Fusion Engineering and Design 129 (2018) 104–108

Contents lists available at ScienceDirect

Fusion Engineering and Design

journal homepage: www.elsevier.com/locate/fusengdes

The ITER interlock system

J.L. Fernández-Hernando[a,f,*], D. Carrillo[b,f], G. Ciusa[c,f], Y. Liu[a,f], I. Prieto-Díaz[d,f], R. Pedica[c,f], S. Sayas[d,f], J. Soni[a,f], A. Vergara[e,f]

[a] ITER Organization, route de Vinon sur Verdon, CS90 046, 13067 St. Paul lez Durance Cedex, France
[b] Ciemat, Av. Complutense, 40, 28040 Madrid, Spain
[c] Vitrociset, via Tiburtina 1020, 00156 Roma, Italy
[d] Iberdrola Ingeniería y Construcción, Av. Manoteras 20, 28050 Madrid, Spain
[e] Arkadia,298 avenue du club Hippique, 13090 Aix-en-Provence, France
[f] European Spallation Source ERIC, P.O. Box 176, SE-221 00 Lund, Sweden

ARTICLE INFO

Keywords:
Machine protection
Interlock
SIL
PLC
FPGA

ABSTRACT

ITER involves the integration of numerous sophisticated systems, many of which must operate reliably close to their performance limits in order to achieve the project's scientific goals. The teams responsible for exploiting the tokamak will require sufficient operational flexibility to explore a wide range of plasma scenarios within an operational framework that ensures that the integrity of the machine and safety of the environment and personnel are not compromised. The instrumentation and control (I&C) systems of ITER are divided into three separate tiers: the conventional I&C, the safety system and the interlock system. This paper focuses on the last of these. The operational experience from existing tokamaks and large superconducting machines, together with many specific aspects of the ITER facility, have been taken into account in the design of the ITER interlock system. This consists of a central element, the Central Interlock System, and several local elements, distributed across the various plant systems of the tokamak and referred to as Plant Interlock Systems. Each Plant Interlock System is connected to dedicated networks and communicates its status and interlock events to the Central Interlock System, which in turn sends the required interlock actions to the Plant Interlock Systems. The Central Interlock System is also responsible for communicating the status of each system to the operators in the main control room. These operators will use the Central Interlock System to perform functionalities such as overrides, resets of central interlock functions and configuration of Plant Interlock Systems. Three different types of architecture have been developed: a slow one, based on PLCs, for functions for which response times longer than 300 ms are adequate, a fast one, based on FPGAs, for functions which require response times beyond the capabilities of the PLC, and a hardwired one to synchronise all the systems involved in a fast discharge of the superconducting coils. The overall design of the Central Interlock System was presented and approved for manufacturing in a Final Design Review in 2016.

1. Introduction

Interlocks are the instrumented functions of ITER that protect the machine against failures of the plant system components or incorrect machine operation. Regarding instrumentation and control (I&C), the Interlock Control System [1] ensures that no failure of the conventional ITER controls can lead to a serious damage of the machine integrity or availability.

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.

The Central Interlock System (CIS) forms, together with CODAC and the Central Safety System (CSS), part of the ITER I&C Central Systems [2]. The CIS is in charge of implementing the Central Protection Functions via the Plant Interlock Systems (PIS) through the Plant Interlock Network (PIN). It also provides access to the local interlock data of the different Plant Interlock Systems.

The ITER interlocks are in charge of detecting, or if possible preventing, any combination of states that may set the machine in a dangerous scenario for one or several of its components. The interlocks are also responsible of performing the required sequence of protective

[*] Corresponding author at: ITER Organization, route de Vinon sur Verdon, CS90 046, 13067 St. Paul lez Durance Cedex, France.
E-mail address: juanluis.fernandez-hernando@iter.org (J.L. Fernández-Hernando).

https://doi.org/10.1016/j.fusengdes.2018.02.059
Received 22 June 2017; Received in revised form 30 January 2018; Accepted 16 February 2018

actions to bring back the machine to a safe state while minimizing the time to resume operations.

2. System integrity and performance requirements

The ITER interlock system, as an essential component for the success of ITER, shall be designed, built and operated according to the highest quality standards. The international standard IEC-61508 [3] has been chosen as the reference.

