Memorandum / Note

PIS Operation and Maintenance

This document presents a preliminary study on future operation and maintenance of the PIS that have impact on the design of the systems. The document is the first version of one of the PCDH Satellite Documents for the interlocks.
<table>
<thead>
<tr>
<th>Version</th>
<th>Latest Status</th>
<th>Issue Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>v0.0</td>
<td>In Work</td>
<td>06 Nov 2012</td>
<td></td>
</tr>
<tr>
<td>v1.0</td>
<td>Approved</td>
<td>24 Jan 2013</td>
<td>Version for PCDH v7</td>
</tr>
<tr>
<td>v2.0</td>
<td>Approved</td>
<td>28 May 2014</td>
<td>New version before the iFDR and after results from R&amp;D contract and prototypes.</td>
</tr>
<tr>
<td>v3.0</td>
<td>Approved</td>
<td>21 Dec 2017</td>
<td>Major review of the document, updated according to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- ITER concept of operations (ITER_D_U3F88Z)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- CIS Override strategy(ITER_D_PKMDA8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- CIS Operation plan(ITER_D_RVUEU7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- CIS Maintenance plan (ITER_D_RVUJCC)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- CIS DDD (ITER_D_QCH3GJ)</td>
</tr>
</tbody>
</table>
# Table of Contents

1 SCOPE ........................................................................................................................................... 2
  1.1 PCDH CONTEXT .................................................................................................................. 2

2 ACRONYMS ..................................................................................................................................... 3

3 REFERENCE DOCUMENTATION .............................................................................................. 3

4 PRINCIPLES .................................................................................................................................. 4

5 INTERLOCK OPERATION REQUIREMENTS ........................................................................... 5

6 INTERLOCK OPERATION AND MAINTENANCE RELIABILITY ........................................... 8
  6.1 ICS OVERRIDE ASSESSMENT .............................................................................................. 9
    6.1.1 Threshold management ............................................................................................... 9
    6.1.2 Management of overrides ......................................................................................... 10

7 OPERATION ROLES AND ORGANIZATION ........................................................................... 11

8 IMPLEMENTATION OF INTERLOCK OPERATIONS ....................................................... 13
  8.1 MONITORING FROM CODAC TERMINALS ...................................................................... 13
  8.2 INTERLOCK DESK .............................................................................................................. 14
    8.2.1 Interlock desk profiles ............................................................................................ 15
    8.2.2 CIS Operation Introduction .................................................................................... 16

9 MAINTENANCE ............................................................................................................................. 17
  9.1 MAINTENANCE AND ENGINEERING FUNCTIONS ............................................................ 17
    9.1.1 System Diagnostics .................................................................................................. 17
    9.1.2 Post Mortem Analysis Tools .................................................................................... 17
    9.1.3 Function configuration ............................................................................................ 18
    9.1.4 Software updates ...................................................................................................... 18
1 Scope

This document presents the concepts of Interlock operation and the maintenance approach for the part of the plant system I&C which implements the investment protection functions (PIS). The document describes the operations that will be executed from the Control Room and the proposed tools. It also introduces the notion of procedures for operation and maintenance activities.

This document does not provide the guidelines to be followed by the plant system I&C designers for the implementation of the interfaces with the operation and maintenance tools. These are described in Guidelines for PIS design [RD3] for the hardware part and in Guidelines for PIS Configuration and Integration [RD4] for the configuration part.

Some of the explanations provided in this document only affect the CIS but they are provided to provide the whole framework. For example, the DLIB/BLIB are part of PBS-46 and are managed by CIS, since they are stored in the plant system cubicles and interact with that plant system, they are being mentioned.

The PIS designer can contact the PBS 46 responsible for more detailed information.

1.1 PCDH context

The Plant Control Design Handbook (PCDH) 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.

