Fusion Engineering and Design 85 (2010) 540–544

Contents lists available at ScienceDirect

Fusion Engineering and Design

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

The ITER safety control systems—Status and plans

Luigi Scibile*, Jean-Yves Journeaux, Wolf-Dieter Klotz, Izuru Yonekawa, Anders Wallander

ITER Organization, CS 90 046, 13067 Saint-Paul-lez-Durance, France

ARTICLE INFO

Article history:
Available online 10 May 2010

Keywords:
ITER
Safety control system
Instrumentation and Control
I&C system
Plant system I&C

ABSTRACT

The operation of a complex experimental machine like ITER will involve a number of potential hazards to personnel, the environment, and to the machine itself. While some protections are usually embedded within the overall control system, when it comes to the protection of people, the environment or the safe operation of the machine, dedicated systems are required. At ITER, the safety control systems are dedicated to the protection of people and the environment. These systems represents one of the three independent tiers on which the ITER Instrumentation and Control is based. They have to respect stringent requirements in terms of reliability, availability, safety and maintainability for operation, security and national and/or international safety regulations. This paper describes the current status and plans of the safety control systems, the functions to be performed, the envisaged architecture and the main design options including the principles of separation and independence between the three tiers.

1. 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: the main hazards being linked to radiations. These 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. In these documents, the fundamental safety objectives and the principles to attain them are also defined. The safety principles are: the defense-in-depth and the radiation protection, as per the principle of optimization and the ALARA approach (As Low As Reasonably Achievable).

For the control of the main identified hazards, two fundamental safety functions have been identified [3]: the confinement of the radioactive material and the limitation of internal and external exposure to ionizing radiations.

The most important contributions (that basically limit the effect) 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 (like limiting the inventories of tritium) and by the application of a radiation protection approach. Nonetheless, safety systems are required:

- To guarantee the confinement with 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.
- To limit the radiological impact in the case of an incident/accident with contamination monitoring.

While most of the safety systems are either passive or purely mechanically activated, some are operated by a safety control system. At ITER, the safety control systems are dedicated to the protection of people and the environment. These systems represents one of the three independent tiers on which the ITER Instrumentation and Control is based [4].

This paper is structured as follows: Section 2 provides an overview of the context of the safety control systems in ITER, Section 3 describes the main functional requirements, in Section 4, the main design requirements and the principle of tiers separation is presented and Section 5 addresses the plans and future works.

2. Context of the safety control systems in ITER

The context of the safety control systems in ITER can be viewed from two main perspectives:

* Corresponding author. Tel.: +33 442 17 64 09.
E-mail address: Luigi.Scibile@iter.org (L. Scibile).

0920-3796/$ – see front matter © 2010 ITER Organization. Published by Elsevier B.V. All rights reserved.
doi:10.1016/j.fusengdes.2010.03.028

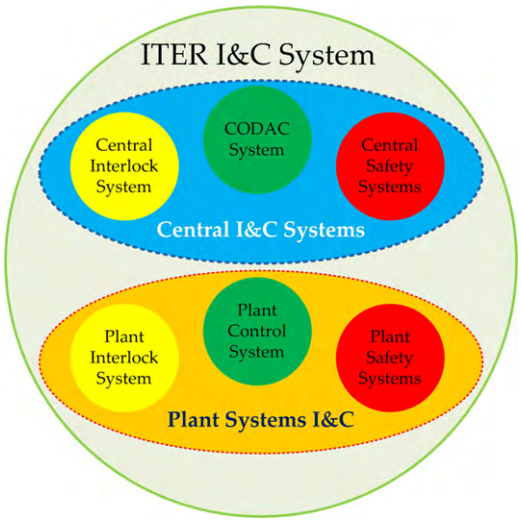

Fig. 1. ITER I&C system concept.

- The regulatory context.
- The procurement structure and the proposed technical organization.

ITER is classified as Basic Nuclear Installation 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 based on a continuous dialogue during the various project phases and analyzing greater and greater details reflecting the progress in the definition and the construction of the project. This approach is regulated by a French Law [1].

This approach implies 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. A set of applicable standards has been selected and included in [3] and the plant control design handbook [5] and the most important one are included in the reference [6–8].

For the technical organization, ITER has been broken down in different logical and functional parts usually referred to as plant systems (i.e. cryoplant, vacuum systems, power supplies, and tritium plant). These different parts constitute the ITER Plant Breakdown Structure.

Some of these plant systems participate in the realization of the safety functions and, for that reason, they are designed to guarantee that the General Safety Objectives are attained. Requirements for these plant systems have been derived from the Accident Analysis Report [9].