To be compliant with the recommendations of this standard, a system providing interlock functions should meet the reliability design requirements that are:

- Qualitative requirements on fault behavior
- Quantitative requirements translated into probability of loss of function

The IEC-61508 introduces the notion of Safety Integrity Level (SIL). In order to avoid confusion with ITER terminology in which the term 'Safety' is used only for environmental and personal safety, the term 'SIL' is avoided within the interlock context. The term 'ITER Interlock Integrity Level' or '3IL' (tril) is proposed to differentiate different dependability levels for an interlock function.

The CIS has performance requirements such as:

- The CIS shall be designed to be continuously operational 24 h/24 h: repair of one faulty component shall be possible without interruptions of the CIS. The CIS hardware is redundant and geographically separated.
- During local commissioning of non-online systems, it shall be possible to apply the CIS operational states locally to the non-online system.

3. Protection functions and architecture

The main sources of risk to the ITER investment are (not necessarily by order of importance): the superconducting magnet system and its associated equipment, the plasma itself, the plasma heating and fueling equipment (e.g. neutral beams and electron/ion cyclotrons), and the vacuum, cryogenic and water cooling systems.

In order to simplify and modularize the design, the protection functions for each plant system were divided in two types: local and central. The first ones are the protection functions implemented autonomously by one plant system without requiring intervention of other ITER equipment. In other words, local functions are those in which the sensors, actuators, and interlock logic are implemented by one ITER system. In contrast, the central interlock functions are those protection functions for which the event is detected by one (or several) plant systems and the protection action carried out by another one. The central interlock functions are coordinated by the CIS via the Central Interlock Network (CIN) and implemented together with the PIS of the affected plant systems.

3.1. Response time requirements

In both CIS and PIS cases two main architectures are used: a slow architecture based on PLC technologies, for the local and central functions with response time requirements slower than 100 ms and 300 ms respectively; and a fast architecture, for the functions with faster time requirements, based on FPGA technologies. This fast architecture is not required for all plant systems. Communication within the different architectures is carried out through the CIN and/or hardwired interconnections, for the CIS, and through the PIN for the case of local interlock functions (within one plant system).

Apart from the slow (PLC based) architecture, and fast (FPGA based) architecture, a third architecture (hardwired) is also used at certain situations for the direct coordination of different plant systems: hardwired loops, also called discharge loops, are connected to sensors and actuators of different systems in order to maximize integrity and simplicity. The hardware loops are managed by the CIS and the clients are connected to the loop via a Discharge Loop Interface Box (DLIB), providing electrical isolation for assuring the segregation between the current loops and the user connected to the interface box. The design of the discharge loops and the DLIB is based in the LHC Beam Interlock System [4] and their user interface [5].

3.2. Modular design

The CIS is divided in different functional and hardware modules in order to allow flexible operation and maintenance as well as progressive integration and commissioning. The concept behind this division is that the different central interlock functions are assigned to one (or several) module(s) based on different criteria like installation & commissioning, operation & maintenance (modularity should provide flexibility) or performance.

According to the identification and classification of the central interlock functions, the following considerations are met:

- Installation: the system shall be designed in such a way that the incorporation of new PIS to an existing and operating version of the CIS involves a minimum modification on the running components installed for the previous versions.
- Operation and maintenance: one of the main objectives of modularity is to ease operation and maintenance, providing as much flexibility as possible. It should be possible to perform modifications or even disconnect a module, depending on the operation circumstances, while other CIS functions remain active.
- Key systems: some systems are critical from an interlock point of view (e.g. superconducting magnets) so it is convenient to group all the interlock functions involved in only one module. On the other hand, the interaction with one system may be of such nature (e.g. Plasma Control System) that it is required to centralize the interface via one CIS module.
- Performance requirements: functions requiring fast performance should be implemented on the fast architecture while functions having slow performance requirements can be implemented either in fast or slow modules.
- Integrity requirements: interlock functions are classified in 3IL-2 and 3IL-3 levels of integrity. All modules included in CIS are suitable for architectures up to 3IL 3, and thus can comply with all required integrities. The use of several modules in series for the implementation of an interlock function should be also minimized as much as possible.

In all cases the organization of the different CIS modules has taken into account the integrity requirements imposed to the different central interlock functions. Five modules have been defined based on the above criteria (see Fig. 1).

The Supervisor Module (SM) is not executing any central interlock function, therefore it is not considered as part of the machine protection chain. However, it is in charge of all general management of the ICS data, providing interfaces to the administrative services of the CIS.

The System Protection Module (SPM) is in charge of the interlock functions triggered by the plant systems related to utilities (Steady State Electrical Power, Vacuum, etc.), and in general most of the interlock functions required during all ITER operating phases. SPM is implemented based on the slow architecture.

