Fusion Engineering and Design 129 (2018) 73–77

Contents lists available at ScienceDirect

Fusion Engineering and Design

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

Methodology for the deployment of ITER Fast Plant Interlock system. Use case: ITER Poloidal Field and Central Solenoid coil's power converter protection system

E. Barrera[a,*], M. Astrain[a], I. Prieto[b], M. Ruiz[a], J.L. Fernandez-Hernando[b], R. Pedica[c], J.M. Barcala[d], J.C. Oller[d], M. Afif[e]

[a] Instrumentation and Applied Acoustic Research Group, Universidad Politécnica de Madrid, Spain
[b] ITER Organization, St. Paul-lez-Durance, France
[c] Vitrociset, SPA, Via Tiburtina, 1020, Roma, Italy
[d] Asociación Euratom/CIEMAT para la Fusión, Madrid, Spain
[e] National Instruments, Austin, TX, USA

ARTICLE INFO

Keywords:
Interlock
FPGA
CompactRIO
IEC-61508
Reliability
Availability

ABSTRACT

Interlocks are the instrumented functions of ITER that protect the machine against failures of the plant system components or incorrect machine operation. Regarding I&C, the Interlock Control System ensures that no failure of the conventional ITER controls can lead to severe damage of the machine integrity or availability.

ITER Interlock System incorporates several Plant Systems that require response times below 1 ms to perform the required protection actions. Systems like the Coil Power Supply System (CPSS), Ion Cyclotron Heating and Current Drive (ICH&CD), Neutral Beam Injectors and Current Drive (NBI&CD), Disruption Mitigation System (DMS), and others. ITER developed a methodology to create the fast architecture for the Plant Interlock Systems (PIS) that ensures high integrity on the final solution.

The functional safety standard IEC 61508 has been used to define a methodology for the configuration of the RIO (Reconfigurable Input/Output) platform from National Instruments (compactRIO platform).

This work describes in detail this methodology, valid for most cases just selecting different input/output signal types to be handled and choosing different numbers of interlock functions to be performed. In addition, this paper describes the development of the interlock system for the ITER Poloidal Field and Central Solenoid Coil's Power Converter protection, a special case due to its unique configuration, the most complex implemented up to date. The development of this special case "puts to a test" the methodology's approach. Finally, the discussion of the fitness of the methodology and the performance of the system is presented.

1. Introduction

ITER's design philosophy recommends Commercial off-the-shelf (COTS) hardware usage and establishes "in-kind" supply of Plant Systems. To ensure compatibility between all Plant Systems and Central Interlocks the Plant Control, Design Handbook (PCDH) defines the design rules [2]. This philosophy entails an interface rich environment and requires a flexible design. ITER's Fast Plant Interlock systems (F-PIS) aims at delivering performance, adaptability, and reliability all at once. Previous state-of-the-art technology can be seen in [3] with similar requirements (< 100 us) interlock functions, and a safety integrity level 3 (SIL-3) were realized with Versa Module Europe (VME) chassis technology and custom-made hardware [4]. While this approach proved to be very effective, ITER's procurement approach implies that another method needs to be explored.

To meet the requirements, ITER explored FPGA technologies. An architecture has been defined and developed following a failure modes analysis and adding diagnostics to improve the final integrity of the solution. The Fast-PIS solution consists of a "double-decker" configuration: two NI compact RIO (cRIO) 9159 chassis, each containing a Virtex-5 FPGA, implementing diagnostics and voter architectures with a communication link between them to coordinate the parallel operation [1].

The logic implemented on the FPGA and the I/O modules are chosen to meet the specifications of each Plant subsystem [5]. Each of these ITER subsystems (like the ECH, ICH, vacuum, etc.) requires different

* Corresponding author.
E-mail address: eduardo.barrera@upm.es (E. Barrera).

https://doi.org/10.1016/j.fusengdes.2018.02.057
Received 14 October 2017; Received in revised form 15 February 2018; Accepted 16 February 2018

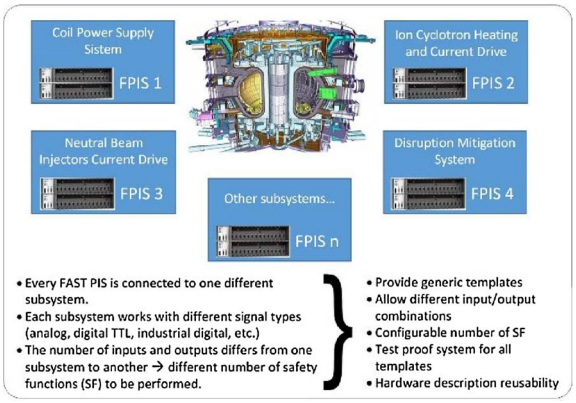

Fig. 1. Examples of ITER Plant Subsystems.

signal types: analog, digital TTL, industrial digital (24 V), etc. The number of input and outputs, as well as the number of interlock functions, is also dependent on the system (see Fig. 1).

