Available online at www.sciencedirect.com
ScienceDirect
Fusion Engineering and Design 82 (2007) 1167–1173
Fusion Engineering and Design
www.elsevier.com/locate/fusengdes

The ITER CODAC conceptual design

J.B. Lister [a,*], J.W. Farthing [b], M. Greenwald [c], I. Yonekawa [d]

[a] *ITER IT JWS, Cadarache, France*
[b] *EURATOM/UKAEA Fusion Association, Culham Science Centre, Oxon, UK*
[c] *Plasma Science and Fusion Center, MIT, MA, USA*
[d] *JAEA-Naka, Ibaraki, Japan*

Available online 6 March 2007

Abstract

CODAC orchestrates the activity of 60–90 Plant Systems in normal ITER operation. Interlock Systems protect ITER from potentially damaging operating off-normal conditions. Safety Systems protect the personnel and the environment and will be subject to licensing. The principal challenges to be met in the design and implementation of CODAC include: complexity, reliability, transparent access respecting security, a high experiment data rate and data volume since ITER is an experimental reactor, scientific exploitation from multiple Participant Team Experiment Sites and the long 35-year period for construction and operation.

Complexity is addressed by prescribing the communication interfaces to the Plant Systems and prescribing the technical implementation within the Plant Systems. Plant Systems export to CODAC all the information on their construction and operation as "self-description". Complexity is also addressed by automating the operation of ITER and of the plasma, using a structured data description of "Operation Schedules" which encompass all non-manual control, including Plasma Control.

Reliability is addressed by maximising code reuse and maximising the use of existing products thereby minimising in-house development. The design is hierarchical and modular in both hardware and software. The latter facilitates evolution of methods during the project lifetime.

Guaranteeing security while maximising access is addressed by flow separation. Out-flowing data, including experimental signals and the status of ITER plant is risk-free. In-flowing commands and data originate from Experiment Sites. The Cadarache Experiment Site is equated with the Remote Experiment Sites and a rigorous "Operation Request Gatekeeper" is provided.

The high data rates and data volumes are handled with high performance networks. Global Area Networks allow Participant Teams to access all CODAC data and applications.

Scientific exploitation of ITER will remain a human as well as technical challenge, to find methods of effectively combining the experience and observations of a geographically distributed research team.

Keywords: ITER; Control; Data Acquisition; Communication

* Corresponding author. Permanent address: CRPP-EPFL, Association EURATOM-Confédération Suisse, CH-1015 Lausanne, Switzerland. Tel.: +41 21 693 3487.
E-mail address: Jo.Lister@epfl.ch (J.B. Lister).

0920-3796/$ – see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.fusengdes.2007.01.013

1. Introduction

ITER [1] operation requires the orchestration of 60–90 Plant Systems, procured "in kind" from the Participant Teams, including all the technical systems as well as the plasma diagnostic systems. The orchestration is guaranteed by three clearly separated tiers: CODAC, Central Interlock Systems (CIS) and Central Safety Systems (CSS), indicated in Fig. 1 by their three respective networks.

CODAC provides the COntrol, Data Access and Communication functions for ITER, allowing integrated operation. This includes: continuously monitoring the Plant Systems; displaying their status to operators including alarms; preparing and automating scheduled operations (including plasma pulses); recovering data from Plant Systems; storing and making all the experimental data available. CODAC uses multiple logical and physical networks separating the specific requirements of each.

Interlock Systems provide protection of investment for ITER. Each Plant System may have a Plant Interlock System. The Central Interlock System handles multiple Plant Systems, where their uncoordinated operation is potentially damaging. The signal sources, networks and logic will have a higher degree of reliability and availability than CODAC.

Safety Systems provide protection of personnel and the environment during ITER operation. Safety Systems can shut down plasma operation and can inhibit access to potentially dangerous areas. Safety Systems are both local in the Plant Systems and coordinated by a Central Safety System. They have the highest level of reliability and availability, provided by redundancy and proof of functionality, appropriate to the ITER safety case. Safety Systems use very few signals, separated from CODAC. Safety Systems are subject to licensing and must be demonstrably safe.

Separating the surveillance and operation of ITER into three tiers is a major design feature, since CODAC is inevitably unprovable, due to its complexity. All instrumentation and control must clearly fall into one or other of these categories and comply with appropriate standards.