![PCDH Documents structure](image-url)
2 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLIB</td>
<td>Bypass Loop Interface Box</td>
</tr>
<tr>
<td>CBS</td>
<td>Control Breakdown Structure</td>
</tr>
<tr>
<td>CIN</td>
<td>Central Interlock Network (-A: Administrative / -P: Process)</td>
</tr>
<tr>
<td>CIS</td>
<td>Central Interlock System</td>
</tr>
<tr>
<td>CODAC</td>
<td>Control, Data Access and Communication</td>
</tr>
<tr>
<td>DLIB</td>
<td>Discharge Loop Interface Box</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>ICS</td>
<td>Interlock Control System</td>
</tr>
<tr>
<td>ES</td>
<td>CIS Engineer Server</td>
</tr>
<tr>
<td>PIS</td>
<td>Plant Interlock System</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller (slow controller)</td>
</tr>
<tr>
<td>PSH</td>
<td>Plant System Host</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervision Control And Data Acquisition</td>
</tr>
<tr>
<td>SM</td>
<td>CIS Supervisor Module</td>
</tr>
<tr>
<td>WinCC OA</td>
<td>WinCC Open Architecture – the ICS SCADA</td>
</tr>
</tbody>
</table>

Table 2-1: List of acronyms

3 Reference documentation

[RD1] Plant Control Design Handbook (27LH2V)
[RD2] Management of Local Interlock Functions (75ZVTY)
[RD3] Guidelines for the Design of the Plant Interlock System (PIS) (3PZ2D2)
[RD4] Guidelines for PIS configuration and integration (7LELG4)
[RD7] Implementation of High Integrity Operator Commands in the Interlock Control System (PKMDA8)
[RD8] 1-S1-01 Operation Plan (RVUEU7)
[RD9] 1-S1-02 Maintenance Plan (RVUJCC)
4 Principles

The plant systems will be delivered with their own control systems (Plant System I&Cs). The plant interlock systems are the part of plant system I&Cs which implement investment protection functions.

The CODAC (Control, Data Access and Communication) system is the central (supervisory) control system for the conventional plant control systems of ITER. CODAC is responsible for integrating all plant systems I&C and enabling the operation of ITER as a single integrated facility, providing overall plant system coordination, supervision, alarm handling, data archiving and plant visualization (HMI).

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 comprises the Central Interlock System (CIS), the various Plant interlock systems (PIS) and its networks. The ICS does not include the plant system sensors and actuators but it controls them.

The Central Interlock System (CIS) implements the central protection functions via the Plant Interlock Systems (PIS). It also provides access to the local interlock data of the various plant interlock systems.

The Plant Interlock System (PIS) are part of the plant systems I&C. Each PIS provides local protection by implementing the local interlock functions of the corresponding plant system. Also, most of the PIS participate in the central interlock functions coordinated by the CIS. All the sensors and actuators involved in machine protection in ITER are connected to at least one PIS in their plant system. The PIS constitutes the interface between the CIS and the plant systems.

One important characteristic of the Interlock Control System as machine protection system is that the operator does not take part in the protection function, no operation intervention is required during the execution (from event detected to action triggered) of an interlock function. The fact of a system being fully automatic minimises the hazard of human errors. The operation of the interlocks is, as well, independent of the operation of the process conventional control.
5 Interlock Operation Requirements

Operations affecting the interlocks are classified into two main blocks: the routine operations executed during the daily operation of the Tokamak and its associated systems, and the special ones carried out during commissioning, maintenance and calibration periods.

- Routine machine operation:

  ✓ Monitoring of CIS and PIS status and of interlock-related process variables and parameters. All the interlock variables and parameters required for operation of the interlock systems are displayed in the control rooms (e.g. machine states, central and local interlock events and actions, sensor information, results of diagnostics). In addition, messages are used to highlight deviations from routine operating conditions. The messages are identified with an understandable code label, with easy access to information linked to the messages and providing guiding means. The message processing and prioritization provides information on the first cause of the initiation of a protection action, filtering of redundant messages, inhibition of the messages which are induced by a common event which is itself signalled by an message, validation or inhibition of the messages depending on the plant situation in order to eliminate messages which are not significant in a given plant situation and messages grouping other individual messages that will be re-activated each time an individual message occurs. All the interlock variables and parameters, messages and relevant signals are logged and appropriate specialized analysis tools are available to analyse the interlock events.

