AN OVERVIEW OF THE ITER INTERLOCK AND SAFETY SYSTEMS

Luigi Scibile, Jean-Yves Journeaux, Wolf-Dieter Klotz, Izuru Yonekawa, Anders Wallander,
ITER Organization, Saint-Paul-lez-Durance, France

Abstract

Many systems that make up the ITER machine have to respect stringent requirements in terms of reliability, availability, safety and maintainability either for the protection of people, the environment or the safe operation of the machine. International standards have been selected to manage the lifecycle of the different types of systems, to harmonize the work that is carried out in the countries of the seven ITER partners and to satisfy the French safety regulations. These systems often embed the basic means for local self protection. For example, a system will not exceed its own safe level regardless of what external demand signal it receives. However, there are additional levels of protection required for those combinations of systems' conditions that are dangerous, even though each system may be within its own safe limits. These additional levels of protections are provided by the Central Interlock System and the Central Safety System. The Central Interlock System deals with the safe operation of the machine (protections of the investment) while the Central Safety System deals with the protection of the people and the environment. This paper gives an overview of the Interlock and Safety Systems based on the current requirements, the survey of the protection systems and the application of international standards.

INTRODUCTION

The main objective of ITER is to demonstrate the scientific and technical feasibility of a controlled fusion reaction. To reach its goal, ITER will operate using deuterium (D) and tritium (T) as fuel. The fusion reactions will produce neutrons that will activate part of the ITER structures. The tritium and the activated material are radioactive, hence the classification of ITER as Basic Nuclear Installation (Installation Nucléaire de Base, INB) based on the French Laws [1].

Independently of its classification as an INB, the operation of a complex experimental machine like ITER involves a number of potential identified hazards to personnel, the environment, and to the machine itself.

For the personnel and environmental safety, the main hazards have been reported initially in the ITER Generic Site Safety Report (GSSR) [2] and further developed in the Preliminary Safety Report (Rapport Préliminaire de Sûreté, RPrS) [3] submitted to the French authorities for the licensing process. For the control of the main identified hazards, two fundamental safety functions have been identified (RPrS): the confinement of the radioactive material and the limitation of internal and external exposure to ionizing radiations. The most important contributions to these functions are implicit in the features of a Tokamak, in the inherent difficulty of getting a burning plasma, in limiting by design hazardous situations and by the application of a radiation protection approach. Nonetheless, safety systems are required to guarantee the confinement within confinement barriers, associated confinement systems and the protection of these confinement barriers, to limit the exposure during normal operation with shielding, ventilation and detritiation systems and radiological monitoring and to limit the radiological impact in the case of an incident/accident with contamination monitoring.

For the protection of the machine, the main hazards have been identified in the design of the various sub-systems and a detailed requirement analysis is currently under development. The main identified hazards are in three main fields: the stored energies, the operation of the large industrial systems and the operation of the plasma.

While most of the protection systems are either passive or purely mechanically activated, some are operated by protection control systems. At ITER, the control systems dedicated to the protection are structured in two groups: the safety control systems, dedicated to the protection of people and the environment, and the interlock control systems dedicated to the protection of the machine. These systems represents two of the three independent tiers on which the ITER Instrumentation and Control is based [4]. An overview of these systems is given in Section 2.

OVERVIEW OF THE ITER PROTECTION CONTROL SYSTEMS

ITER is composed by a number of complex plant systems. The coordinated operation of all ITER is done via automated Instrumentation and Control (I&C) systems. This is structured in two layers (Central I&C systems layer and Plant System I&C layer) and three clearly separated tiers (Control, Interlock and Safety) [5], [6]. This concept is illustrated in Fig. 1. The ITER Protection Control Systems represent two of these three tiers.

At the plant system layer, the plant systems I&C provide the functionalities required for its own safe operation. This includes: the plant control system for the control of all the required processes including the means to limit the evolution of the processes towards dangerous situations (for example limit and range control, exception management and controlled shutdowns), the Plant Interlock System (PIS) for the local implementation of the protection of investment functions that are required to complement and to support the plant control system and the Plant Safety System (PSS) for the local implementation of safety functions.

At the central system layer, CODAC system as a central conventional control system of ITER I&C system provides the Control, Data Access and Communication functions for ITER, allowing integrated operation. The

Central Interlock System (CIS) provides protection of investment by handling multiple PIS to avoid uncoordinated operation that could potentially damage the facility and providing additional levels of protection and interlock required for dangerous combinations of Plant Systems conditions. The Central Safety Systems (CSS) coordinates the individual protection provided by the intervention of locally distributed PSS by the activation of additional protections in order to remove or reduce the detected hazardous conditions.

