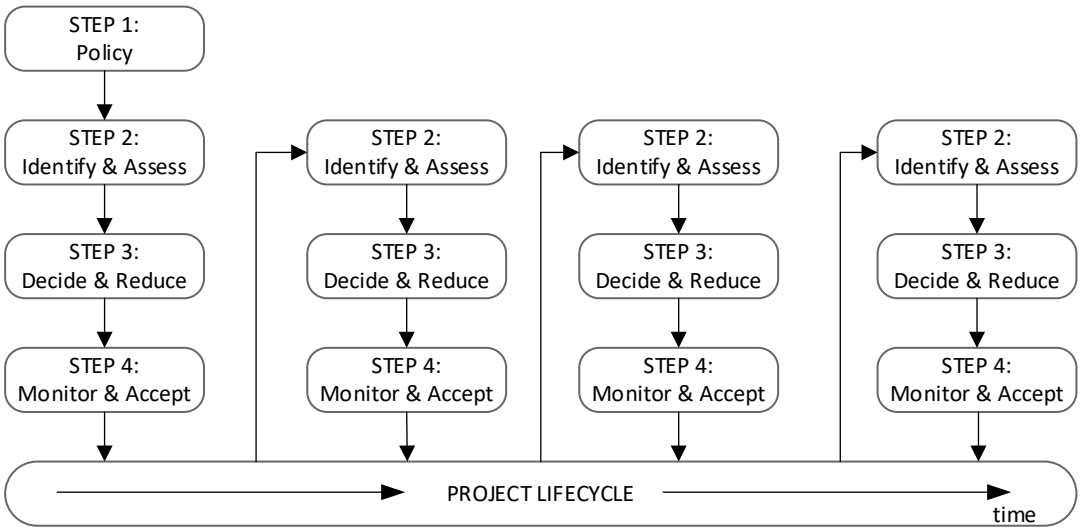

Figure 1: Risk Management Process cycle

The status of the development of the investment protection functions mapped to the ITER gate reviews [1] is shown in Table 1. Note that for the ORR gate, the validation and verification of the local functions should be as much as possible, and that this step for the C-IPF is performed during integrated commissioning.

Gate reviews	Expected status of the risk assessment
PDR	Draft analysis of the risk assessment
FDR	Final risk assessment, identification of the IPFs and appropriate 3IL identification
ORR	Validation and Verification and functional assessment of L-IPF before start of operations.

Table 1: Development of the IP strategy and the ITER gates

6. Investment Protection Framework

The Investment Protection Framework establishes the principles, structure, and methodologies necessary to ensure that ITER plant systems are safeguarded against hazardous scenarios that could result in damage, downtime, or financial loss. This framework aligns with internationally recognized

standards, including IEC 61508 and IEC 61511, to provide a systematic approach for identifying risks, evaluating their severity, and implementing mitigation measures.

The framework focuses on achieving defence-in-depth by integrating multiple layers of protection, including active interlock systems, passive barriers, and operational procedures. The goal is to reduce risks to an acceptable level while maintaining system reliability and operational continuity.

The following sections describe the objectives of the Investment Protection strategy and the hierarchy of protection systems that implement these objectives across local and central levels of the plant systems.

6.1 Objectives of Investment Protection

The primary objective of Investment Protection (IP) is to prevent or minimize damage to ITER plant systems, components, and equipment while ensuring the continuity of operations and safeguarding significant financial investments. The IP function addresses risks arising from failures, faults, or hazardous scenarios that may lead to repair costs, loss of operational time, or propagation of failures to interconnected systems. When a proposed Independent Protection Layer is an I&C Investment Protection Function (IPF), its dependability level shall be defined by the "ITER Interlock Integrity Level" (3IL).

The Investment Protection strategy establishes a framework to:

1. Identify and mitigate hazardous scenarios that could compromise the integrity or availability of plant systems. These scenarios include internal system failures, external events originating from other systems, and hazardous conditions impacting multiple systems during integrated operations.
2. Provide defense-in-depth protection by implementing active interlock systems, passive safety barriers, and operational or administrative measures. This layered approach ensures that hazards are mitigated locally, when possible, while central coordination addresses broader or more complex events.
3. Minimize downtime and operational losses by defining mitigation actions that restore systems to safe or operational states. The impact of failures is measured through Expected Value Loss (EVL), which combines repair costs and loss of operational time (CLOT).
4. Ensure systematic risk management through a structured process of hazard identification, risk analysis, and acceptance based on severity, probability, and required Risk Reduction Factors (RRF). This approach ensures risks are reduced to an acceptable level, following the ALARP (As Low As Reasonably Practicable) principle.
5. Achieve and maintain integrity levels appropriate for each protection function. The required Interlock Integrity Level (3IL), mapped to Safety Integrity Levels (SIL) in IEC 61508/61511, ensures the reliability and performance of interlock systems throughout their lifecycle, including design, implementation, validation, and maintenance.
6. Coordinate interlock actions across systems to prevent propagation of faults or failures. Investment Protection functions are allocated to Plant Interlock Systems (PIS) at the local level and coordinated through the Central Interlock System (CIS) for plant-wide events.
7. Integrate passive barriers and operational procedures alongside active protection systems. In certain cases, risk mitigation may rely on system redundancy, inherent design safety features, or operator-driven measures.

By achieving these objectives, Investment Protection ensures that ITER systems operate reliably, failures are managed effectively, and risks to the investment are systematically reduced and controlled.

6.2 Hierarchy of Protection Systems

The Investment Protection strategy is part of the broader hierarchy of protection systems implemented at ITER. This hierarchy defines the priorities and layers of protection to address different categories of risks, ranging from safety-critical events to operational disruptions.