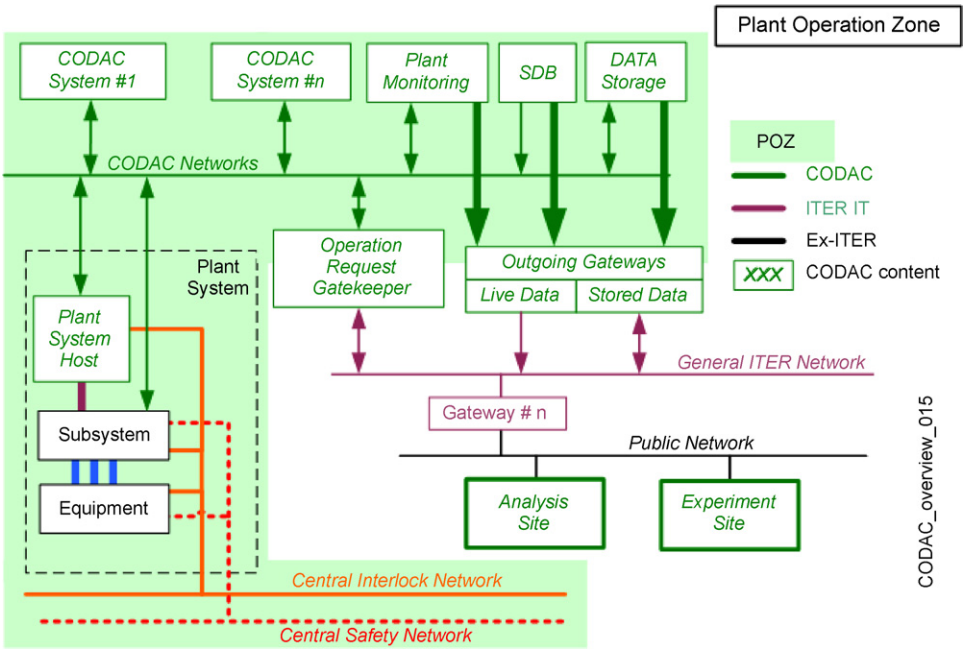

Fig. 1. Outline of the ITER control tiers: CODAC, Interlock Systems and Safety Systems. The Plant Operation Zone is shown with a shaded background, with the Operation Request Gatekeeper for incoming requests. CODAC components are shown in green italics. The network links to Experiment Sites are also shown. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of the article.)

The three tiers are inter-related by a set of Operating Limits and Conditions (OLC). Some OLC correspond to the Safety requirements. Others protect investment. Others restrict normal operation within the limits. One aim of CODAC is to use all the OLC to avoid triggering the Interlock Systems and in turn, it is the aim of the Interlock Systems to avoid triggering the Safety Systems.

Plant Systems will be maintained by the ITER project after final acceptance. To reduce the number of technologies and methodologies supported by ITER, the Plant Systems are subject to standards and methods for each of these three tiers.

The present paper presents some of the more challenging aspects of the 2006 conceptual design of the ITER CODAC. This work is based on the previous preliminary design completed in 1998 to which the fusion community has password protected access [2]. The challenges which are particular to ITER were identified in two previous papers [3,4]. The great wealth of work which has led to the generation of the ITER CODAC requirements and conceptual design is best illustrated by contributions to the most recent IAEA TCM in Budapest [5]. It would be inappropriate to single out a small number of these.

2. Requirements

The principal functional requirements on the CODAC tier have been identified and the non-functional performance properties are being derived. The design features easing the implementation of CODAC and the integration of Plant Systems are outlined in Table 1.

Table 1
Major CODAC design features

Design decision	Driving reason
Use international standards wherever possible and practical	Simplicity and uniformity between partners
Accumulate a structured data description of all Plant Systems, including their construction, input/output list and dynamical behaviour. This "self-description" shall be part of each procurement package, using tools provided by CODAC	Complexity and uniformity to allow data-driven solutions and data-driven integration and to provide high quality uniform documentation for ease of operation and maintenance
Define a minimum set of acceptable hardware and software standards	Complexity and "in-kind" procurement, and to guarantee long-term maintenance
Restrict message protocols for Plant System communication	Uniformity
Provide tools and support for factory validation of Plant Systems	Procurement tracking and integration
Use of structured data in all aspects of CODAC	ITER lifetime, for evolution, maintenance, reducing code volume
Inhibit initiation of standard communication by Plant Systems with other Plant Systems	Simplicity and mastery of the communication bandwidth
Protect the Plant Operation Zone against inappropriate commands by an Operation Request Gatekeeper which approves any incoming request to a Plant System or CODAC System	A model for allowing remote experimentation while maintaining access integrity
Automate Plant Systems using standard Sequential Function Chart formalism, IEC 61131-3, using SCXML representation	Uniformity, clarity and data-driven use