The methodology is based on templates of FPGA implementations for the various types of Interlock Function (IF), allowing different I/O combinations. Additionally, the critical communication with the Central Interlock System (CIS) required for global coordination of interlock functions is based on Manchester coding with a specifically defined message frame. This functionality has been included in some templates to allow the communication of Events and Actions when they are required to perform an interlock function [5].

A proof-test system, also based on NI cRIO technology and NI TestStand, is used to provide the validation of the configuration and to assess the performance, generating all the input combinations for the F-PIS and reading the outputs.

2. Methodology

The methodology is based on the development and deployment of different templates, which manage the combinations of the specified inputs and outputs.

The methodology incorporates two different phases:

First, development of templates. This stage consists of the design of the hardware description for different configurations, all of them based on cRIO, but incorporating mixed input/output signals (analog, digital −TTL and 24V-) and providing a configurable number of interlock functions. All of these templates are stored in an ITER SVN repository (see Fig. 2). For each of them, a specific configuration of the test proof system has been developed to prove their proper operation and to obtain data on its performance.

Second, deployment of specific fast PIS. This phase is addressed for

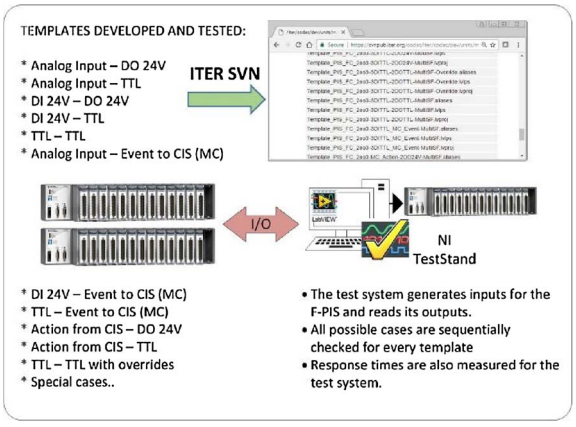

Fig. 2. ITER SVN repository with developed and tested templates.

each particular F-PIS. To do this, the hardware modules are assembled into the cRIO chassis according to the system requirements. Based on the specific case, the corresponding template is downloaded from SVN, opened and then appropriately configured (number of interlock functions, thresholds, default values, communication with CIS, etc.). Once configured, templates have to be compiled, to generate a bitfile. The bitfile is then downloaded to the FPGAs, and the system is ready to be tested with the TPS. Finally, if the system under test meets all the requirements, it is connected to the sensors and actuators of the final system.

This methodology allows deploying the different F-PIS in a secure and controlled way, providing extensively tested systems and reusing the hardware description of previous F-PIS.

This methodology is valid only for direct application to the different interlock systems that fit the requirements of the templates developed (regarding number of available interlock functions, type of input and output signals, etc.). However, the modular design of the developed architecture allows implementing other cases with minimum changes in the hardware description logic. Next section describes the details of a particular case for the Poloidal Field and Central Solenoids' Power Converter protection system, which does not fit the requirements of the generic templates but reuses logic blocks created on the template generation phase.

3. Use case. Poloidal Field and Central Solenoids' Power Converter protection system

This special case belongs to the Poloidal Field and Central Solenoids' Power Converter protection interlock. The central solenoid and poloidal field super-conducting coils hold up around 40 GJ of energy at very low temperatures. In the case of a loss of the superconducting condition, detected by the magnet system, the power supplies in combination with a bank of resistors, the Fast Discharge Units, are requested to remove the current from the coils before energy can destroy the coils [6]. The fast discharge required to remove the energy from the coils in case of loss of the superconducting conditions is coordinated by a hardwired loop, the discharge loop, which ensures that the action is propagated to the required plant systems via an interface box, the DLIB. The connection of the DLIB to the power supply is a critical function with strict constraints in terms of integrity and time performance. As a result, the F-PIS solution is an excellent candidate to achieve the required functionality. To achieve this, the PF and CS power converters are connected to the F-PIS as shown in Fig. 3.

On one side, Coil's sensors are connected to DLIB systems, which conform a hardwired loop [2]. The signals from the DLIB (via 24 V interface) are used as inputs (6 IF, each for a PF segment and 5 IF for the CS) of the F-PIS, these are wired on the FPGA to the power converters (via 5 V TTL interface) to shut them down if triggered.

On the other side, power converters' health status signals (5 V TTL) are used as inputs (7 IF) for the F-PIS and wired as outputs to the BLIB (via 24 V interface) to trigger the discharge of the magnets in case of

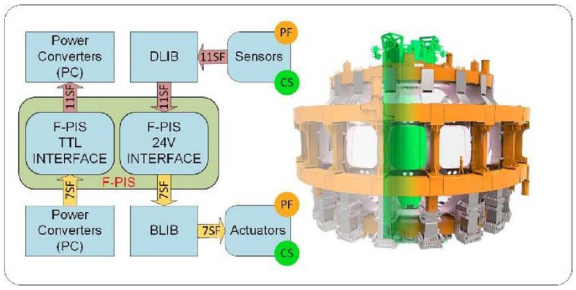

Fig. 3. PIS interfaces with other systems and their relation to Poloidal Field Coils (orange) and Central Solenoid (Green). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)