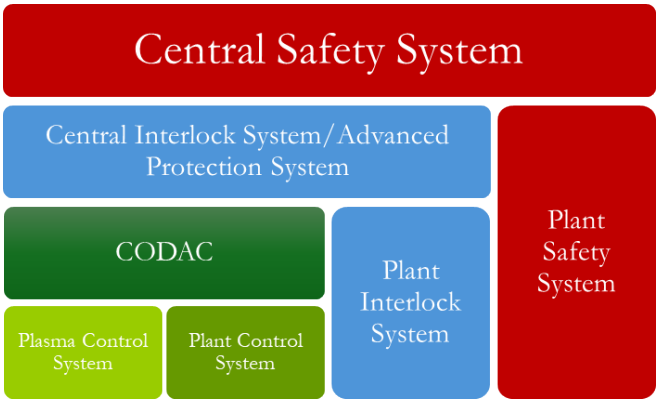

Figure 2: Hierarchy of Protection and Control Systems

The three main protection levels are Safety Protection, Investment Protection, and Conventional Control Systems (see Figure 2). Each level has a distinct scope, role, and implementation approach.

1. Safety Protection: The highest priority in the protection hierarchy, Safety Protection is implemented to prevent risks to personnel, public safety, and the environment. This is achieved through the Central Safety System (CSS; -O for Occupational and -N for Nuclear) and Plant Safety Systems (PSS), which ensure compliance with safety regulations and standards. Safety functions operate independently from Investment Protection systems and are designed to achieve Safety Integrity Levels (SIL) required for life protection and environmental safety.
2. Investment Protection: Investment Protection is the second layer of the hierarchy and focuses on preventing damage to equipment and minimizing loss of operational time. It is implemented through the Interlock Control System (ICS), which includes three coordinated subsystems:
    - Plant Interlock System (PIS): Operating at the local system level, the PIS ensures protection against internal failures, input utility dysfunctions, or control system errors. Local protection functions are embedded in individual plant systems to detect and mitigate hazards as close as possible to the source.
    - Central Interlock System (CIS): The CIS ensures coordinated protection actions across multiple systems. It processes events from the PIS, the APS, or other sources and implements central mitigation functions. This coordination prevents fault propagation and ensures plant-level protection.
    - Advanced Protection System (APS): The APS complements the CIS by providing advanced predictive and reactive capabilities. Using algorithms and monitoring functions, the APS identifies evolving hazardous scenarios that may require central mitigation actions via CIS.

Together, these three layers – PIS, CIS, and APS – form a defence-in-depth approach to investment protection, ensuring both local and centralized mitigation of hazardous situations.

3. Conventional Control Systems: The third layer consists of the CODAC (Control, Data Access, and Communication) System, Plasma Control System, and Plant Control Systems. These systems manage operational processes and provide real-time monitoring and control

of ITER systems. While they play a role in system stability, their primary purpose is avoidance rather than protective.

The hierarchy of protection systems ensures a structured and layered approach to managing risks, with Safety Protection addressing life-critical hazards, Investment Protection preventing damage and downtime, and Control Systems supporting operational performance. Investment Protection plays a central role in minimizing financial losses while ensuring reliable and safe plant operations.

6.3 Hazardous Scenarios

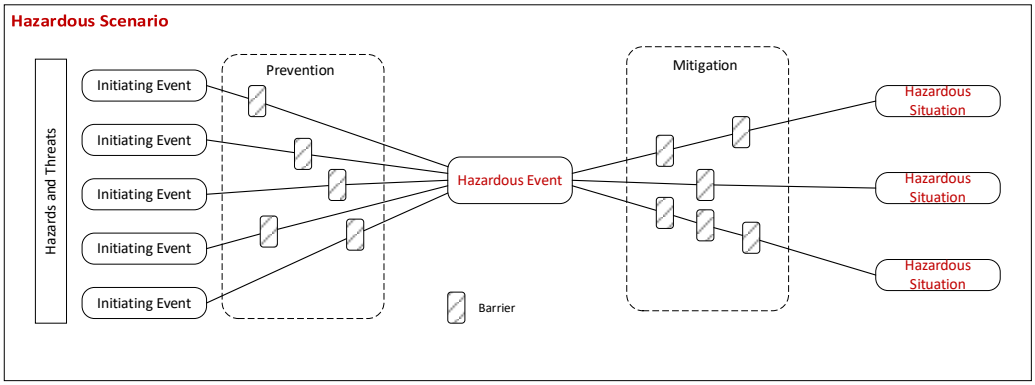

Figure 3: Relationship between hazardous scenario, hazardous event and hazardous situation

Hazardous scenarios (see Figure 3), refer to specific conditions or events that, if not mitigated, can lead to hazardous situations, i.e., damage of systems, downtime, or cascading failures that propagate across plant systems. To systematically address and manage these risks, hazardous situations are categorized into three main types:

Internal Hazardous Situations (I-HS) occur within a single system and are generated by failures or events that originate internally. These events do not directly impact other systems, although the affected system may lose its functionality. Internal hazards are typically mitigated at the local level using the Plant Interlock System (PIS).

External Incoming Hazardous Situations (EI-HS) occur when failures or hazardous events in other systems propagate into the system under consideration. These hazards require coordinated protection measures that may involve both local protection (PIS) and central mitigation through the Central Interlock System (CIS).

Finally, **External Outgoing Hazardous Situations (EO-HS)** arise from failures or events within the system under consideration but propagate to other systems, leading to broader risks or operational interruptions. These hazards are mitigated through both local protection (to stop fault escalation) and centralized actions to contain the impact.

Categorizing hazardous situations into I-HS, EI-HS, and EO-HS allows for a structured approach to risk assessment and mitigation:

- I-HS focuses on local failures managed by Plant Interlock Systems (PIS).
- EI-HS emphasizes incoming risks and the need for central coordination through CIS.
- EO-HS highlights the importance of containment strategies to prevent fault propagation to dependent systems.

This categorisation ensures that appropriate mitigation measures – whether local interlocks, central coordination, passive barriers, or operator interventions – are applied at the right level to maintain system integrity and operational continuity.

6.4 Defence-in-depth

A defence-in-depth strategy is a layered approach to risk management that ensures redundant and complementary protection measures are in place to mitigate failures or hazardous events. Rather

than relying on a single layer of protection, this strategy combines multiple barriers—each serving as a checkpoint to prevent risks from escalating and propagating.