  ✓ Monitoring of Interlock Controllers: The critical health monitoring provides basic monitoring of the interlock controllers in the control room. It allows easy recognition and rapid reaction in case of problems related to the hardware involved in the performance of the interlock functions.

  ✓ Reset (unlatch) of interlock functions, actuators and sensors: after the activation of certain central interlock functions, it is necessary to reset it before routine operation can resume. The interlock system will always supervise that all the conditions required for safe operation are met, and will only allow the function to be reset as the last step after a recovery from an interlock event. The reset shall be ignored by the system as long as the hazard (represented by a set of conditions and events) has not disappeared. This is why the reset is not considered a critical operation. These actions are performed from the interlock desk for the central functions and from CODAC by the Plant System expert for the local ones.

  ✓ Manual activation of Permits and Inhibits: These are operator preventive commands. Their activation (in the first case) or deactivation (in the latter) prevents the system from operating. A Permit can be raised by the operator but it is only granted by the interlock system if all other conditions for a safe operation are met. The difference with the reset is that the permit can be removed manually by the operator while the reset can only be performed when an automatic action has been triggered. These actions are performed from the interlock desk for the central functions and from the plant control by the Plant System expert for the local ones.
• Critical manual actions during operation and commissioning:

✓ **Overrides**: Interlock functions are put in place to protect ITER from wrong operation and other hazards. Therefore, masking an interlock event, disabling an interlock function or forcing an interlock action should be avoided as much as possible. However, in some situations during commissioning and maintenance it is necessary to operate certain systems outside their nominal conditions and thus the related interlock functions might have to be bypassed or certain interlock signals masked or forced. The masking of an event consists in artificially replacing its value by a pre-determined one (absence of event). The function disabling consists in disabling the coordinated function logic in order to avoid the action triggering (it is used when it is not possible to mask the event because the event is used for several functions for example). The forcing of an action consists in forcing it to a pre-determined state to avoid triggering the actuators. As these operations present a potential hazard, they must be managed in a way that the operator is aware at all times of the particular configuration and they should be easy to remove. An additional protective measure that is considered is to remove all the overrides when certain states are reached.

Overrides always set the overridden status in the dangerous mode: no interlock event, deactivation of the protection function or blocking of the protection action. Overrides are not used to test the systems by forcing events or actuators, but they put the system in a *blind* mode to allow special commissioning and maintenance tasks.

That is the reason why they are critical and have to be treated very carefully from the technical implementation point of view but also from the administrative side. These actions are only performed from the interlock desk.

✓ **Thresholds management**: thresholds normally remain fixed during routine operation, but have to be tuned during commissioning and maintenance. A design philosophy based on two threshold levels is proposed: one changeable threshold to select from the operational window, and a second fixed threshold value related to the design value of the components or system.

The threshold management is considered critical as it has an impact on the operational space and can affect the machine availability. This is the reason why they are also critical and have to be treated very carefully from the technical implementation point of view but also from the administrative side. These actions are only performed from the interlock desk.

**DLIB and BLIB verification**: All the interface boxes connected to the discharge and bypass loops of the system shall be tested periodically. The operator, following an administrative procedure allows the test mode before accessing the tool for interface boxes verification. This tool provides the information about the status of the different connections and will allow each channel to interfere individually. Due to the criticality of this operation, the test mode is only granted by the interlock system if all other conditions for a safe operation are met. These actions are only performed from the interlock desk.

• Critical actions during maintenance, performed by the CIS expert from the engineering workstation:
Detailed system diagnostics: Certain operation closely related to the interlock controllers may also be required in the control room for rapid reaction in case of problems such as the monitoring of the CPU and memory stats or network performance and parameters. So, in order to improve maintenance activities (i.e. repair and preventive), detailed diagnostics generally accessible via specific applications linked to the controller technology must be available in order to monitor hardware components (e.g. CPU, I/O modules, etc.), network status and performance and of communications links.