The CSS and PSSs form the ITER Safety Control Systems. They have been structured according to their functional allocation and classification in: nuclear safety, non-nuclear safety (conventional safety) and personnel access. They have the highest level of reliability and availability, provided by redundancy and proof of functionality, appropriate to the ITER safety case. They use dedicated signals, which are segregated from corresponding measurements in the conventional control system. The CIS and PISs form the ITER Interlock Control Systems. They have been structured according to their required performances in terms of Safety Integrity Levels (SIL) allocation. Depending on the SIL level, they use multi-redundant signals, which are dedicated and segregated from corresponding measurements in the conventional control system in some cases.

The conceptual architecture of the overall ITER I&C system as described above is illustrated in Fig 1.

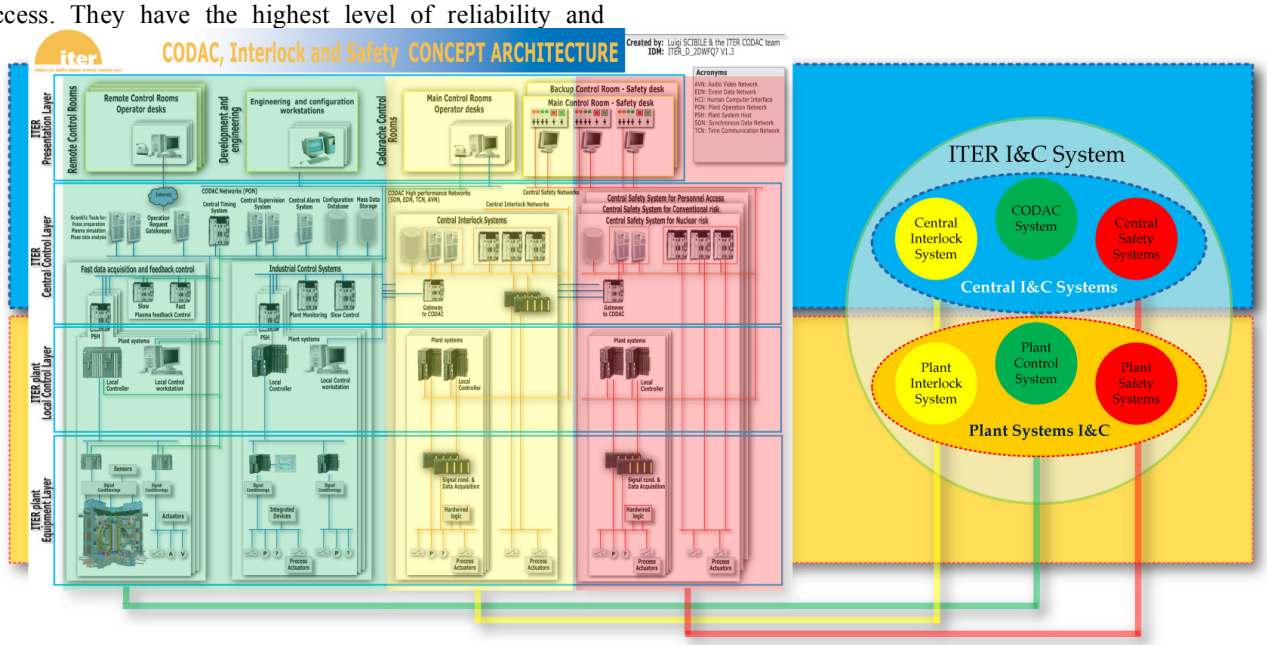

Figure 1: ITER I&C concept architecture.

Application of International Standards

For the development of the Interlock and Safety control systems, it has been decided to use, as much as possible, international standards. The decision has been based on many factors ranging from the international nature and the procurement model of the project, the attempt to minimize diversity in the development approach and the unify the communication in terms of common objectives to the compliance to the national regulations that are enforced in France where ITER is located.

From the regulatory point of view, ITER is classified as Basic Nuclear Installation (Installation Nucléaire de Base, INB) based on the French Laws [1]. On these bases, the work carried out on systems that are part of the licensing are subject to the French regulations. These are based on a non-prescriptive approach regulated by a French Law [1].

The approach states that the application of national and/or international standards is neither necessary nor sufficient for the licensing. However, the use of standards is recommended for all the project phases.

From the organizational point of view, ITER will have to work with a very large community. This has directed our choice towards standards of ample use, both in industry and in scientific laboratories, and that can address the largest percentage of systems.

On these bases, the IEC 61508 [10] family of standards has been selected. While for the interlock control systems, the IEC 61508 has been considered sufficient for all analysed cases, for the safety control systems, the IEC 61513 [8] has been selected. This standard is derived from the IEC 61508 and it is applicable to the Instrumentation and control of systems important to safety in nuclear power plants. Even if derived from the IEC 61508, the IEC 61513 has quite some fundamental differences since it is based on deterministic criteria and engineering judgement about consequences in case of malfunction rather than the probabilistic approach of the IEC 61508. However, the IEC 61513 is not sufficient on its own. To complete the set of standards for the nuclear sector, the following is required: the IEC 61226 [9] for the analysis and the classifications of the safety functions,

the IEC 61880 for the realisation of the software for the category A functions and the IEC 62138 for the realisation of the category B/C. A synthetic overview of these standards and their correspondence is given in Fig. 2.