The Coil Protection Module (CPM) implements all the protection functions related to the superconducting coils and the associated equipment such as the ACDC converters, resistive bus bars, etc. The idea of focusing all functions related to powering of the machine is to simplify the configuration and maintenance activities. This module

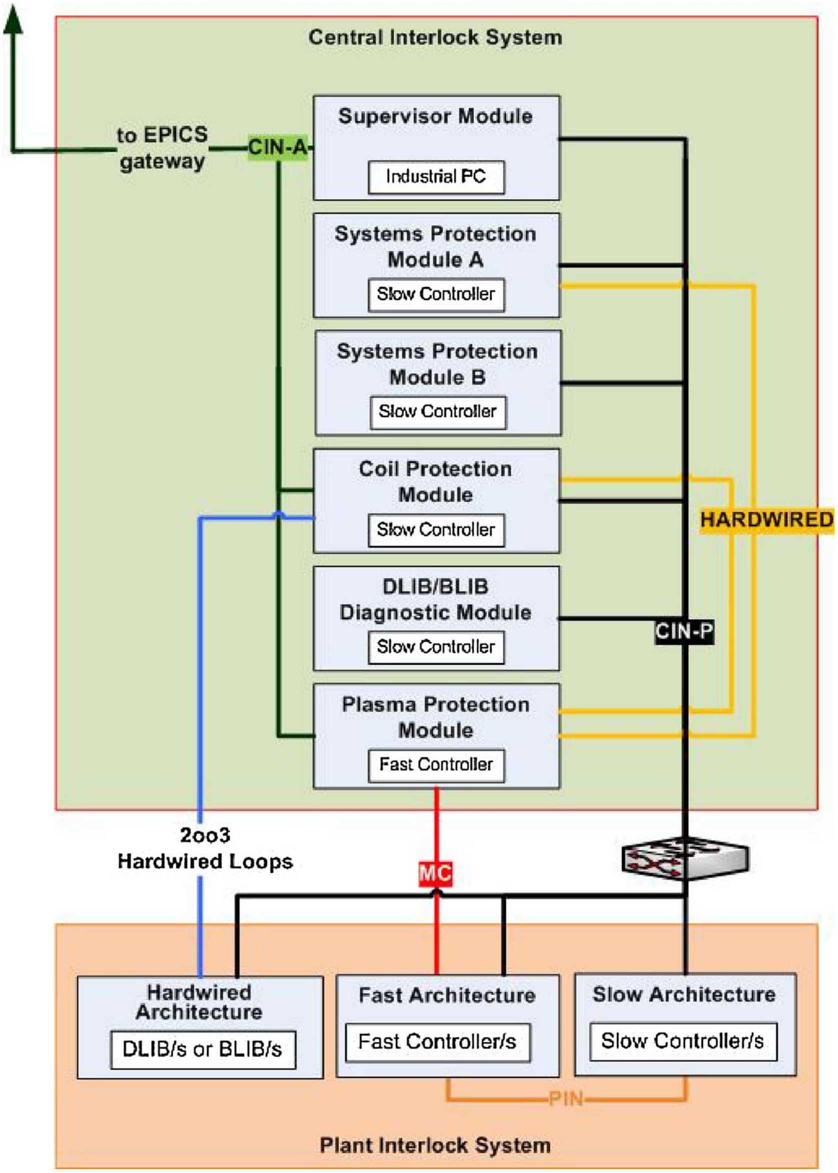

Fig. 1. Central Interlock System Modules together with the different Central Interlock Networks (CIN-A, CIN-P), hardwired connections, Manchester Coding (MC) serial protocol connection (for fast architecture) and Plant Interlock Network (PIN).

implements as well the interface with the hardwired architecture, implementing the direct control on the opening/closing and monitoring of the different current loops, through remote I/O. CPM is implemented based on the slow architecture.

The Plasma Protection Module (PPM) is in charge of the interlock functions related to plasma (e.g. PCS, plasma heating systems, Disruption Mitigation System, etc.), requiring a fast response. Therefore, during non-plasma activities, disconnection of the module should be possible for configuration or maintenance purposes. This module has the particularity that, given the interaction with PCS and other plasma requirements, it has tighter timing constraints and thus has to be implemented on a fast architecture, based on FPGA technology.

The DLIB Diagnostic Module (DDM) is in charge of acquiring the diagnostic data of all DLIBs through CIN-P (which is a sub network of CIN). This module is not involved on the machine protection function and its purpose is only diagnostics and tests of the hardwired loops.