Function configuration: for correct operation, an interlock function may require certain parameters to be provided manually, depending on the operating state of the machine or a given component. These parameters have a direct impact on the performance of the interlock function and therefore are centralized in a database.

Software/Firmware updates: interlock functions, controller software and firmware may evolve in time as a result of changing requirements or improvements. These changes require a full or partial stop of the system (temporary disconnection of a module while the others stay on-line) and imply a direct intervention in the cubicle. A verification and validation cycle for each interlock function will have to be completed and changes will have to be thoroughly tested on the test bench. The procedure is described in Guidelines for PIS configuration and integration [RD4].
6 Interlock Operation and Maintenance Reliability

The Interlock Control System is a critical system with very strict reliability constraints. Prevention of malfunctioning due to hardware failures is achieved through several architectural strategies, including redundancy, high integrity of the components or test and maintenance policies. In order to protect against human operational errors, several aspects are considered during the design:

- Physical and geographical protection:
  
  ✓ Access to critical components and the performance of dangerous operations is only possible from certain locations. Depending on the type of intervention, it may be better either to centralize the actions in the Main Control Room or to only allow intervention at the cubicle level.

  ✓ Interlock cubicles must be easily distinguishable (i.e. labels) and use different keys to other systems’ cubicles.

- Protections at the Human Machine Interface level:

  ✓ Role-based access to the system: a role-based login system manages the kind of actions that an operator can perform using the HMI depending on his/her expertise and rights.

  ✓ Identification and label: interlock data must be easily distinguishable and labels will allow the operator to be aware of the interlock classification for the monitoring data and controls displayed/accessible on the HMIs.

  ✓ Confirmation step: a repeat confirmation step minimizes unintentional operator commands and may be used for some critical commands.

  ✓ Lock/Unlock system: a button may be used to lock the commands accessible on a system in order to prevent unintentional commands. Once locked all the operation manageable by the HMI cannot be performed: the locked system is still active but operator commands related to this system are disabled.

  ✓ Values of numeric configuration data shall be selectable among a list of possible values instead of manually entered

- Interlock system automatic self-protection against human errors: this self-protection should cover all possible routine operational mistakes as well as some special cases, including:

  ✓ The interlock system should ignore a manual instruction from the operator if it may lead to a dangerous situation or if the conditions are not correct for changing its internal status (e.g. request to close/reset the quench loop when there is still current in the coils; recovery of the Power Permit in a converter when cryogenic conditions are not met, etc.).
The interlock system should ignore an interlock override (input mask, function disabling or output forcing) when there is a dangerous pre-defined machine status (e.g. interlock override not allowed during certain plasma scenarios or coil current levels).

Even if some thresholds are changeable, the interlock system implement also fixed thresholds sticking with the design of the components or of the system.

Reliable administrative procedures, specially affecting the procedures of interlock overrides, shall be put in place.

6.1 ICS Override assessment

In assessing the significance of the overrides, all aspects of their use must be considered, as their application can impact on the machine availability in dissimilar ways. These critical operator actions are available from the CIS Desk, and only can be performed after the convenient administrative procedures have been correctly completed identifying the conditions when the override can be applied and the limitations on system operation.

The following points will be considered during the assessment of all overrides:

- The reason for the override, its means of implementation and justification.
- The equipment providing the required function, or change of function, should be engineered, not provided by temporary modification, e.g. the use of jumper leads is not allowed.
- The control interface of the operator and the system performing the function should be arranged to minimise the possibility of error.
- Arrangements to alert the operator, and ensure continuous awareness, of the current status of all devices and change of state.
- An analysis should be performed to determine the course of an inadvertent applied override in the event of an interlock or when the permissive conditions are lost, introduced. The analysis should consider the safety implication to plant and personnel independently, and the effects of inadvertent, incorrect application, removal of a function. These should be fail safe wherever reasonably practicable.

