IDM UID
VCGGUA

VERSION CREATED ON / VERSION / STATUS
15 Feb 2018 / 1.1 / Approved

EXTERNAL REFERENCE / VERSION

Technical Specifications (In-Cash Procurement)

Technical Specification for the Service Contract of I&C design support for GIS and GDC PDRs

The purpose of this document is to define the technical specifications for a contract to support the design and integration of ITER GIS and GDC I&C system in the preliminary stage.

Table of Contents

1 Purpose

The purpose of this document is to define the technical specifications for a contract to support the design and integration of ITER GIS and GDC I&C system in the preliminary design stage.

2 Scope

This document summarizes the activities to be provided for the preliminary design of GIS and GDC I&C. It includes the design, verification and integration of local I&C for CODAC, interlock and safety (partially). This document specifies the requirements for the services under the scope of this Contract.

3 Glossary and Acronyms

CODAC	Control, Data Access and Communication
COTS	Commercial off-the-shelf
CIS	Central Interlock System
CSS-N	Central Safety System for Nuclear safety
CSS-OS	Central Safety System for Occupational Safety
DA	ITER Domestic Agency
DO	Design Office
GDC	Glow Discharge Cleaning
GIS	Gas Injection System
I&C	Instrumentation & Control
IDM	ITER Document Management (system)
IO	ITER Organization
IT	Information Technology
KoM	Kick-off Meeting
N/A	Not Applicable
PBS	Plant Breakdown System
PCDH	Plant Control Design Handbook
PD	Preliminary Design
PDR	Preliminary Design Review
PIC	Protection Important Component
PIA	Protection Important Activity
PLC	Programmable Logic Controller
PSS-N	Plant Safety System for Nuclear safety
QA	Quality Assurance
RD	Reference Documents
RO	Responsible Officer
SCS-N	Safety Control System for Nuclear safety
SCADA	Supervisory Control And Data Acquisition
SIC	Safety Important Component
SIL	Safety Integrity Level

For a complete list of ITER abbreviations see ITER Abbreviations 2MU6W5.

4 References

4.1 Applicable Standards

[AS1] IEC 61513 Nuclear power plants – Instrumentation and control important to safety – General requirements for systems, 2011
[AS2] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1 to 7, 2010
[AS3] IEC 61511 Functional safety - Safety instrumented systems for the process industry sector - Part 1 to 3, 2016
[AS4] IEC 60964 Nuclear Power Plants –Control rooms – Design, 2009
[AS5] IEC 61839 Nuclear Power Plants – Design of Control rooms – Functional analysis and assignment, 2000
[AS6] ISA-5.1-1984(R1992) Standard for Instrumentation symbols and Identification
[AS7] IEC 61158 Digital data communications for measurement and control
[AS8] IEC 61000 Electromagnetic compatibility Requirement (includes IEC 61000-5-2)
[AS9] IEC 62402 Obsolescence management
[AS10] IEEE 802.3 Standards for Ethernet based LANs
[AS11] IEEE 61850 Standard applicable to Power Station I&C components
[AS12] IAEA NS G 1.3 Instrumentation and control systems important to safety in nuclear power plants
[AS13] IEC 60709 Suitable physical separation between systems
[AS14] IEC 61069 Industrial-process measurement and control. Evaluation of system properties for the purpose of system assessment.
[AS15] IEC/ISO 62061 Safety of machinery-Functional safety of safety-related electrical, electronic and programmable electronic control systems.

4.2 Reference Documents

The following documents are referenced in this document:

[RD1] ITER_D_27LH2V - Plant Control Design Handbook

[RD2] ITER_D_2YNEFU - Plant Control Design Handbook for Nuclear control systems

[RD3] ICD18 (Fueling & Wall Conditioning)-45(CODAC) (ITER_D_BFATV3 v1.1)

[RD4] ICD-18-46 Fuelling & Wall Conditioning (PBS 18) - Central Interlock System (PBS 46) (A68FEP v2.0)

[RD5] ICD-18-47 Interface Control Document for Plasma Control System (PBS 47) and Fuelling & Wall Conditioning (PBS 18) (ITER_D_32CB9K v2.3)

[RD6] ICD-18-48 Interface Control Document between Fuelling & Wall Conditioning (PBS 18) - Central Safety System (PBS 48) (ITER_D_2LKF6C v2.2)

[RD7] HMI Style Guide and Toolkit (3XLESZ v3.7)

[RD8] ITER Process for Human Machine Interface (HMI) Development (3T9UK2 v2.0)