Fig. 2 shows an scheme of the interface between a PIS, combining fast and slow architectures, and the CIS. The fiber optic cables (F.O. cable) are the ones transmitting the Manchester Coding serial protocol between the fast PIS and the PPM. The twisted pair (TP) cables are Ethernet cables connecting the slow architecture. Between the two chassis of the fast controller a Serial Peripheral Interface (SPI) [6] connection is used for monitoring purposes. The PIS is also connected to CODAC networks such as the Plant Operation Network (PON) and the Time Communication Network (TCN).

4. System performance

The kernel of the slow architecture is the Siemens S7 400-FH PLC. This slow controller is certified as suitable for its use as a SIL-3 controller (by an independent organization) and it is used for the implementation of all 3IL-2 and 3IL-3 central interlock functions. This high level of integrity is achieved by means of redundant code execution (internally in each CPU) and a fail-safe communications protocol. S7-400 FH is used because it allows a redundant configuration which is a design requirement for the CIS. Each CIS module will be distributed between two server rooms at different buildings. S7-300 series would

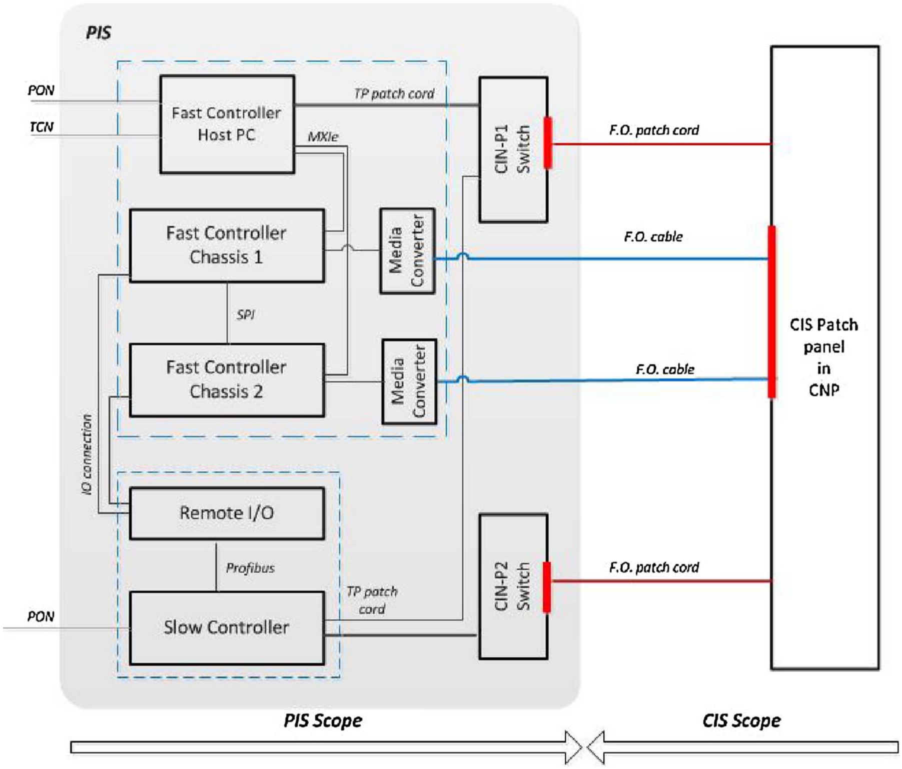

Fig. 2. Connections of a PIS to the CIS.

Table 1
System performance values.

Parameter	Value
Overall CIS availability (20 years)	0.999585
CIS Integrity (Probability of Failure per Hour)	
Lowest (Best)	5.30×10^{-9}
Highest (Worst)	3.21×10^{-8}
Max. number of Central Interlock Functions	1000
Number of CIS modules	6
Number of PIS modules	42
slow controller modules:	35
fast controller modules:	7
Nominal slow architecture performance (t)	
For local functions:	100 ms
For central functions:	300 ms
Worst case[1] slow architecture performance (t)	2.2 s
Nominal PPM performance (t)	~50 µs
Worst case[2] PPM performance (t)	< 100 µs

[1] PLC switch-over due to power failure of PLC.
[2] Event arrives just after PPM has read the previous one. PPM reads events at the interval of 50 µs.

not allow this.