3. Plant System features

Plant Systems are procured "in kind" with specific technical specifications to meet their design purpose and with CODAC specifications to allow their integration into centralised ITER operation. Plant Systems have differing degrees of complexity, ranging from a single subsystem controller to a hierarchy of subsystem controllers. Each Plant System has a single Plant System Host which:

- Marshals the data flow to and from the Plant System.
- Provides the self-description of the Plant System in the form of structured data.
- Provides non-structured textual or graphical documentation of the Plant System.
- Handles structured configuration data.
- Handles structured transition requests to the Plant System.

The Plant System Host is not responsible for the internal integrity of the operation of the Plant System.

This responsibility is in the Subsystem Controller(s), normally PLCs prescribed by CODAC.

Beneath the Subsystem level is the equipment level, interfaced by a prescribed set of fieldbuses. Equipment such as digitisers can communicate with the Plant System Host, or with the controllers, depending on design choices.

This architecture leaves freedom in the design of each Plant System, while presenting a generic image via the Plant System Host and restricting implementation to a set of ITER CODAC standards.

The Plant System Host is responsible for exporting information concerning the Plant System, Table 2, the subject of an accompanying paper at this conference [6]. This information is exchanged between CODAC and the Plant System at final acceptance and is stored in a CODAC database. The structured information from the Plant System Host is exported as data, validated against explicit schemas and naming conventions, using tools provided by CODAC. Exporting this Plant Self-Description (using the CODAC Markup Language being developed) is tested during construction and commissioning at the factory using a "mini-CODAC" emulator, ensuring problem-free on-site integration at the CODAC level.

Regardless of any control and monitoring functions provided by CODAC, the primary responsibility for assuring the integrity of the Plant System rests with the Plant System supplier rather than with CODAC. Plant Systems must not rely on a rapid (or indeed any) CODAC response to abnormal conditions.

4. The Plant Operation Zone

The operation of ITER takes place in a Plant Operation Zone (POZ), which is logically and physically separate from the Experiment Sites, to guarantee operational integrity. The Plant Operation Zone is shown as a shaded background in Fig. 1 and constitutes a major part of CODAC.

The major data-flow is outgoing experimental signals and plant status, presenting no security risk. These data are stored outside the POZ, to avoid any operational security problems when accessing the data from outside the POZ.

Actions and data entering from outside the POZ are examined by the Operation Request Gatekeeper. The Operation Request Gatekeeper interprets all incoming commands and data and decides whether they should be transmitted into the POZ. This decision is made on the basis of: the authenticated originator; the current location and role of the originator; the current operation mode of the equipment; the operation mode of ITER.

Table 2
Summary of major elements inside the Plant System self-description

Schema	Information
Signal list	Signals on wires, origins, drawing references, etc.
Input-output list	Signals exported by the Plant System Host, names, meanings, units, properties, etc.
Module list	Hardware modules, origins, types, conversions, limits, configuration data, jumpers, etc.
Software	Firmware in modules, software in the Subsystem controllers, software in the Plant System Host, etc.
Documentation	List and source of all documents, drawings, concerning the Plant System
Alarms and warnings	List of alarm conditions and their meanings
Common Operating States (COS)	List of COS and their transition commands and transition conditions, standard delays, alarm delays, using SCXML, etc.
Plant Operating States (POS)	List of POS and their transition commands and transition conditions, standard delays, alarm delays, using SCXML, etc.
Mimics	Structured data description of engineering mimics using a CODAC symbol library, mimics delivered by the supplier, etc.
Data handling	Data sampling frequencies, dependence on COS, upper and lower limits, etc.
Operating Limits and Conditions	Restrictions on operating this Plant System, independently of other Plant Systems, etc.
Contacts	Information for contacting sub-contractors for this equipment, etc.
Network use	Requirements for use of the Synchronous DataBus and the Event Distribution Network, connection to the Time Communication Network and to the General ITER Network, etc.
Data Streams	Description of the data streams produced by the Plant System Host, etc.
Operation Request Gatekeeper	Operations to be allowed on the Operation Request Gatekeeper, including access rights, etc.