The strategy operates at three primary levels:

- Inherent Safety by Design: Implementing systems with built-in safety features to reduce the likelihood of hazardous events (e.g., passive barriers, redundancy in system components).
- Active Protection Systems: Automated interlock systems such as the Plant Interlock System (PIS) and Central Interlock System (CIS), which detect and respond to hazardous conditions in real time.
- Operational and Administrative Controls: Procedures and manual actions undertaken by operators to monitor, intervene, and manage residual risks when automated measures are insufficient.

Each layer works independently but is also interconnected to ensure there is no single point of failure. For example, if a local interlock (PIS) fails to contain an event, the Central Interlock System (CIS) provides a coordinated response to manage the situation. Additionally, advanced systems, like the Advanced Protection System (APS), predict and address evolving scenarios that require higher-level intervention.

7. Risk Assessment Process

The risk management begins at the start of a project and the various steps in the process must be iterated throughout the project life cycle as shown in Figure 1.

The risk assessment process is a structured methodology to systematically identify, analyse, and mitigate risks associated with hazardous situations, ensuring compliance with safety standards such as IEC 61508 and IEC 61511. Scarce Resources are also to be included in the risk assessment. The consumption of scarce resources as a result of a hazardous situation can contribute for the determination of the severity category.

This process integrates multiple steps to evaluate potential risks at various system levels and define appropriate integrity levels (3IL) for mitigation. The workflow consists of five key phases:

- **Risk Identification:** Using proven techniques such as HAZOP (Hazard and Operability Study) [3] [4], FMECA (Failure Mode, Effects, and Criticality Analysis) [5], SPHA (System Preliminary Hazard Analysis) [6], and LOPA (Layers of Protection Analysis) [7][8] to systematically identify hazards within the system (see [9][10] for a summary explanation of the methods referred here).
- **Risk Consequence:** Once hazards are identified, their consequences are evaluated using metrics like the Severity Category to quantify their impact based on the expected value loss (EVL).
- **Risk Probability:** The likelihood of each hazardous event occurring is determined, considering failure rates, operational data, and system behaviours.
- **Risk Acceptance Criteria:** Risks are then evaluated against predefined acceptance thresholds to determine whether further mitigation is required.
- **Minimum 3IL Identification:** Finally, based on the risk severity and probability, the minimum ITER Integrity Level (3IL) is established to ensure risks are reduced to an acceptable level through appropriate safety functions.

This step-by-step approach ensures that risks are addressed comprehensively, starting from identification to the assignment of specific mitigation measures. Details are provided in subsequent sections. The RACI matrix for this process is defined in Table 12.

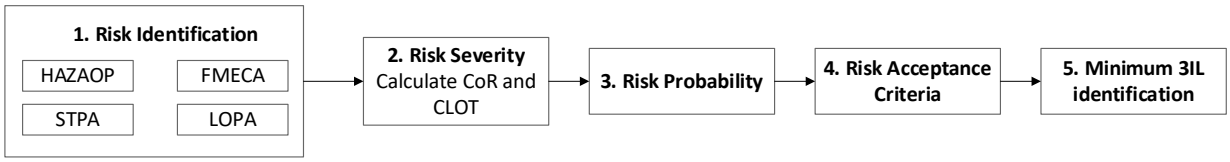

Figure 4: Workflow for risk assessment

7.1 Risk Identification

Risk identification is the first step in the risk assessment process, aimed at systematically identifying potential hazards, failure scenarios, and weak points in the system. It forms the basis for all subsequent analysis and mitigation measures, ensuring alignment with IEC 61508 and IEC 61511 standards. To achieve comprehensive and structured identification, the following methodologies are applied (following the process is detailed further in the Management of Local Interlock Functions [9]):

- **Hazard and Operability Study (HAZOP):** A systematic approach to identifying deviations from design intent and their consequences, based on structured guidewords (e.g., more, less, reverse).
- **Failure Modes, Effects, and Criticality Analysis (FMECA):** Identifies component-level failure modes, assesses their effects, and prioritizes risks based on severity and likelihood.
- **System-Theoretic Process Analysis (STPA):** A method that identifies hazards by analysing control system interactions and unsafe system behaviours rather than individual component failures, suitable for complex systems.
- **Layers of Protection Analysis (LOPA):** A semi-quantitative technique that evaluates the adequacy of independent protection layers (IPLs) to mitigate specific hazards and determine risk reduction requirements.

As an output, the Risk Identification Process should produce at least:

- Hazard Register: A detailed list of hazardous situations, categorized as Internal (I-HS), External Incoming (EI-HS), and External Outgoing (EO-HS).
- Failure Scenarios: Documented pathways of hazard initiation and escalation.
- Identification of Critical Areas: Weak points requiring further analysis or mitigation.

Hazardous situations can arise from either damage to the system itself or interactions with other systems/components during both individual and integrated operation. At this stage, the analysis must account for hazardous situations that may result from the mitigating actions of local protection functions, as well as plant-level information, such as design requirements, design documentation, and operational modes. The input data for this analysis includes key references such as RAMI/FMEA analyses, System Requirement Documents (SRD), Design Description Documents (DDD), and interface sheets (see [9]). The output of this functional analysis is a set of identified hazardous scenarios that require mitigation through central interlock functions to prevent or address hazardous conditions effectively.

7.2 Risk Severity

Risk Severity quantifies the cost of an occurrence of a failure by calculating the Expected Value Loss (EVL), which is a function of Cost of Repair (CoR) and Cost of Loss of Operational Time (CLOT). This is expressed as:

$$\text{EVL} = \text{Cost of Repair (CoR)} + \text{Cost of Loss of Operational Time (CLOT)}$$

Where Cost of Repair (CoR) is the cost to repair any damaged component, including induced damage to other components. This cost is divided into categories (see Table 2), based in kIUA[3] which allows to maintain the criteria updated throughout the ITER lifecycle.

Cost of Loss of Operational Time (CLOT) categories (see Table 3) is based on the RAMI analysis on machine unavailability, except for row 7 ("greater than 2 years") which has been added to cover catastrophic failures. This machine down time is translated into kIUA using the ITER yearly operational cost. As per ITER Cost Baseline for Operation of 2024 the yearly operational cost is 188kIUA/yr.