The implementation in the CIS final version will include protective measures to remove certain overrides when defined states are reached.

A complete description of the override concept developed for the ITER Interlock System can be found on [RD7].

6.1.1 Threshold management

The interlock thresholds normally remain fixed during routine operation. However some thresholds may need to be tuned up during commissioning and maintenance and, for very particular cases, some may even need to be changeable during normal plasma operations to allow certain operational scenarios.

The design principles applied for the Interlock System concerning thresholds are:

i. No interlock threshold management can be done from the plant system or CODAC conventional screens.
ii. No interlock threshold value can be directly entered by an operator from the CIS operation stations.

iii. If a threshold requires changes within an operational campaign, the possibility to select between different pre-set threshold values has to be engineered in the CIS operation station HMI.

iv. Any other change of a threshold value can only be made using the expert tools running in the interlock engineering workstation (which is only used during maintenance and commissioning periods) and following a strict authorisation and validation procedure.

6.1.2 Management of overrides

All the Overrides required for the operation of any Interlock controller will only be available from the Interlock Desk. The CIS Supervisor Module (WinCC OA – SCADA) will transmit the overrides commands to the controller via standard communications. The overrides will be applied only after the successful verification of the sequence of commands received from the Supervisor Module. The exchanged messages will be converted to be managed by the safety program.

The override commands will be used for masking an input, forcing an output or disabling a function.

The activation of overrides in the PLC safety program will stay active until the operator decides to remove that measure or when defined states are reached.

When a controller is shutdown, all the overrides are removed and shall be configured by the Interlock Operator to the required state.

The amount of information available in the CIS Desk requires a standardized representation and operation of the overrides to support a reliable operation.

Figure 2 provides an example of this representation in the operation screens in the CIS desk. The override commands will be represented by two different buttons, one for setting the override and the second one for its release.

The process status of the signal is represented as the main element and this status is not only indicated only by colour but also by text. An orange rectangle on the left of the main status representation indicates the presence of an override. Additionally; the status of the variable if the override is not present, is represented using a small square in the top right of the signal representation. Figure 2 provides also an example of the naming convention for the required variables, according to [RD4].
Figure 2 Concept of override representation in the CIS Desk
7 Operation roles and organization

There are three main actors in the operation of the Interlock System, as defined in [RD6]. From one side the ITER Engineer in Charge is the responsible of the coordinated technical operation of the whole ITER facility. The Plant System Operator is responsible of executing the operational procedures of the system, including the routine operations on the PIS. The Interlock Operator performs the routine operation of the Central Interlock System, but also is in charge of the critical operation of the whole Interlock System. Both the Plant system Operator and the Interlocks Operator are coordinated and report to the ITER Engineer in Charge. The Figure 3 provides a summary of the interactions in the operation of the Interlock System; the communication with the Engineer in Charge is represented by white arrows, while the critical operations on the PIS are represented by yellow and the non critical with grey.

![Figure 3: Operation roles and organization](image)

The detailed tasks and responsibilities of these roles are described below:

**- ITER Engineer in Charge**

The Engineer in Charge leads the Tokamak Operation Team in the Control Room and supervises and approves all operational activities based on the current Operating Procedures and Instructions.

The Engineer in Charge is responsible for:
- The safety of personnel in operational areas
- The safe technical operation of the ITER facility

**- Plant System Operators**

Plant System Operators are Suitably Qualified and Experienced Persons responsible for the commissioning, monitoring, configuration and operation of Plant Systems. Related to the operation of the PIS, the Plant System Operator is in charge of the non-critical operations on the plant interlock system, reducing the Interlock Operator tasks. The kind of PIS operations available to the Plant system Operator are the ones defined as “local routine” operations, including:
Local function reset
Sensor reset
Actuator rearm

Each Plant System Operator reports to the Engineer in Charge and is responsible for:

- Monitoring the status and availability of the Plant System and responding to alarms by implementing the appropriate procedure.
- Configuring and operating the Plant System Conventional Control subsystems according to the Operating Instructions to support the experimental and operational needs.
- Informing the Engineer in Charge and the Session Leader of any special condition that is likely to influence the ITER pulse or operation.
- Assisting the Engineer in Charge and the Session Leader in the identification and resolution of operational issues regarding the Plant System.
- In case of accident/incident, and always under the supervision and coordination of the Engineer in Charge, operating the Plant System so as to bring and maintain the ITER facility into a safe state.