The Plant Operator intervenes if the Operation Request is neither accepted nor rejected. This model allows rule-based automation for some requests and an "air gap" interception by the Plant Operators for other requests, and will evolve during ITER operation.

The exploitation of ITER will take place in Experiment Sites, one of which is in Cadarache and the others are Remote. The functionality of these sites is common, ensuring that Remote Experiment Sites can exploit ITER with the same efficiency, using the same interfaces and tools, as the Cadarache Experiment Site. All Experiment Sites only interact with the POZ via the Operation Request Gatekeeper, shown in Fig. 1.

Plant Systems can be operated under "local control", if authorised by the Plant Operators. The equipment then functions under front panel control, if provided by the Plant System supplier, for commissioning and testing. Local Control uses the Interlock and Safety Systems of the Plant System itself for protection. The Central Interlock and Safety Systems inhibit inappropriate commands. Local Control is not an obligatory feature of a Plant System. In some cases, cost can be significantly reduced by not providing Local Control, but using CODAC control for commissioning and testing. When the equipment is transferred back under "CODAC control", the local control room is outside the POZ and commands and data again pass the Operation Request Gatekeeper.

Plant Systems integrated into CODAC can never be operated under "direct communication" between any computer, inside or outside the POZ and the Plant System. This would present too high a security risk to CODAC. All Plant Systems must be designed so that all communication between a user and his equipment is established as Operation Requests, during the construction of the Plant System. There will be no means of establishing "on the fly" communication inside the POZ once the equipment is operational.

5. CODAC components

CODAC contains multiple components, introduced in bold on the following description.

The principal CODAC System is the **Supervisory Control System** (SCS). SCS dynamically allocates any required resources to an ITER operation Task. SCS respects the formal ITER **Global Operating States** to determine what operations are authorised. SCS manages a dynamically evolving set of concurrent activities, each of which is driven by an **Operation Schedule**. The Operation Schedule is prepared by **Schedule Preparation** and each Operation Schedule requires **Schedule Validation** before becoming executable. An Operation Schedule is executed by **Schedule Execution** once the resources are made available by SCS. There is a strong interface between scheduling and ITER operation planning. SCS has responsibility for respecting the Operation Limits and Conditions. Given the importance of protecting the ITER investment, CODAC functions closely linked to protection of investment are isolated in **Error Avoidance**, providing rule-based confirmation of all commands to actuators. This enhances their degree of QA and avoids pollution from evolving packages. Error Avoidance includes alarm display, prioritisation, automated responses and proposed manual responses.

The status of ITER is obtained from **Plant Monitoring**, which also generates a data stream for **Data Logging**. The maximum refresh frequency is 3 Hz, corresponding to a human reaction. The minimum rate is 0.1 Hz to ensure a continuous record and continuous functionality checking. Monitoring data are available in the Experiment Sites to enhance contact with operation. The functionality is typical of an industrial SCADA (Supervisory Control And Data Acquisition), providing displays on mimic diagrams, trending, warning and alarm handling, manual triggering of commands or changes to set-points. Generic **Operator Consoles** are provided in the Main Control Room as well as in other areas of the ITER plant.

Plasma Control is implemented as a specific Operation Schedule to maximise reuse of automation and plasma control tools. General feedback control, including Plasma Control, uses a **Synchronous DataBus** to communicate data converted to physics units, including an estimate of the error on each signal. Evaluation of plasma diagnostic information is local in the diagnostic Plant System if this is straightforward. Information is collected over the Synchronous DataBus for analysing data from multiple Plant Systems and finally transmitted over the Synchronous DataBus to the actuators. Plasma Control is formulated within the frame of general operation scheduling, allowing reuse of complex code and taking advantage of the relative slowness of ITER plasma control compared

with existing tokamaks. This includes **Rescheduling**, which allows an ITER pulse to follow a trajectory which is changed on the fly to maximise the use of the long ITER pulses, including on the fly revalidation. Present experiments limit rescheduling to soft stop termination, such as on JET, by which the Pulse Operator can request the plasma current to be brought down rapidly but safely due to some unexpected event or plasma state. Additional features for operation include **Time Communication** and **Event Distribution**.