CoR	CoR (M€ in 2024)	CoR (kIUA)
1	CoR <0,12	CoR <0.06
2	0,12 ≤ CoR <1.3	0.06 ≤ CoR <0.64
3	1.3 ≤ CoR <13	0.64 ≤ CoR < 6.44
4	13 ≤ CoR <67	6.44 ≤ CoR < 32.2
5	67 ≤ CoR <671	32.2 ≤ CoR < 322
6	CoR >671	CoR > 322

Table 2: Categories defined for Cost of Repair

CLOT	Down time	Maximum Cost [kIUA]	CLOT [kIUA]
1	< 1 hour	0.02	0 < CLOT < 0.02
2	1 hour ≤ dt < 1 day	0.52	0.02 ≤ CLOT < 0.52
3	1 day ≤ dt < 1 week	3.61	0.52 ≤ CLOT < 3.61
4	1 week ≤ dt < 2 months	29	3.61 ≤ CLOT < 29
5	2 months ≤ dt < 1 year	188	29 ≤ CLOT < 188
6	1 year ≤ dt < 2 years	376	188 ≤ CLOT < 376
7	≥ 2 years		CLOT ≥ 376

Table 3: Categories defined for Cost of Loss of Operational Time

The Risk Severity is then based on the EVL as shown in Table 4 and Table 5.

Severity	Category	EVL [kIUA]
1	Minor	EVL < 0.31
2	Severe (-)	0.31 ≤ EVL < 0.64
3	Severe (+)	0.64 ≤ EVL < 6.4
4	Major (-)	6.4 ≤ EVL < 32.2
5	Major (+)	32.2 ≤ EVL < 322
6	Catastrophic	EVL ≥ 322

Table 4: Risk Severity category based on the EVL

	CLOT	1	2	3	4	5	6	7
	Down Time	<1h	<1d	<1w	<2m	<1y	<2y	≥2y
CoR	**[kIUA]/[kIUA]**	**<0.02**	**<0.52**	**<3.61**	**<29**	**<188**	**<376**	**≥ 376**

[3] In 2010 the conversion was 1 IUA = 1,552.24€, while 2024 conversion is 1 IUA = 2,086.03€.

1	**< 0.06**	0.04	0.30	2.1	16	108	282	376
2	**< 0.64**	0.37	0.62	2.4	17	109	282	376
3	**< 6.44**	3.6	3.8	5.6	20	112	286	380
4	**< 32.2**	19	20	21	36	128	301	395
5	**< 322.1**	177	177	179	193	286	459	553
6	**≥ 322.1**	322	322	324	338	431	604	698

Table 5: Risk severity categories based on EVL (kIUA). The EVL cell values are the average of four interval boundaries.

7.3 Risk Probability

The following categories, to maintain coherence with the ITER RAMI Analysis Programme [9], shall be used for quantifying the risk probability (i.e., probability of a Hazardous Situation occurring).

	Probability of risk occurring	**Frequency (per year)**	**Expected occurrence in 20 years**	**Probability of at least 1 occurrence in 20 years [%]**	**Probability of 0 occurrences in 20 years [%]**
1	Frequent	>5	>100	100	0
2	Probable	$5.10^{-1} \leq f < 5$	55	100	0
3	Occasional	$5.10^{-2} \leq f < 5.10^{-1}$	5.5	99.59	0.41
4	Remote	$5.10^{-3} \leq f < 5.10^{-2}$	0.55	42.3	57.69
5	Improbable	$5.10^{-4} \leq f < 5.10^{-3}$	0.055	5.35	94.65
6	Negligible	$f \leq 5.10^{-4}$	<0.01	0.99	99

Table 6: Risk probability categories

7.4 Risk Acceptance Criteria

Once the identified risks have been evaluated in terms of severity and probability, they should be compared against the ITER IP Risk Acceptance Criteria[4], as presented in the following table.

According to the Risk Acceptance Criteria, a risk can belong to one of the following 3 categories (as listed in Table 8) depending on its required Risk Reduction Factor. The higher the required RRF, the higher the risk criticality value. For a given cell (Table 7), the required Risk Reduction Factor (RRF) is defined as the vertical gap [5](i.e. probability axis) to the Acceptable risk region (green).

		Severity	**1**		**2**		**3**		**4**		**5**		**6**
			Minor		**Severe-**		**Severe+**		**Major-**		**Major+**		**Catastrophic**
Probability		**Freq[yr^{-1}]/EVL[kIUA]**	0.0	0.31	0.31	0.64	0.64	6.4	6.4	33.2	33.2	322	>322
1	**Frequent**	>5											
2	**Probable**	$5.10^{-1}<f< 5$											
3	**Occasional**	$5.10^{-2}<f< 5.10^{-1}$											
4	**Remote**	$5.10^{-3}<f< 5.10^{-2}$											
5	**Improbable**	$5.10^{-4}<f< 5.10^{-3}$											
6	**Negligible**	$f<5.10^{-4}$											

Table 7: ITER IP Risk Acceptability Matrix

[4] Note: The criteria is applicable to each individual risk. The overall global risk to which the ITER plant will be exposed will be defined by the number of risks in each cell and their statistical interdependencies.

[5] Due to the logarithm scale used for the probability axis on the ITER RAC matrix, a vertical gap of 1 cell implies a RRF=10, 2 cells a RRF=100, 3 cells a RRF=1000 and 4 cells a RRF of 10000.

categories	Definition	Required RRF
Acceptable	Acceptable risk without extra mitigation measures	<1
ALARP	Tolerable risk when appropriate mitigation measure is implemented (As Low As Reasonably Possible; further mitigation measures are unfeasible or exceeding cost of equipment to protect)	$\leq 10^4$
Unacceptable	Non-acceptable region, even after implementation of a mitigation; further risk reduction measures in these regions are mandatory.	$>10^4$

Table 8: Risk categories

As per IEC61511-1 9.2.2, even if multiple safeguards are present, only the Independent Protection Layers (IPL) can be credited for RRF implementation. After considering the RRF provided by the other present IPLs, the remaining RRF to be allocated to the proposed IPF (RRF_IPF) can be computed.