- Interlock Operator

The Interlock Operator is the shift technician responsible for monitoring and operating the Interlock Control System, which includes both the CIS and PISs, performing the appropriate procedures to bring and maintain the safe operation of the plant.

The Interlock Operator is responsible for the continuous operation and monitoring of the facility on a 24 hour basis, responding directly to the Engineer in Charge during the operational shift. The Interlock Operator is in charge of the central functions “routine” operations, like the resets and permits. But it will be in charge of all the critical operations, for both local and central functions operation, meaning:

- Local function overrides
- Central function overrides
- PIS configuration
- CIS configuration

The Interlock Operator is supported by a CIS expert and will be in charge of performing the maintenance and engineering task, including: Software / Firmware updates and the monitoring of controllers and networks.
8 Implementation of Interlock Operations

One important characteristic of the Interlock Control System, as machine protection system, is that the operator does not take part in the protection function, no intervention is required during the execution (from event detected to action triggered) of an interlock function. The fact of having a system fully automatic minimises the hazard of human errors. The operation of the interlocks is, as well, independent from the normal operation via the conventional control system.

In terms of operator task, it has to differentiate between the routine operations that will be performed during the machine exploitation and the critical actions required for commissioning and maintenance.

![Figure 4. ITER Interlocks Operation](image)

The Operation plan for the CIS can be found on [RD8], where the scenarios and human resources allocation have been defined.

8.1 Monitoring from CODAC Terminals

Through the CODAC workstations in the control room, CODAC displays the state of the Interlock Control System to the control room operators, based on the information sent by CIS through the CODAC/CIS gateway and by the PIS through the PSH. From the Interlock System, the main functionality of these screens is the general monitoring of the different variables and management of the post mortem tools.
In the CODAC workstations, some screens/terminals are devoted to the expert operators of the different plant systems (Plant System Expert Supervisory). These screens allow a full access to all data (critical and non-critical) managed by each Plant Interlock System. The actions, however, are limited to non-critical actions (monitoring, reset of local interlock functions) as data are transferred through PON via CODAC PSH for the corresponding plant system.

8.2 Interlock Desk

The infrastructure in control room (replicated in main and back-up rooms) dedicated to the operation of the interlock is the Interlock Desk. This facility is composed of two different terminals (or groups of terminals): one devoted to conventional operations through SCADA, the CIS Operation Station, the other focused on maintenance tasks by means of specific software, the Engineering Workstation.

The Interlock Desk is connected directly to the CIN, and is accessible by the CIS supervisor module and the different servers (engineering, archiving...).

A set of dedicated terminals are available for the active execution of certain tasks on the CIS, either considered critical (override) or not critical (monitoring, reset / permits of interlock functions). This set of terminals also handles the access to CIS critical archiving database.

From an operational point of view, the CIS Supervisor is a SCADA consisting of one or several terminals that manage all connections to CIS and PIS through the CIS Supervisor module. It allows access the state of each function and memory variables of all the CIS controllers. All actions that are executed from this terminal during operation and commissioning require specific developments in the SCADA, in order to assure the adequate integrity of the operations and minimize the possibility of a dangerous situation in case of operator error.

When MCR cannot be used, the operators shall move to BCR for alternative operation of the CIS.

During commissioning and maintenance the design allows the presence of two operators and one expert working simultaneously in the Main Control room.