The **Plant System Host** is responsible for marshalling all experimental data streams (signal data, undersampled signal data, plant monitoring data, configuration data, source code, some simple analysis, etc.), converting it to physics or engineering units and delivering it to the Data Logging. This in turn marshals the data from all the Plant System Hosts. Data Logging presents this data to **Data Storage**, which physically stores the data outside the POZ, archiving it and backing it up. An undersampled data stream is continuously available at all Experiment Sites and archived by CODAC as an additional data stream. **Data Access** provides access to all ITER data for all users on-site or at Remote Experiment Sites. Uniform access is provided to all data streams. Features provided by Data Access include management of the signal names, server-side evaluation of data, server-side undersampling of data, typically used on existing experiments.

Some features are considered as services. **Data Visualisation** groups the visualisation tools for plant monitoring, undersampled data monitoring, trending and scientific visualisation needed during operation and provides a homogeneous HMI environment. **General Reporting** allows Plant Systems and CODAC to report correct or incorrect functionality using a standard interface for recording, archiving and tracing reports, including error and performance reports. **Computing Support** provides guaranteed access to distributed computing power for ITER operation, as well as file servers to store CODAC Systems data and experimental data. **Message Service** provides an ITER-wide definition of inter-process and inter-processor communication middleware using standard ITER protocols. **Event Notification** allows signalling between processes in the distributed CODAC Network and off-site. **Database Tools** provide basic CODAC support and interface to a global ITER database.

Features are built in to assist integration. **Performance Testing** emulates CODAC with a "mini-CODAC" which can be used to verify the functionality and performance of a Plant System during factory testing and acceptance, and again during on-site acceptance. A **Plant Simulator** uses the self-description of the Plant Systems to build a simulator of the ITER plant. Combined with CODAC, this allows early testing of the integration of the Plant Systems into CODAC, and identifies potential problems well before on-site commissioning. **Operator Training** provides a fully realistic simulator of ITER using the Plant Simulator and a copy of all CODAC Systems. Replaying incidents allows operators to test new responses to problems. Operator Training also doubles up as a backup to the Main Control Room in case the latter becomes non-operational. Full functionality of ITER is not maintained in the Backup Control Room, but vital functions are guaranteed at the same level as the Main Control Room. **CODAC Development** provides a full replica of CODAC and its networks to develop and test CODAC Systems.

6. Summary

The CODAC conceptual design has focused on abstraction concealing the physical identity of the ITER plant, but respecting its underlying functional requirements. The absence of specifics suggests it will evolve as and when required over its long time-frame. The tokamak features only appear later as structured data. Integration of multiple in-kind delivered Plant Systems will be enhanced by a CODAC Markup Language.

Acknowledgements

The work was partly funded by the Swiss National Science Foundation and by the EPFL. This work, supported by the European Communities under several contracts of Association was carried out within the framework of the European Fusion Development Agreement. The views and opinions expressed herein do not necessarily reflect those of the European Commission.

A large number of colleagues in the Participant Teams have contributed significantly to the present

state of development of this conceptual design and we specifically acknowledge contributions from H. Fernandes, E. Joffrin, E. Jones, B. Guillerminet, A. Maslennikov, Y. Matsumoto, A. Neto, G. Neu, G. Raupp, J. Vega, V. Vitale.

References

[1] http://www.iter.org.
[2] ITER Baseline documentation, http://www.iter.org/bl (under password protection).
[3] J.A. How, J.W. Farthing, V. Schmidt, Proceedings of the 22nd SOFT Conference on Trends in Computing Systems for Large Fusion Experiments, Helsinki, Finland, 2002.
[4] J.B. Lister, B.P. Duval, J.W. Farthing, T.J. Fredian, M. Greenwald, J. How, et al., Proceedings of the 9th ICALEPCS Conference on The ITER Project and its Data Handling Requirements, Gyeongju, Korea, 2003.
[5] Fifth IAEA Technical Meeting on Control, Data Acquisition, and Remote Participation for Fusion Research, Budapest, Hungary, July 12–15, 2005. http://tm2005.rmki.kfki.hu/.
[6] A. Neto, J.B. Lister, H. Fernandes, I. Yonekawa, C.A.F. Varandas, Proceedings of the 24th SOFT Conference on XML Diagnostics Description Standard, Warsaw, 2006.