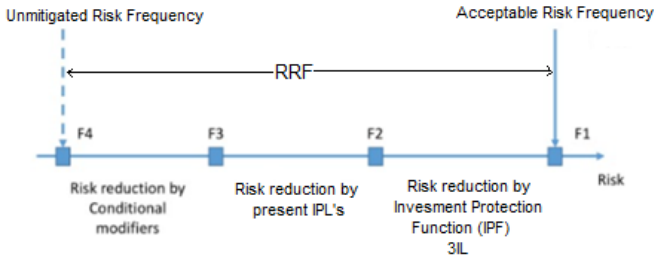

Figure 5: Required Risk Reduction Factor

In case it will not be technically or economically viable to implement a barrier with the required RRF, the residual risk after reasonable mitigation shall be reviewed by MPP and accepted by the appropriate management level. The residual risk shall be documented in the Investment Protection Risk Register.

7.5 Monitoring and Acceptance of Risks

It is necessary to control all acceptable, resolved and unresolved risks and risk reduction actions by systematic monitoring and tracking. This involves periodic re-assessment and review of the risks and the updating of the assessment results after iteration of the previous risk assessment steps. New risks or changes to existing risks are identified, as well as areas where a more detailed risk analysis must be performed, or better data is required to reduce uncertainties. It is verified whether the risk reduction and control activities have the intended effects. The risk trend over the project's evolution is illustrated by identifying how the risk magnitudes have changed over the project's lifetime. Finally, the residual risks are again subjected to a new risk acceptance.

8. Mitigation of Hazardous Scenarios

This chapter outlines the strategies, criteria, and processes for mitigating hazardous scenarios identified during the risk assessment phase. It establishes a systematic approach for assigning protection functions, defining system behaviour under fault conditions, and addressing residual risks to ensure comprehensive hazard management.

The mitigation measures for investment losses resulting from the unavailability of the failed component itself is handled within the RAMI program [9]. For this type of risk (i.e. "Stop operation due to loss of a required function"), the "safe state" is "the system continues to perform the required function". This type of "safe state" can be achieved by design modification (i.e. adding redundancy to the original system), not in the implementation of an IPF.

8.1 Concept of Investment Protection Functions

Investment Protection Functions refer to any form of prevention/reduction or attempt to guarantee that a loss of investment will not occur due to any fault or failure in Structures, Systems or Components. Such failure may be local to the system, or through the action of other Systems or due to events related to the operation of the plant or the plasma.

Based on the risk evaluation, mitigating actions can be implemented through design changes, investment protection functions (IPFs) and/or written procedures to minimise the risk. The required mitigating actions are determined based on the risk and on the actuators available to mitigate the risk. For each identified risk, the detection of the event and a mitigating action or set of actions must be identified. If an acceptable residual risk is not achieved, then the risk shall be registered in the Investment Protection Risk Register (and/or ITER Risk and Opportunities Register).

The investment protection philosophy relies on a series of IPFs based on the concept that an event, or combination of events, triggers an action or a combination/sequence of actions. This concept is transversal to all systems. The C-IPF receives the interlock event and calls for the mitigating actions following a pre-defined logic. From an implementation perspective, the events and actions are managed by the plant systems through the dedicated Plant Interlock System. The PIS is a control system linked to a particular plant system that manages, in addition to the local protection functions, the interfaces with the Central Interlock System by sending events and receiving actions.

8.2 Minimum 3IL level criteria

In line with IEC61508/IEC61511 methodology, the minimum 3IL required to mitigate the identified risk to an acceptable level is presented in the following matrix.

		Severity	1		2		3		4		5		6
			Minor		Severe-		Severe+		Major-		Major+		Catastrophic
Probability		Freq/ EVL [kIUA]	0.0	0.31	0.31	0.64	0.64	6.4	6.4	33.2	33.2	322	>322
1	Frequent	>5	3IL2 (*)		3IL3 (*)		3IL4						
2	Probable	5.10^{-1}<f< 5	3IL1 (*)		3IL2 (*)		3IL3		3IL4				
3	Occasional	5.10^{-2}<f< 5.10^{-1}			3IL1 (*)		3IL2		3IL3		3IL4		3IL4
4	Remote	5.10^{-3}<f< 5.10^{-2}					3IL1		3IL2		3IL3		3IL3
5	Improbable	5.10^{-4} <f< 5.10^{-3}							3IL1		3IL2		3IL2
6	Negligable	f<5.10^{-4}									3IL1		3IL1

Table 9: Minimum required 3IL matrix

For the cells marked with (*), the implementation of an Investment Protection Function shall be required only to prevent investment losses resulting from damage caused by the propagation of a component failure on other components.

The minimum 3IL, is calculated based on the required Risk Reduction Factor (RRF) i.e., min 3IL = log RRF_IPF. For the IPF operating in Low Demand, the RRF is equal to 1/PFD. However, for IPFs operating in High Demand or Continuous mode, extra care is need it to properly evaluate the Unmitigated Risk Frequencies (see [13][14]) (see Table 10 for equivalence to SIL).

The red areas require an RRF>10^4. As per IEC61508/61511 it is considered not possible, with current technology, to provide a risk barrier with an RRF>10^4. Therefore,

i. 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.
ii. Investment protection functions with a 3IL higher than 3 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.

The equivalence between the 3IL and the SIL as per IEC 61508 [15] and the ITER I&C implementation for such requirement, as specified in [17] is given in Table 11.

SIL	Low-Demand Mode of Operation PFD_{avg}	High-Demand Mode of Operation $PFH\ (h^{-1})$
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Table 10**:** Equivalence **between** SIL **and** PFD and PFH intervals

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-1 – QC-2	SIL-3	High Integrity Interlock
3IL-2	QC-2	SIL-2	Low Integrity Interlock
3IL-1[6]	QC-3	SIL-1	Interlock performed by Conventional Control

Table 11: Minimum 3IL required and equivalence with QC and SIL

9. Acceptance Process

To satisfy the requirements of this handbook, acceptance of the investment protection strategy for a particular system/sub-system, is called for in two places, where this acceptance is to be given by the MPP. Acceptance is to be a positive and recorded action (see deliverables).