[RD9] Machine Protection Panel https://user.iter.org/?uid=QF6S6S

[RD10] PBS 18 - Risk assessment (HIRA) report (QFFK98 v1.2)

[RD11] ITER_D_7M2YKF - Order dated 7 February 2012 relating to the general technical regulations applicable to INB - EN

[RD12] ITER_D_SBSTBM - Provisions for Implementation of the Generic Safety Requirements by the External Interveners

[RD13] ITER_D_48Y3CS - I&C Nuclear Safety Control System - Overall Quality Plan

[RD14] ITER_D_JLEVGX - CSS-N Qualification Plan

[RD15] ITER_D_QEZGLD - Central Safety System for Nuclear Safety (CSS-N) - Preliminary DDD

[RD16] ITER_D_347SF3 - Safety Important Functions and Components Classification Criteria and Methodology

[RD17] ITER_D_JHQLDP - ITER catalogue for Nuclear Safety I&C products - Hardwired controllers and slow controllers

[RD18] ITER_D_PSTTZL - List of ITER-INB Protections Important Activities

5 Estimated Duration

The duration of services under this Contract will be for one (1) years.

The contract covers the preliminary design of GIS and GDC.

6 Technical Context

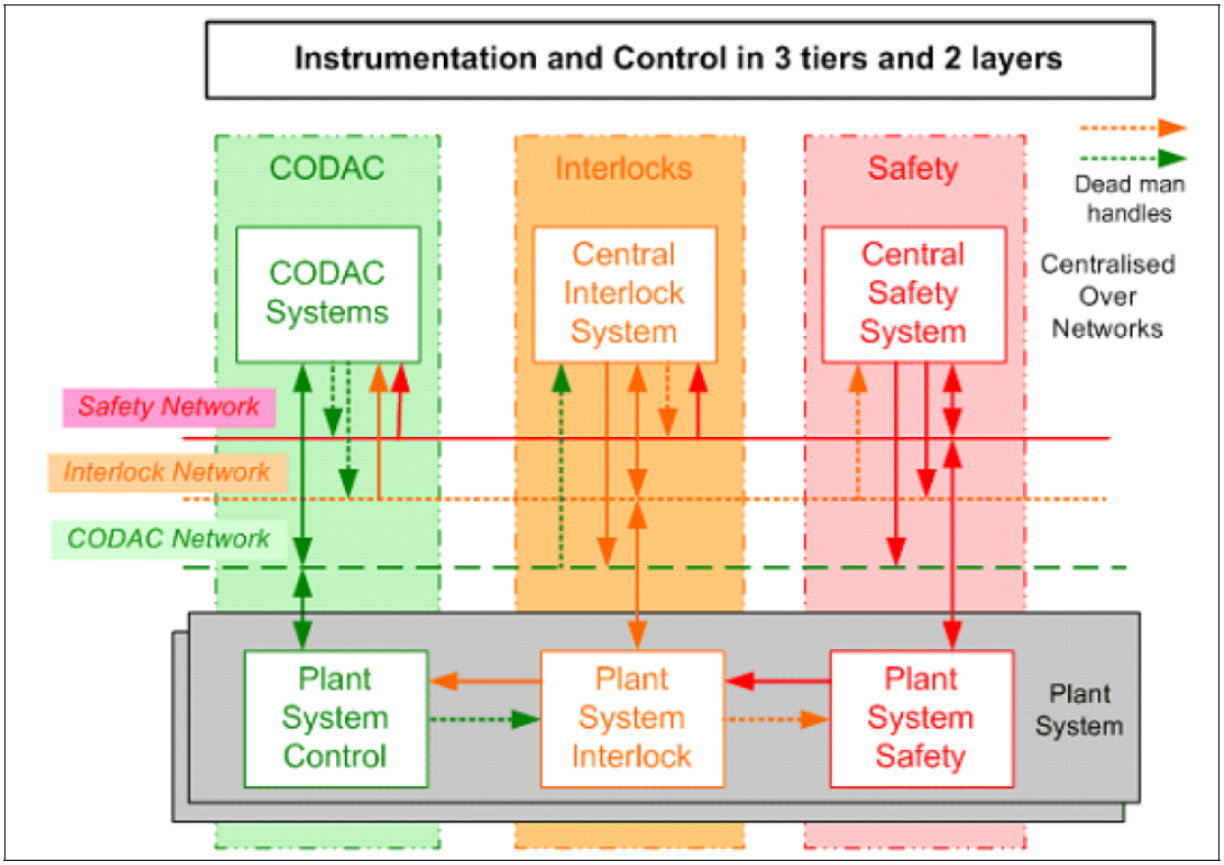
6.1 Background and Objectives

The ITER project is broken down into several “plant systems”, and the individual plant systems are in many cases themselves large, expensive and complex facilities. GIS and GDC are two essential systems for ITER operation. They will be delivered with its own control system (so-called “Plant System I&Cs”) and all of these must be integrated at Cadarache.