In general, operation of complex plants is done via automated Instrumentation and Control (I&C) systems. In ITER, 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) [10,11]. This concept is illustrated in Fig. 1.

At the plant system layer, the plant systems I&C provides the functionalities required for the safe operation of the specific plant system. This includes: the plant control system for the control of all the required processes, the Plant Interlock System (PIS) for the local implementation of the protection of investment functions 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 *C*ontrol, *D*ata *A*ccess and *C*ommunication functions for ITER, allowing integrated operation. This includes: continuously monitoring the plant systems status, displaying their status to operators including alarms, preparing and automating scheduled operations (including plasma pulses), retrieving data from plant system I&C, storing and making all the data available. CODAC uses multiple logical and physical networks to segregate these disparate functions. 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 those combinations of plant systems conditions that are dangerous, even though each plant system may be within its own safe limits. The Central Safety Systems (CSS) coordinates the individual protection provided by the intervention of locally distributed safety control systems (PSS) by the activation of additional protections in order to remove or reduce the detected hazardous conditions. The conceptual architecture of ITER I&C system is illustrated in Fig. 2.

The CSS and PSSs form the ITER safety control systems. They have been structured according to their functional allocation 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. Safety control systems use dedicated signals, which are segregated from corresponding measurements in the conventional control system. This paper focuses on the nuclear safety aspects, as they are the most constraining one. In this respect, for clarity the notations CSS-N and PSS-N will refer to the safety control system for nuclear risks.

The ITER procurement model is such that the participating parties procure most of the plant systems as a form of “in-kind” contribution to the project. The remaining parts are directly procured by the ITER organization with its own funds: this type of procurement is referred to as “in-fund”.

The structuring of the ITER Instrumentation and Control in two layer also reflects the ITER procurement model since the central I&C system layer is procured “in-fund” and most of the plant systems I&C is procured “in-kind”.

3. Main functional requirements

The main functional requirements for the safety control systems derive directly from the General Safety Objectives, the Preliminary Safety Report and the Accident Analysis Report [2,3,9]. These are grouped in two main categories: protection functions and monitoring functions. These have been recorded in the baseline documentation in the corresponding system requirement documents. These requirements have also been reported in [3] and have been analyzed in previous work [12,13].

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 various PSS-N and the CSS-N. This functional analysis has been structured in a database that collects:

- The risks with their characteristics including the risk category (nuclear, conventional, access) and the risk class (I–IV).
- 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 class (IEC61226 [8]) or SIL (IEC 61508 [14]).
- For each function, the implementation details in terms of sensors, logic and actuators and their allocation in the corresponding PBSs.

The functional analysis is completed for the nuclear risks but some work has to be performed for the remaining risks.