Figure 5: Interlock desk for commissioning
Two dedicated workstations equipped with Siemens WinCC OA client (as part of the Interlock Desk) are available for the supervision and management of the CIS. The range of available operations includes reset of central and local interlock functions and the execution of high level actions like threshold selection, inhibits and overrides.

The CIS supervisor does not share any infrastructure with CODAC. This allows a proper segregation between the SCADA of the two systems.

Specific interlock commissioning, or the commissioning of other systems requiring critical actions on the CIS (i.e. overrides), are carried out through the CIS supervisor by means of specific HMI screens. These ad-hoc screens help the operator avoiding human errors and warn that the situation entails a potential hazard for the machine. Self-defense methods are implemented. The use of direct access to the code or the controller memory positions is avoided for these tasks and not possible from this terminal.

All dangerous operations possible from the CIS Operation Station are engineered in the HMI.

8.2.1 Interlock desk profiles

There are three profiles with different levels of access for interlock operation. The lowest access profile is the CIS supervisor. This profile has no login level for CIS desks (CIS operation, CIS Engineering workstation). The CIS supervisor has only visualization rights, he or she can only monitor statuses, access to archived data and logged messages. Also it can only recognize warning messages. This access level cannot give any command to the CIS operation stations.

The second access authority is CIS Operator. This access authority is for operating the CIS and includes the CIS supervisor authority. The access authority of the CIS Operator can: release CIS interlocks, handle Permit/Inhibit, controlling overrides (i.e. event masking, action forcing, function disabling), and select of thresholds.

The third and highest access authority is CIS Expert. This access authority is for actions related to the commissioning and maintenance of Interlock System. The CIS Operation Station and the Engineering Workstation have independent access authority, so the CIS Expert can access only to the Engineering Workstation and it is not allowed to access the CIS Operation Station. The kind of operations allowed to the CIS Expert ranges from function configuration, threshold management, and update and administration of programmable software/software tools/firmware.

The Table 7-1 provides a summary of the interlock desk profiles.

<table>
<thead>
<tr>
<th>Access Authority Level</th>
<th>CIS Supervisor</th>
<th>CIS Operator</th>
<th>CIS Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Station</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS Operation Station</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Engineering Workstation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowed Operation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring archived data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message recognition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Include CIS Supervisor Authority</td>
<td>Release CIS Interlock</td>
<td>Handling Permit and Inhibit status</td>
<td>Override</td>
</tr>
<tr>
<td>Masking event</td>
<td>Forcing action</td>
<td>Disabling function</td>
<td>Selection of threshold</td>
</tr>
<tr>
<td>Function configuration</td>
<td>Threshold management</td>
<td>Update programmable software</td>
<td>Update software tools</td>
</tr>
<tr>
<td>Update firmware</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 8-1 Summary of Interlock desk profiles
8.2.2 CIS Operation Introduction

The interlock operation is arranged with a page hierarchy which present progressive exposure of more detailed information. The first page provides an Overview screen, providing a summary of the whole Interlock system. Then the next pages comprise detailed information where the actual interactions with a process occur. The page hierarchy enables operator to navigate from the overview to the more detailed information in a logical manner. The HMI hierarchy has been arranged in several levels:

- Level 1: This Page 0 contains an overview that covers monitoring of the entire plants by operators.
- Level 2: This level shows the sub-units of a large process for CBS 1. This screen should show the information and controls necessary to perform the tasks for each of the sub-units.
- Level 3: This level is separated by the function groups of HMI. Therefore, operators easily approach it on their own purpose.
- Level 4: If, it is hard to show all of the sub-units in a screen for the Level 3, other screens, separated by CBS can be reached. These screens should show the information and controls necessary to perform the tasks for the sub-units for each plant systems.

A preliminary tree hierarchy for the CIS screen is illustrated on Figure 6, and examples of a page 0 and an operation screen are provided in Figure 7.