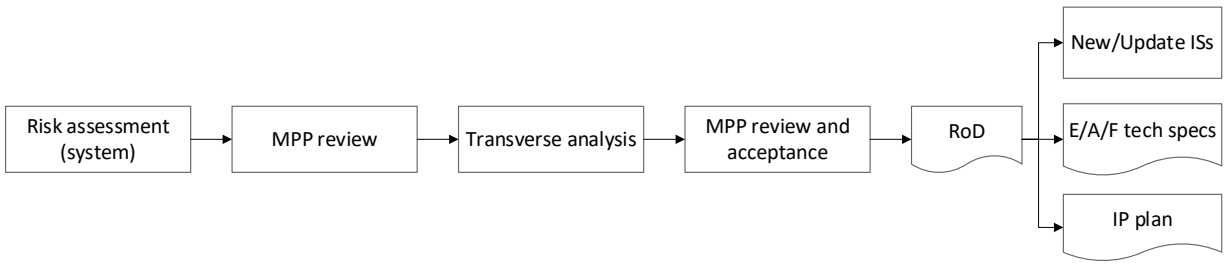

Figure 6: Workflow for review and acceptance of investment protection strategy

[6] in ITER, in line with IEC61511, it is considered acceptable to implement a 3IL-1 function by using the conventional control tier (i.e. CODAC). However, any 3IL-1 function shall be still implemented as a dedicated Protection Function (independent from the conventional function controlling the process). This conventional control function is still to be considered as Investment Protection Function and subject to the rest of applicable procedures. Detailed requirements for are provided in IEC61511-1 9.3 with extra available in IEC61511-2 A9.3 in addition to those in the PCDH [11].

A first analysis carried out by the projects identifying the following hazardous situations shall be presented and reviewed at an MPP meeting. This analysis shall include defence-in-depth actions, i.e., the potential hazardous situations generated by conventional control as mitigation tool.

The following step is for MPP to perform a transverse analysis to verify the integration within the plant systems own protection and interaction with the other protection systems. In addition, the request for simultaneous protection functions will be verified to ensure that there are no conflicts/redundancy of the mitigating actions. The overall analysis shall be discussed at a second MPP meeting. Acceptance of the protection strategy for a system or sub/system is formalised in the RoD issued by MPP [19]. This document is a formal document and officially informs all stakeholders on what has been agreed and mandates the projects and the CIS to implement the agreed strategy for risk mitigation.

10. Design, Implementation and Verification and Validation

The C-IPFs are executed within the domain of CIS, and the implementation process is the responsibility of PBS46. The L-IPFs are executed within the domain of the systems and the implementation, verification and validation process is under the responsibility of the systems. The design and implementation of a IPF shall follow the guidelines defined in [9] and satellite documentation. Depending on the C-IPF scope, one or more PIS and one or more APS/CIS modules can be impacted. As per IEC61508/61511 the IPF (both software and hardware), design and implementation shall be verified. Once the detailed design finalised, the 3IL verification report shall be issued, and the required functional safety review performed. A CIS Test Platform has been developed to allow the process of verification of the C-IPF, emulating PIS events and analysing the corresponding generated actions to verify the C-IPF implemented logic against its functional specification.

As a pre-requisite to the IPF validation, the ICS systems implementing the IPF, i.e. PIS and CIS, shall be validated against its specific requirements as part of their System Commissioning Test.

The CIS/PIS validation testing should be decoupled from the IPF functional testing as much as possible. However, for certain specific CIS or PIS requirements (e.g. performance), a IPF functional validation test might be utilized as means to validate a specific CIS/PIS requirement.

The ICS validation plan, and the detailed IPF functional testing procedures (each IPF has its own individual procedure) shall be reviewed and approved prior to the IPF Test Readiness Review.

Each IPF shall be validated against its own specification. Each IPF has a validation plan, defining the validation scope, validation strategy, validation platform, required interfaces, pre-requisites, and a requirements traceability matrix shall be provided.

The IPF non-functional requirements can be validated by analysis, engineering documentation or inspection, and functional requirements shall be validated by functional testing.

The objective of functional testing is to demonstrate ICS operates correctly, performing its intended function in compliance with the IPF functional requirements. Functional testing of the IPF should adhere to the end-to-end principle, which encompasses the entire chain, from sensor to actuator. This principle dictates that functional tests must be conducted across the full functional chain, initiating the process event to be detected and verifying the proper execution of the required action in the field.

The end-to-end principle offers a more reliable proof as it more accurately reflects real-world conditions. Furthermore, since it does not require reconfiguring the ICS for testing, it eliminates potential reconfiguration errors and the need to revalidate de-configured interfaces.

If end-to-end testing is deemed not feasible, a segmented testing strategy (e.g., first sensor-to-logic and later logic-to-actuator) should be established. The ICS design must be compatible with the segmented testing strategy, with clearly defined testing interfaces and simulator needs if required.

Special attention should be given to defining the overlapping conditions of the functional interfaces between the scopes of two segmented tests.

11. Commissioning and Operation

The IEC 61508/61511 standards outline the need to establish proof test procedures, frequency, and documentation to ensure that protection systems are adequately maintained and that their functionality is maintained throughout their lifecycle (3IL preservation). The goal of proof testing differs from that of functional testing. Proof testing reveals hidden failures present on the components participating on the ICS whilst functional testing ensures that the functions behave as expected.

- Proof test shall be executed following equipment manufacturer documentation. Proof testing procedures may not be available for all equipment, as some manufacturers, such as those of PLCs, consider it is not possible to define a test that reveals more hidden failures than those already detected by the equipment's online self-diagnostic testing.
- A proof test should be considered perfect (100% test coverage, meaning all the hidden failures will be revealed) only in case the manufacturer documentation supports this claim. Preventive Maintenance and Inspection activities can be used as proof test, with a test coverage due justified.
- Proof tests are executed periodically, and the testing frequency shall be calculated to ensure that the required 3IL is maintained throughout the function lifecycle.
- In case the Proof Test requires a de-configuration of the protection components, a functional validation test should be performed before putting the ICS function back in service.
- Records shall be maintained that certify that proof tests and inspections were completed as required
- Functional Assessment shall be carried out periodically during the operations and maintenance phase to ensure and operation are being carried out according to the assumptions made during design [15][16].
- Any change to the application program requires full validation and a proof test of any IPF impacted by the change. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were designed per the updated IP requirements and correctly implemented [15][16].