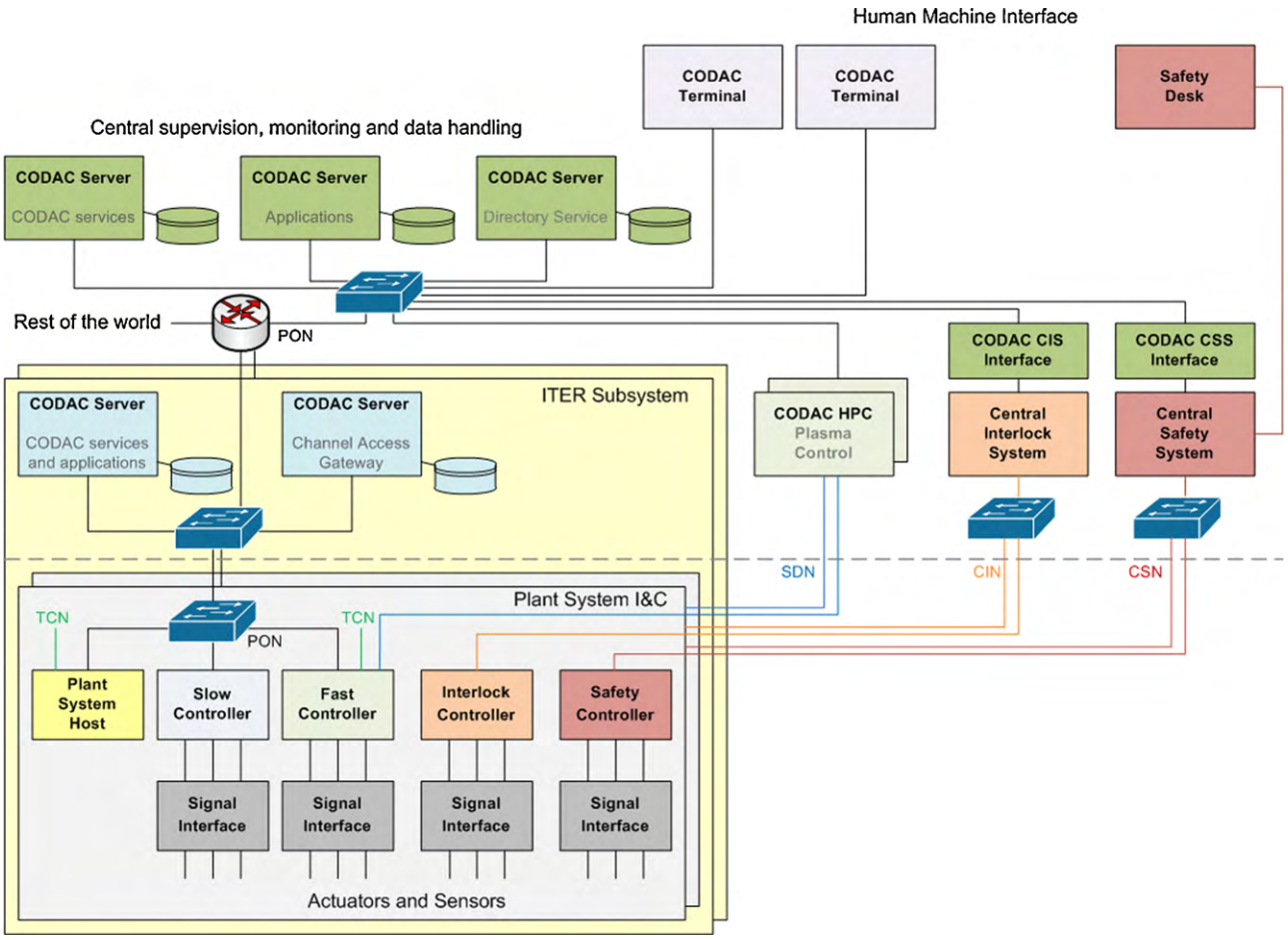

Fig. 2. ITER I&C concept architecture.

The distribution of the functional requirements between the CSS-N and the PSS-N can be summarized as follows.

The PSS-N are in charge of providing safety measures if the safety Operation Limit Conditions (OLC) [9] are exceeded using on their own sensors and actuators.

The main functions that fall under this category are:

- Restoring pressure in the Tokamak Cooling Water System vault.
- Limit coolant spill.
- Limiting Vacuum Vessel overpressure.
- Control of the detritiation and ventilation systems of the Tokamak and Tritium Plant modules.
- Control of the detritiation and ventilation systems of the Hot Cell/Low-Level Radwaste.
- Starting diesel generators and connecting them to emergency buses.

In order to manage its safety measures, each PSS-N manages its own sensors corresponding to the safety OLC. The CSS-N is not directly involved in these specific safety measures.

The Central Safety System is in charge of the safety measures that involve two or more Plant Safety Systems. It generates commands to each Plant System to reach a safe state if the safety Operation Limit Conditions (OLC) are exceeded.

The main functions that fall under this category are:

- Primary and secondary confinement systems in the Tokamak building,
- Primary and secondary confinement systems in the Tritium plant building,
- Primary and secondary confinement systems in the Hot Cell/Low-Level Radwaste building,
- Fusion power termination system,
- TF magnets fast discharge and stopping power to the PF coils.

The Central Safety System is 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 and send parameter values to CIS to cope with impossible sensors duplication. This includes the operator's safety desks: the main operator's safety desk and the backup operator's safety desk.

4. Main design requirements and the principle of tiers separation

The top level principles for the design of the safety control systems are based on the fundamental safety objectives defined in the GSSR [2], in the RPrS [3] and on the recommendations and requirements from selected standards for nuclear installations [6–8]. The most important are:

- Defense-in-depth principles and separation
- Redundancy and single failure criteria
- Avoidance of hazards
- Priority among the three tiers