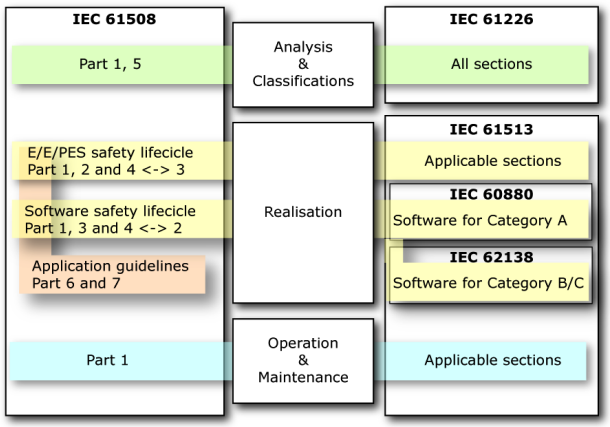

Figure 2: IEC61508 compared to IEC 61513.

Functional Requirements

The main functional requirements for the protection control systems derive directly from the General Safety Objectives, the preliminary safety report and the site analysis report [2], [3]. These are grouped in two main categories: protection functions and monitoring functions. Recently, a functional analysis has been carried out to map the functional requirements to actual plant systems and to identify and formalize the interfaces between the central systems and the plant systems. This functional analysis has been structured in a database that collects the risks with their characteristics and, for each risk, the prevention and/or protection functions with their definition, allocation (local to a plant system or distributed) and classification in terms of category (IEC61226) or SIL (IEC 61508). The functional analysis is completed for the nuclear risks and some work has still to be performed for the remaining risks [11].

The functional requirements have been distributed so that: the plant systems are in charge of providing local protective measures if the safe limits are exceeded using on their own sensors and actuators; the central systems are in charge of the protections that involve two or more plant systems, they generate commands to each plant system to reach a safe state if a combination of safety limits is exceeded and they are also in charge of the post accident monitoring, acquisition of additional parameters to those available to the computers generating the automatic actions, send status information to CODAC. The human machine interface for the interlock protection systems is managed via CODAC while the safety control systems have dedicated operator's safety desks.

Main Design Requirements and Architectures

The main design requirements for interlock and safety control systems have been directly derived from the selected standards in accordance with the result of the classification. These include, in some cases, redundancies of sensors (2oo3) and actuator chain. These requirements have been extended to all plant systems via publication of the ITER Plant Control Design Handbook [12].

The requirements also include prescriptions for standardized equipment and architectures types adapted to the level of classification and performance (Volume of data, response time, type of operation and geographical location) in order to minimize the design effort, to limit the safety assessments and to optimize the future maintenance costs.

CONCLUSIONS AND FUTURE WORK

This paper has presented the current status and an overview of the ITER interlock and safety systems. The main results have been in organizing the interlock and safety control systems in a manageable structure via the correct distribution of the work between the various plant systems based on a functional allocation of the safety requirements. The main priority for the future work is the completion and validation of a comprehensive conceptual design.

REFERENCES

[1] C. Alejandre et al., ITER on the Way to Become the First Fusion Nuclear Installation, 22nd IAEA Fusion Energy Conference, 2008, Geneva, Switzerland.
[2] Generic Site Safety Report - Volume1 - Safety Approach ITER_D_ ITER_D_2298PR v2.0.
[3] Preliminary Safety Report, (Rapport Préliminaire de Sûreté, RPrS), ITER_D_2E74AS v1.0.
[4] Wallander et al., ITER Instrumentation and Control – Status and Plans, 7th IAEA Technical Meeting, Aix-en-Provence, France, June 2009.
[5] J.B. Lister, J.W. Farthing, M. Greenwald and I. Yonekawa "Status of the ITER CODAC conceptual Design", ICALEPCS, Knoxville, USA, 2007.
[6] J.B. Lister, J.W. Farthing, M. Greenwald and I. Yonekawa, "The ITER CODAC Conceptual Design", Fusion Engineering and Design 82 (2007) 1167-1173.
[7] IAEA Safety Guides No. NS-G-1.3:2006, I&C Systems Important to Safety in Nuclear Power Plants.
[8] IEC 61513: 2001, NPP – I&C for systems important to safety -General requirements for systems.
[9] [IEC 61226:2005, NPP – I&C systems important for safety – Classification.
[10] IEC 61508:1998, Functional safety of E/E/PES safety related systems - All Parts.
[11] L. Scibile et al., The ITER Safety Control Systems – Status and Plans, Technical Meeting, Aix-en-Provence, France, June 2009.
[12] ITER CODAC Team, "Plant Control Design Handbook", ITER_D_27LH2V v4.1.