STATUS OF THE ITER CODAC CONCEPTUAL DESIGN

Jo Lister, ITER IO, Cadarache, 13108 St Paul-lez-Durance, France and
CRPP-EPFL, Association EURATOM-Suisse, Lausanne, Switzerland
Jonathan Farthing, EURATOM/UKAEA Fusion Association, Culham Science Centre, Oxon, UK
Martin Greenwald, PSFC, MIT, Boston, USA
Izuru Yonekawa, JAEA, Naka, Japan

Abstract

Since the last ICALEPCS conference, a number of issues have been studied in the conceptual design of the ITER **CO**ntrol, **D**ata **A**ccess and **C**ommunication systems. Almost all of the technical challenges have seen workable approaches selected. The conceptual design will be reviewed in 2007, before starting the preliminary engineering design.

One software component which does not have a clear solution is the execution of data-driven schedules to operate the installation at multiple levels, from daily programme management to plasma feedback control. Recent developments in workflow products might be useful.

The present conceptual weakness is not having found a satisfactory "universal" description of the I&C design process for the "self-description" of the 80-120 procured Plant Systems. A vital CODAC design feature is to operate the full plant on the basis of imported "self-description" data, which necessarily includes the process description in each Plant System. The targeted formal link between 3-D design, process design and process control has not yet been created.

INTRODUCTION

The ITER project [1] is now in its 10 year programme to construct with 8½ years left to the planned first plasma. ITER operation requires the orchestration of 80-120 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 3 clearly separated tiers: CODAC, Interlock Systems and Safety Systems, indicated in Figure 1 with the three sets of networks. Each tier is implemented both locally and in a centralised system. The principle is to allow enough semi-autonomy in the Plant Systems to perform protective reflex actions where this is appropriate. The central systems then only have to act to coordinate actions for which information on multiple Plant Systems is essential.

CODAC provides the **CO**ntrol, **D**ata **A**ccess and **C**ommunication functions for ITER, allowing integrated operation of all the plant. This functionality 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.

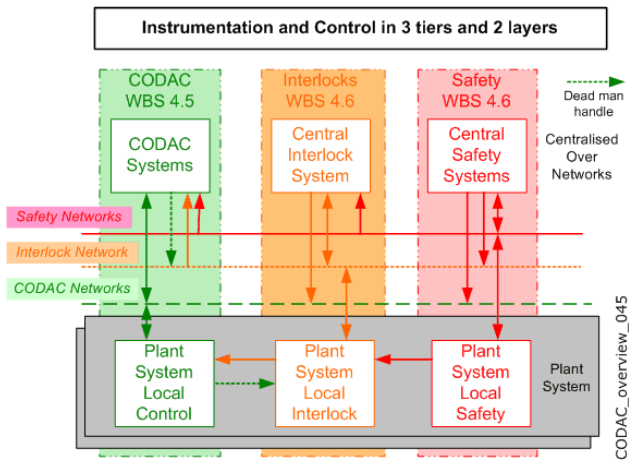

Figure 1: Outline of the ITER control tiers: CODAC, Interlock Systems and Safety Systems. Two layers correspond to local and centralized functionality.

Interlock Systems provide protection of investment for ITER. Each Plant System may have a local Plant Interlock System. The Central Interlock System handles the information from multiple Plant Systems, when their uncoordinated operation is potentially damaging. The signal sources, networks and logic will have a higher degree of reliability and availability than CODAC and will respect the IEC 61508 standards.

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. They will respect IEC 61513 and additional mandatory French standards.

Separating the surveillance and operation of ITER into these three tiers is a major design feature, since the validity of the overall CODAC software 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.

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 pre-determined 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. Triggering the Safety System once in the lifetime of ITER therefore corresponds to a failure of both CODAC and the Interlock 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] and can be summarised as:

- Nuclear installation – new rules will apply
- "In-kind" procurement from 7 Parties
- Reliability/availability higher than any previous fusion project
- Internationally exploited experiment
- Long timescale to construct, operate, maintain
- Continuous operation

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.

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

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.

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. Plant Systems will be based on a mixture of PLC and PC controllers, according to the specifics of each system.

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 PC/PLC controllers, depending on design choices made by the system engineer. Although CODAC constrains the system engineer in the components, a maximum flexibility is proposed to meet the very varied requirements of the Plant Systems, from slow industrial applications to high speed plasma data analysis. This architecture therefore 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. 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. The tool is the "mini-CODAC" emulator, providing all the functionality of CODAC, 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 remains 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 to protect the equipment.