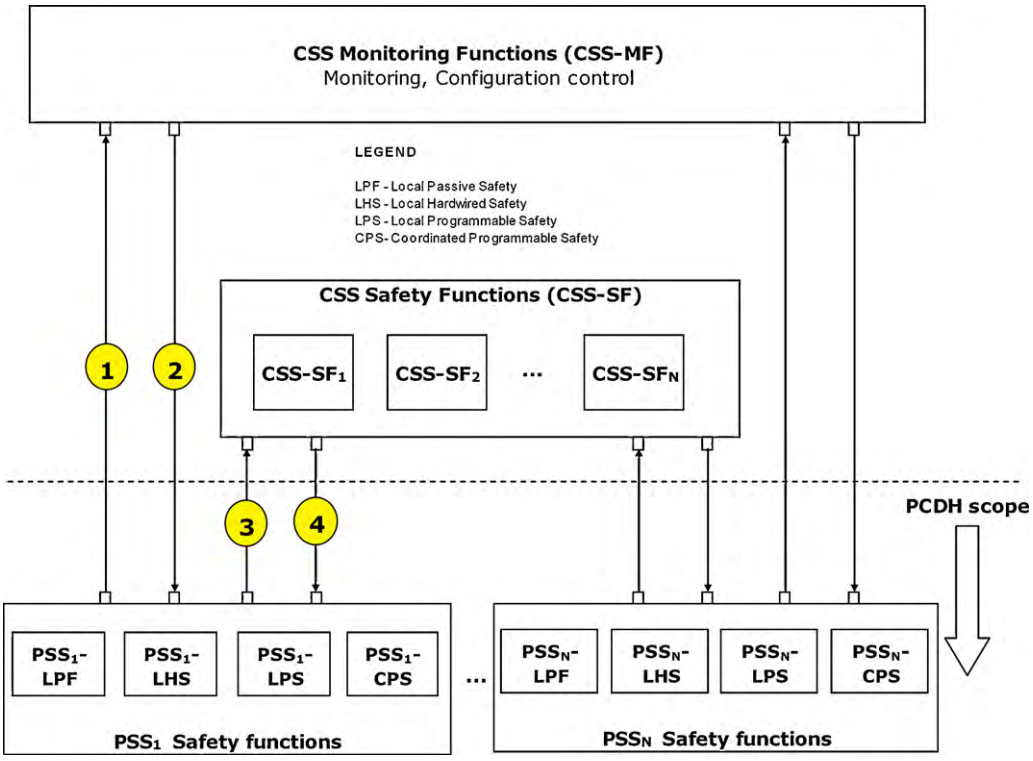

Fig. 3. Standard safety I&C conceptual architectures.

For the defense-in-depth principles and separation, the main implication for ITER I&C systems is a clear separation in three tiers and layers, such that:

- The control tier prevents departures from a set of nominal OLC.
- The interlock tier detects greater deviations from normal operation and takes actions to prevent the excursion from escalating into accident conditions,
- The safety tier takes actions to recover from any accident, returning the facility to a safe state. These systems are the only safety control systems of the I&C.

To remove common mode failures between the control/interlock tiers and the safety tier, it is required the use of diversified industrial products for computers.

For redundancy and single failure criteria, the safety control systems will be designed with sufficient redundancy to ensure that they can perform their intended safety functions in the case of any single failure caused by any of the design basis events.

The design requirements incorporate redundancies as follows:

- Three channels for detection and initiation of automatic safety functions. Initiation will be performed by means of 2003 logic that will ensure system reliability (avoiding failure on demand) without impairing the experiment availability (avoiding spurious trips),
- Two independent trains for actuator commands.

Independence among redundant channels and trains and between these and control and interlock tiers components are ensured by:

- Physical segregation with redundant equipment located in different hazard areas to ensure that an internal or external event such as fire or flood does not cause the unavailability of more than one redundancy.
- Electrical separation avoiding that an electrical failure in one channel or train is propagated to the redundant channels or trains.
- Functional separation so that the safety control system is totally independent of control and the interlock tiers, receiving no input from them.
- Diversified industrial components for Safety Computers compared with the Interlock computers. Remark: the electrical power supply shall have independent or isolated channels to feed the three channels of CSS-N.

For the avoidance of hazards, physical segregation of redundant trains or channels is required to increase the system avoidance of internal and external hazards. The safety control system design requirements are to withstand the environmental conditions and seismic loads of their location (operational and accidental conditions) without loss of functionality.

For the priority among the three tiers, when actuators have commands coming from different tiers of the control systems, the design requirement is that the PSS will manage the priority among those different commands from highest level to lowest level: the highest priority being that of the automatic safety actions.

The main design requirements for the safety control systems have been defined in the in the Plant Control Design Handbook V4.1 [5].