The s7-400 F-CPUs are implemented as 1oo1D structure with diverse application software on a single channel hardware. Fault detection is implemented by comparison of the diverse application software results in the CPU and the independent F I/O, internal self-test and program and data flow monitoring in the CPU and fault monitoring by the F-I/O.

The following failure control measures are implemented in the CPU:

- Redundant execution with data and code redundancy and diversity and comparison of the diverse results.
- Self-test of safety-related operation in each cycle.
- Program and data flow monitoring.

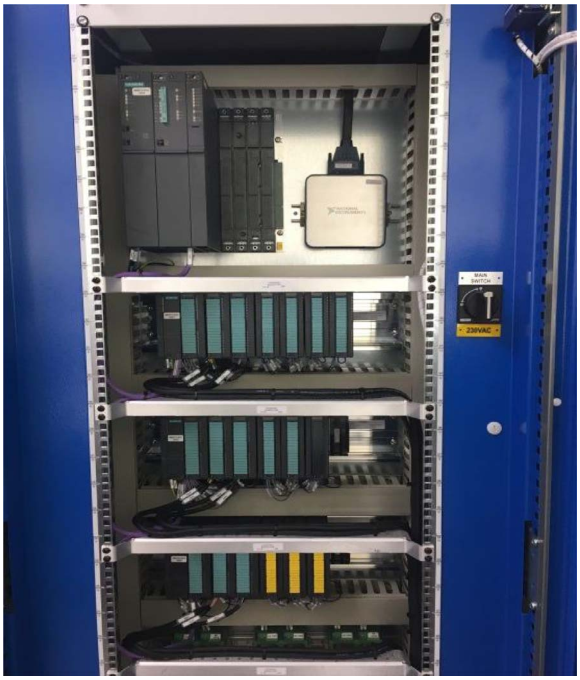

Fig. 3. One of the CPM CPU PLC together with its remote I/O.

Checking of this and fault reaction is done directly by the CPU itself as well as indirectly by the recipients of the CPU's failsafe outputs.

In addition the CPU performs self-test in the background and uses two independent time bases. One CPU is enough to achieve the certified functional safety. In the S7 400FH two redundant CPU are used in 1oo1D configuration to increase availability.

It is intended to execute functions with slow timing requirements, which have been established slower than 300 ms. The typical response time of the slow CIS architecture is between 200 ms and 500 ms.

The fast controller technology shall permit to implement functions requiring response performance starting at 100 μs. The requirement to meet these reaction times and the 3IL-3 make it very hard to rely on software running on a PLC or other type of system. The ability for the user to reconfigure the interlock functions makes field programmable gate array (FPGA) technology an ideal candidate. The chosen fast processor technology is NI compact RIO [7].

Table 1 lists the main performance values of the CIS which are within the requirements needed in order to respond to an interlock event in a timely manner and with the right level of integrity and availability.

5. Conclusions

The ITER interlock system is in charge of protecting the tokamak against component failures or dangerous machine operation. Because of the unprecedented technical and managerial complexity of the ITER Project, the traditional simplicity of the interlock systems for scientific experiments has been replaced by a more complex approach in which new performance requirements, usually out of machine protection systems, are being targeted, while trying to keep the high level of robustness and integrity inherent to interlock systems.

This will most likely be the first machine protection system built with most of its components provided in-kind from up to 36 different countries. A strong effort is being put in place to ensure that all actors involved across the globe design, build and configure the parts of the puzzle under their responsibility such that these can connect properly to the central system, while keeping the global reliability figures above the targeted requirements. Standardization of hardware, software and methods are essential to build an interlock system with such procurement strategy.

The ITER interlock system completed its final design in March 2016. Construction of CIS V.1 was performed in Korea during 2017. Fig. 3 shows the interior of one of the cubicles hosting the CPM.

References

[1] L. Scibile, et al., An overview of the iter interlock and safety systems, Proceedings of ICALEPCS, WEC005, Kobe, Japan, 2009.

[2] A. Wallander, et al., Approaching final design of ITER control system, Proc. of ICALEPCS, San Francisco, 2013 http://jacow.org.

[3] IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems.

[4] The Beam Interlock System, Engineering Specification LHC-CIB-ES-0001-00-10.

[5] User Interface to the Beam Interlock System AB-CO-Note 06-XX 1v4.

[6] SPI Block Guide v3.06, Motorola/Freescale/NXP, 2003.

[7] E. Barrera, et al., Implementation of ITER fast plant interlock system using FPGAs with cRIO, Proceedings of the 2016 IEEE-NPSS Real Time Conference (RT) (2016) (20161997).