12. Documentation

The following documents are produced in the context of MPP, either by the team itself, or supporting external teams. They are required as part of the process described in section 13 in addition to the documentation required described in [10].

12.1 MPP Record of Decisions

The RoD summarises the hazardous scenarios, LOPA diagrams and the strategy agreed and accepted by the stakeholders to mitigate these scenarios. It also describes the logic of protection functions by linking the detection of an event with the actuators required to mitigate the impact of such event (actions) . For each function (and respective events and actions), information on time propagation, the need for slow or fast architecture, 3IL level, etc. is also included.

12.2 Technical Specifications for E/A/F (C-IPFs)

The initiating events, the required actions and the interlock function technical specifications are written using the templates [20][21][22].

The Events (E), Actions (A) and Functions (F) technical specifications shall provide the technical details required for the design and consequent implementation of the central and local interlock controllers. It provides sufficient information to allow the creation/update of the interface sheets between the systems and the interlock system. This activity will support and feed the last stage of detailed design activities, which consists of the definition of the required signals, variables and the verification and validation techniques to be performed during the testing and commissioning of each interlock function individually and integrated into the ITER machine operation.

The IEC61508 and IEC61511 standards are used for the lifecycle of the ITER investment protection. Accordingly, the IPF specification shall follow the philosophy and terminology used in these standards as much as possible.

12.3 Investment Protection Plan

The Investment Protection plan [23] provides an integrated view of the investment protection for a specific system. Gathers all the information relevant to investment protection for each Plant System, describes the analysis performed to identify the external and internal hazardous conditions, the enabling events, their severity according and the measures put in place to mitigate the hazardous conditions. Identifies the conditions of the facility for which the function is required or for which the function is disabled (if it is the case) for the ITER Global Operating States (GOS as per [24]) and includes:

- A list of all the local protection functions within the scope of the Plant System
- The external hazardous situations i.e., originated from other Plant Systems
- The *hazardous situations* generated by the Plant System
- The mitigating *actions* available to that Plant System (whether these correspond to local or external *events*)
- The configuration parameters (i.e. thresholds) available and/or required to be managed centrally
- Time performance requirements for the mitigation actions

This document serves as:

- Reference document for machine operation
- Reference document for the establishment of interfaces between systems regarding investment protection
- Reference document for the periodical review of the system's investment protection
- Part of the Interlock Control System documentation
- Supporting document for the management of operation instructions (exceptional masking of events, forcing of actions, etc …)

13. Machine Protection Process to follow during Operations

Once the initial risk assessment was performed and the protection functions implemented, operations can start. However, during operations there might be necessary to change the protection functions if the plant is either modified or new operational scenarios need to be developed, or due to the modification of the plant or inadequacy of an existing protection.

As well as new requests for protection functions or modifications to existing protection functions, either automatic or procedural, also the update or maintenance of the protection functions can be required.

ITER has five Global Operating States [24], with the Safe state only available in case of incident or accident. For machine protection during operations, only four states are considered (POS, STM, TCS and LTM). Figure 7 shows the possible transition between these GOS states considering the status of the protection functions.

The investment protection functions are ruled by the Global Operating Instructions (GOIs). These, in conjunction with the control systems ensure the compliance of operation within the defined boundaries and the operation of the facility [25]. For the case of the protection functions these boundaries are defined by the limits imposed for the detection of an event, what to do in case a limit is reached and what are the allowed deviations to these limits, for example, during commissioning. Each GOI related to the investment protection functions addresses the description of the constraints applicable to operation, the operational parameter(s) used for monitoring and threshold values for which an action must be taken (these thresholds normally remain fixed during routine operation; however, some will be updated during commissioning and maintenance). What to do in case a boundary is reached i.e., prescribed actions to be taken by the operating staff in the event of deviations from the established boundaries and the time allowed to complete these actions; rules to allow each boundary to be overridden (where change is allowed) always ensuring that the Safety Driven Domain boundaries remain unchallenged and rules to allow modifications to the General Operating Instructions.

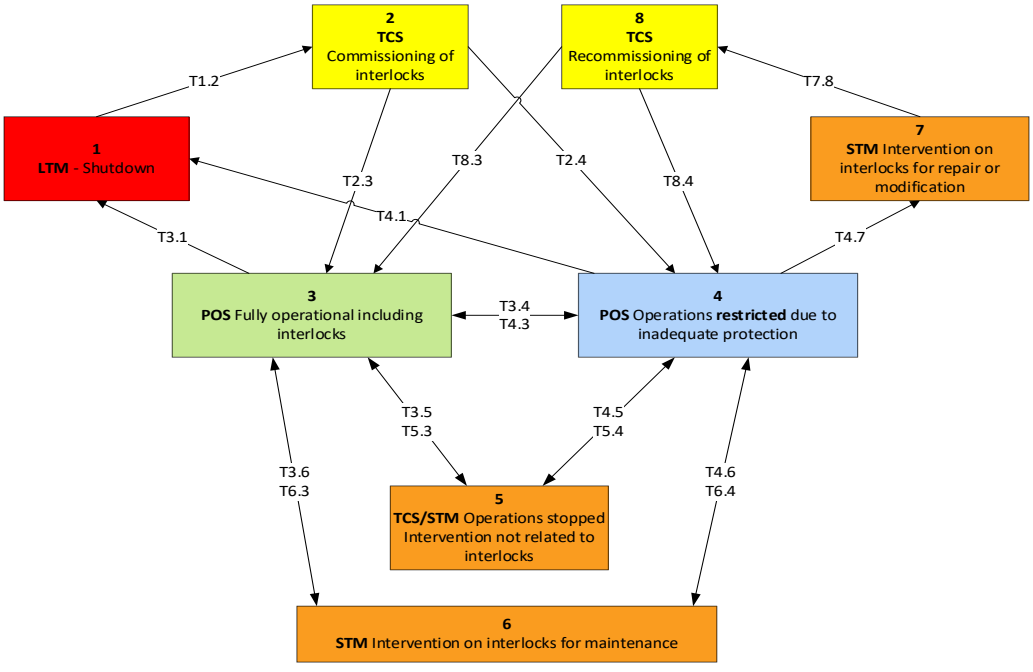

Figure 7: Machine Protection State Diagram

The process to be followed in case of a situation where the implemented protection needs to be modified is shown in Figure 8 where A, B, C and D identify the kind of modification to be performed to the implemented protection. This process can be initiated by anybody. The RACI matrix is defined in Table 13.