Different approaches to implementing the required functionality inside the Plant System Host have been examined. Initially, we favoured a lowest common denominator approach, essentially using the OPC interface to a Plant System Host SCADA. However, the increased functionality of COTS SCADA systems from PLC manufacturers suggest that it is worthwhile examining a design in which most of the vendor SCADA functionality is deployed. This approach considerably reduces the software to be developed for ITER, but it also commits ITER to vendor lock-in. This last point will become crucial as we go towards product evaluation in 2008.

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 Figure 2 and constitutes the majority 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. Some data may be retained inside the nuclear island for security reasons.

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. 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 Operation Request Gatekeeper is the key element allowing a nuclear device to be exploited internationally at a level higher than simply accessing historical data.

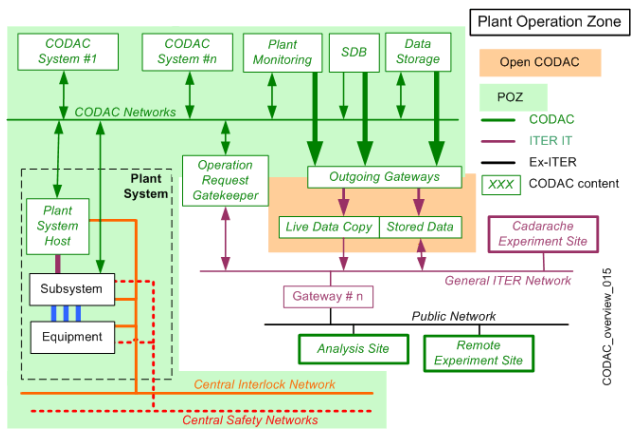

Figure 2: The Plant Operation Zone is shown with a shaded background, with the Operation Request Gatekeeper for incoming requests. CODAC components are shown in green italics. The network links to Experiment Sites are also shown.

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 Figure 2. Separating Experiment Sites from the Main Control Room is a key feature to separate the nuclear licensed operation of ITER from the scientific exploitation of ITER, allowing scientific flexibility and tight operational procedures at the same time.

Plant Systems can be operated under "local control", if authorized 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 does not inhibit inappropriate local commands, unless the action is detected by the Central Interlock as generating an alarm. 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 (into the Plant Operation Network) 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.

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 all 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. A general scheduling tools is needed and a search for an appropriate methodology is currently underway. 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. In the **Main Control Room** and **Experiment Control Rooms**, large area displays enhance human communication.

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. This is based on an industrial Ethernet solution of which three candidates have been identified. ITER feedback control has a much lower bandwidth requirement than existing, more unstable tokamaks. 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 and is assumed to be based on an Application Programming Interface with enhancements added to MDSplus. Features provided by Data Access include management of the signal names, server-side evaluation of data, server-side undersampling of data, as typically used on existing experiments. Providing a project-wide mechanism for redundant fanning out of data from the source to the live and archived data consumers is referred to as **Data Plumbing**, for which several technical solutions are being examined.

Benchmarking suggests throughputs of 400 MB/sec are realistic today.

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.

PLANNING AND CRITICAL PATH

Although CODAC is extremely complex, the critical path is not the CODAC design, but is the specification of the "in-kind" procurement packages. General Instrumentation and Control specifications are being developed to be available for June 2008. These will ensure an adequate degree of homogeneity among the Plant Systems, to allow rational maintenance of all Plant Systems. The timetable for CODAC development is summarised as:

Conceptual design	2006 - 2007
Engineering design of CODAC Systems	2007 - 2009
Retrofitting CODAC design approaches?	2007 - 2012
Factory testing needs "mini-CODAC"	2009 - 2010
Procurement of CODAC Systems	2009 - 2014
Full prototype (maintain during operation)	2010…
Production environment	2010 - 2012
Full simulator using Plant System data	2012…
No developments after…	2014

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, L. Pangione, 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 and V. Schmidt, "Trends in Computing Systems for Large Fusion Experiments", 22nd SOFT Conference, Helsinki, Finland, 2002.

[4] J.B. Lister, B.P. Duval, J. W. Farthing, T.J. Fredian, M. Greenwald, J. How, X. Llobet, F. Saint-Laurent, W. Spears, J.A. Stillerman, "The ITER Project and its Data Handling Requirements", 9th ICALEPCS Conference, Gyeongju, Korea, 2003.