To ease the functional allocation of the requirements, the Plant Safety Systems have been structured in a set of standard conceptual architectures as shown in Fig. 3:

- Local Passive Safety (LPF)
- Local Hardwired Safety (LHS)

- Local Programmable Safety (LPS)
- Coordinated Programmable Safety (CPS)

These correspond to the potential physical architecture to be designed. The requirements impose a classification based on the risk to cover as described in the IEC 61226 [8] and the implementation is then regulated by the application of the standard IEC 61513 [7] for the corresponding systems' categories.

For the design of the operator's safety desks, the following main requirements apply:

- The priority principles between automatic signals and manually initiated control signals;
- The priority principles between the different HMI systems during normal, accident, and post-accident operation;
- Human factor techniques based on IEC 60964 and IEC 60965 shall be used for ensuring the effectiveness of the safety desk in the design of the main control room and the backup control room.

The design of the safety control systems is at the conceptual design stage and its advancement varies between systems.

5. Plans and future work

The current plans foresee three lines of work: R&D, engineering activities and procurements.

The R&D activities include HW and SW prototypes, the analysis of scenarios where the intervention of the safety control systems is expected, the development of tools for the project lifecycle (like the rapid prototyping techniques [15]), the evaluation of the existing technologies and their applicability to the ITER context, as described in Section 1.

For the engineering activities, engineering service contracts are used to reinforce the ITER organization resources. Two contracts are currently running and an additional one is planned to start this year.

As described in Section 2, the CSS is procured "in-fund" including the prototypes and the final systems. For the procurement activities, the current plan is to start by early 2010 to procure the proof-of-concept prototypes to be used for the preparation of the procurement of the complete systems that will take place during the 2011–2015 with initial installation as early as 2013.

6. Conclusions

After a long pause after the conclusion of the design review in 2001, the work on the safety control systems has re-started. In particular, the initial work consisted in assessing the current situation with respect to the French regulations, the organization and distribution of the work between the various plant systems for the implementation of the safety functions and the impact of the ITER design changes on the safety control systems. The main priority for the future work is the completion and validation of a comprehensive conceptual design for the safety control systems.

References

[1] C. Alejandre, L. Rodriguez-Rodrigo, N. Taylor, J. Elbez-Uzan, D. Acker, D. Baker, et al., ITER on the way to become the first fusion nuclear installation, in: 22nd IAEA Fusion Energy Conference, Geneva, Switzerland, October, 2008.
[2] Generic Site Safety Report – vol. 1 – Safety Approach ITER_D_ITER_D_2298PR v2.0, 2005.
[3] Preliminary Safety Report (Rapport Préliminaire de Sûreté, RPrS), ITER_D_2E74AS v1.0, 2008.
[4] A. Wallander, L. Abadie, H. Dave, F. Di Maio, H.K. Gulat, C. Hansalia, et al., ITER instrumentation and control—status and plans, in: 7th IAEA Technical Meeting on Control, Data Acquisition, and Remote Participation for Fusion Research, Aix-en-Provence, France, June, 2009.
[5] ITER CODAC Team, Plant Control Design Handbook, ITER_D_27LH2V v4.1, 2009.
[6] IAEA Safety Guides No. NS-G-1.3:2006, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, 2006.
[7] IEC 61513:2001, Nuclear power plants – instrumentation and control for systems important to safety – general requirements for systems, 2001.
[8] IEC 61226:2005, Nuclear power plants – instrumentation and control systems important for safety – classification, 2005.
[9] N. Taylor, Accident Analysis Report (AAR), vol. I—Event Identification and Selection, ITER_D_2DPVGT, 2009.
[10] J.B. Lister, J.W. Farthing, M. Greenwald, I. Yonekawa, Status of the ITER CODAC conceptual design, in: ICALEPCS, Knoxville, TN, USA, October, 2007.
[11] J.B. Lister, J.W. Farthing, M. Greenwald, I. Yonekawa, The ITER CODAC conceptual design, Fusion Engineering and Design 82 (2007) 1167–1173.
[12] Areva, Monitoring and Control Human Factors—RPrS Support Study, Technical Report 095-063-E-I-00001, Areva, 2007.
[13] L. Topilski, Safety Analysis Data List, Technical Report ITER_D_24LSAE, ITER-IO, 2008.
[14] IEC 61508:1998, Functional safety of electrical/electronic/programmable electronic safety related systems—all parts, 1998.
[15] L. Scibile, G. Ambrosino, G. De Tommasi, A. Pironti, Rapid prototyping of the central safety system for nuclear risk in ITER, in: 7th IAEA Technical Meeting on Control, Data Acquisition, and Remote Participation for Fusion Research, Aix-en-Provence, France, June, 2009.