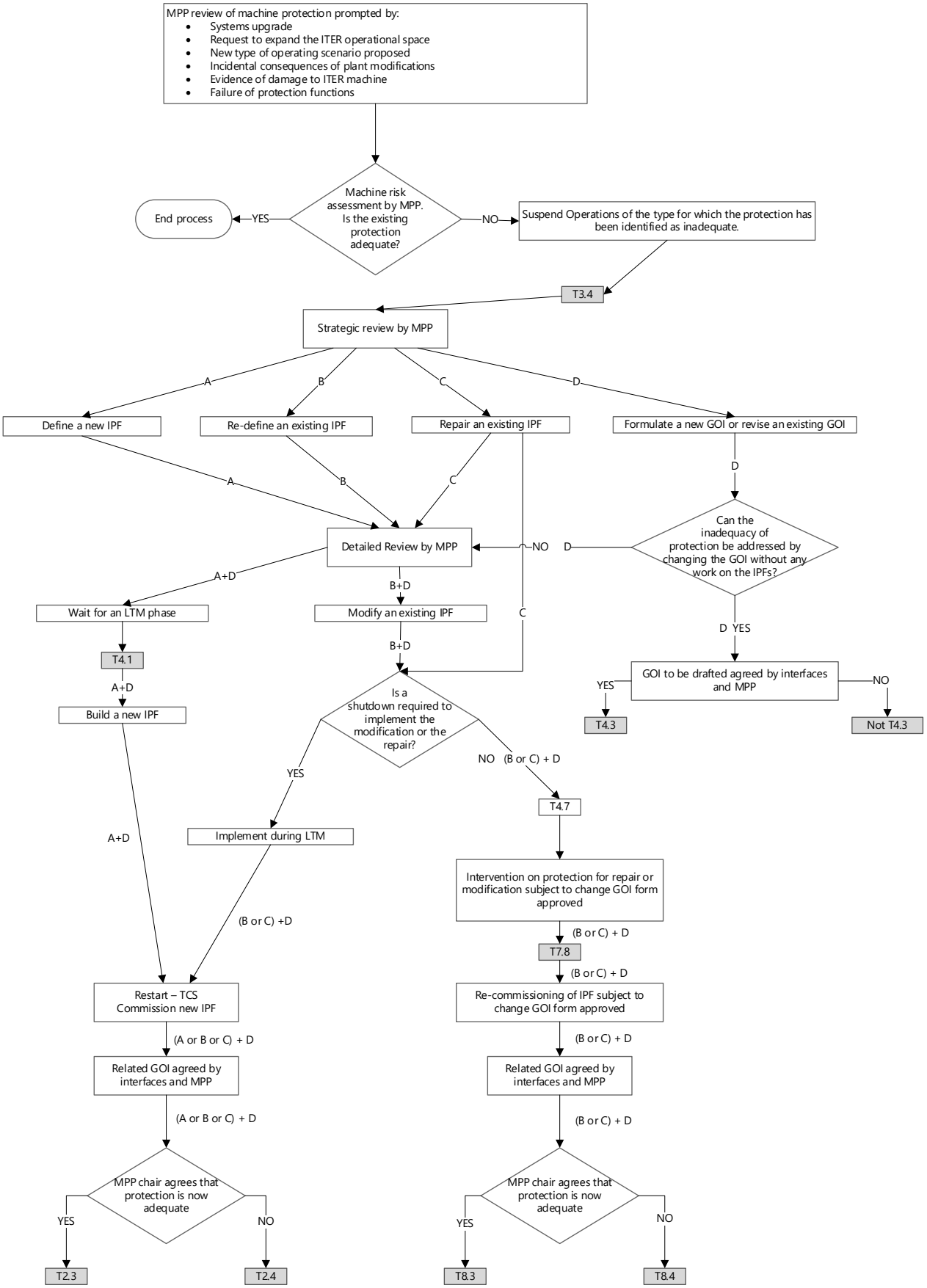

Figure 8: MPP review process and the GOS states required.

14. Responsibilities

The RACI matrices below relate to the initial process for risk assessment (section 7) and to the process during Operations (section 13), where R – Responsible (Doer), A – Accountable (Approver), C – Consulted (Reviewer), and I – Informed (User) .

Steps	MPP chair	MPP members	CIS/APS TRO	CODAC TRO	Plasma Operation TRO	PBS TRO	SID /SIRO
Risk assessment	I	C	C	I	I	A/R	I
MPP review	A	R	C	C	C	C	I
Transverse analysis	A	R	C	C	C	C	R
MPP review and issue RoD	A	R	C	C	C	C	I
Issue E/A/F (LOCAL technical specifications	A	C	C	C	C	R	I
Issue F (CENTRAL) technical specifications	A	C	R	C	C	C	I
Issue Investment Protection Plan	A	C	C	C	C	R	I
Implementation and Verification of IPF	C	C	A/R	I	I	R	I
Validation of ICS (CIS+PIS) (plan, procedures and non-functional validation)	A	R	R	C	C	R	I
Recommendation/justification for design change	A	R	C	C	C	R	I
IO Risk	A	R	I	I	I	I	I

Table 12: RACI matrix for the risk assessment process (section 7)

Steps	MPP chair	MPP members	CIS/APS TRO	CODAC TRO	Plasma Operation TRO	PBS TRO	SID/S IRO
Operation and Maintenance	A/R	R	R	R	R	R	I
Modifications to the ICS	A/R	R	R	R	R	R	I
Recommendation/justification for design change	A	R	R	C	R	R	I
IO Risk	A	R	I	I	I	I	I

Table 13: RACI matrix for the MPP process during Operations (section 13)