![Figure 6: Tree of Screen Hierarchy](image)

Figure 6: Tree of Screen Hierarchy

![Figure 7: Example of Interlock desk mimic – Page 0 and Operation screen](image)

Figure 7: Example of Interlock desk mimic – Page 0 and Operation screen

More detail information about the Interlock Operation HMI can be found on the “Operation” section of [RD5]
9 Maintenance

During operation of ICS there will be continuous preventive maintenance of the physical, computer and communication environment of Interlock System hardware. Any problems will be reported by the Operation Stations and appropriate maintenance/repair activities will be launched.

The preventive maintenance ensures that the software, hardware and network infrastructure used in ITER machine operations are running and are in a healthy condition. The design objective is to fulfil the functional requirements with a minimum load on the network and monitoring systems. If any of the components degrades in the performance, it generates an alarm and/or warns the operator to take the corrective action. It collects health statistics and resource utilization useful to maintenance engineers for capacity planning and scaling up the system.

Hardware (infrastructure) maintenance is very different to maintaining software (CIS applications). The former is driven by component lifecycle management and preventive maintenance, whilst the latter is driven by changing requirements and upgrades to the operating environment in which the software runs. To some extent, the software maintenance is therefore driven by the external factors like the end of support from manufacturers for certain releases of operating systems and commercial software packages.

9.1 Maintenance and Engineering Functions

9.1.1 System Diagnostics

Certain operations closely related to the interlock controllers may also be required in the control room for a rapid reaction in case of problems. This is the case for the monitoring of the CPU, memory statistics or network performance and parameters. So in order to improve maintenance activities (repair and preventive), detailed diagnostics generally accessible via specific applications linked to the controller technology must be available in order to monitor hardware components (CPU, I/O modules, etc.), network status, its performance and of communications links. All Interlock systems integrate auto-diagnostics functions like:

- All hardware components status is monitored (CPU, communications, I/O modules...)
- Communication links are monitored by watchdog principle.
- On failure detection, a common warning system fault is reported to the Interlock desk and shown in CODAC to warn control room operators. The message has different priority levels depending on the criticality of the failure.

9.1.2 Post Mortem Analysis Tools

The Post Mortem Analysis (PMA) is a set of software tools that allows a semi-automatic analysis of the causes and consequences of any event. This kind of analysis for the Interlock events could be done in the CIS Operation station and in CODAC workstation using different tools. The main goal of the PMA is to organize the collection and analysis of the transient data recorded during an Interlock event by all the I&C systems. The PMA makes the reconstruction of the event sequence that leads to the event condition. The online analysis generates an overall view of the interlock event sequence.

The Post Mortem Analysis of non-critical data is related to the conventional logging system and is in the scope of the PBS-45 (CODAC).
9.1.3 Function configuration

An interlock function may require certain parameters to be set manually, depending on the operating state of the machine or a given component. These parameters have a direct impact on the performance of the interlock function and thus are centralized in a database accessible through the Engineering Workstation (see below).

9.1.4 Software updates

Interlock functions, controller software and firmware may evolve with time, due to change in requisites or improvements. These changes require a full or partial stop of the system (temporal disconnection of a module while the others keep alive) and imply a direct intervention on the cubicle. The verification and validation cycle for each interlock function has to be respected, and changes shall be thoroughly tested in the test bench before proceeding with the update via the Engineering Workstation.

Together with the CIS Operation Station, an Engineering Workstation is available to access directly all the programmable or configurable equipment forming the CIS, for monitoring, programming, configuring, firmware update, etc. This Engineering Workstation connects remotely to the Engineering Server, which contains all the software, firmware and associated licenses needed to fulfil its function. The code is stored in a central repository, with strict control to access and modifications, accessible from the Engineering Workstation and Test Platform.

All software updates will be verified prior to its promotion to the production system. The PIS software updates will be verified against the miniCIS and the development process shall follow the guidelines for integration as defined in [RD4].

Figure 8 illustrates the verification flow for new CIS/PIS developments. Additionally, the CIS Replica and PIS Simulator will provide training environment for Interlock operators and CIS experts.

![Figure 8: Implementation and validation of ICS functions](image-url)