ITER operation requires the coordination of the activities of these Plant Systems. This coordination is guaranteed by three clearly separated tiers. These three tiers are: CODAC for conventional controls, Interlock Systems for investment protection and Safety Systems for Nuclear and Occupational safety controls.

Horizontally the ITER I&C System is divided in two layers, one for the Central I&C Systems (CODAC, Interlock and Safety Systems), and another for the different Plant I&C Systems. Both layers are connected through different I&C networks (the general CODAC Systems Networks and the high integrity Central Safety Networks and Central Interlock Networks) besides other specific networks.

This is illustrated in the following figure.



The three-tier CODAC, Interlock and Safety Systems

Figure 1 ITER I&C systems

Rules in [RD1] needs to be followed during the whole lifecycle (safety control needs to follow [RD2]). Interface control documents [RD3], [RD4], [RD5], [RD6] and Interface Sheets between the local systems and the central control are used to record the physical and functional interfaces, which are reviewed regularly during the process of the procurement implementation of each plant system.

This contract aims to ensure the conformity of I&C design to the PCDH and PCDH-N rules for GIS and GDC considering the whole lifecycle and successful reviews in the required hold points of the procurements.

6.2 CODAC I&C

The conventional control of GIS is primarily driven by the needs for plasma operation, which are coordinated by ITER Plasma Control System (PCS). This part of work can be tracked with [RD5] and relevant Interface Sheet. Besides this, other control and monitoring of GIS needed for system running or maintenance should also be performed. The CODAC I&C work can be tracked with the deliverables required in [RD1].

Comparing with GIS, GDC will include additionally the development of a Human Machine Interface (HMI) as the central control coordinating the involved systems during GDC since PCS is not covering this activity.

6.3 Interlock I&C

Similar to CODAC control, Interlock I&C can be tracked with the deliverables required in [RD1]. Besides, there is an ITER Machine Protection Panel ([RD7]) which coordinates the

interlock relevant topics. For investment protection, the interlock functions involving more than one plant systems are called integrated interlocks and need coordination by the Central Interlock System (PBS46).

6.4 Safety I&C

The Safety Control Systems (SCS) are split depending of the type of hazards to be mitigated:

- The Safety Control System for Nuclear safety (SCS-N) addresses radiological hazards.
- The Safety Control System for Occupational Safety (SCS-OS) copes with non-radiological hazards.

The Central Safety System for Nuclear safety (CSS-N) coordinates the individual protection provided by the intervention of locally distributed Plant Safety Systems for Nuclear safety (PSS-N) in charge of the activation of additional protections in order to remove or reduce the detected hazardous conditions. This coordination is performed via the Central Safety Network for Nuclear safety (CSN-N). It should be noted that the implementation of the control logic of several PSS-N has been transferred to the CSS-N. Therefore the CSS-N will combine its role of coordination of the different PSS-N with the implementation of control logic and the direct interface with sensors and actuators.

The SCS-N will implement category A, B and C nuclear safety functions. It will be subject to a nuclear qualification process according to the requirements of IEC 61513 and associated IEC standards and the RCC-E.

The CSS-N is currently in the final design stage. The qualification of the system is ongoing according to the CSS-N qualification plan **Error! Reference source not found.**. These activities are essentially performed by contractors supervised by IO. It should be noted that the components (hardware and software) being qualified for the CSS-N will be also used to implement the control logic previously assigned to PSS-N. The architecture used to implement category A and B functions is hardwired and HIMA Planar 4 has been selected as logic solver; the architecture of systems implementing category C functions is computerized and based on safety PLCs Siemens S-400 FH. The SCADA will be WinCC-OA.

The Central Safety System for Occupational Safety (CSS-OS) coordinates the individual protection provided by the intervention of locally distributed Plant Safety Systems for Occupational Safety (PSS-OS) in charge of the activation of additional protections in order to remove or reduce the detected hazardous conditions. This coordination is performed via the Central Safety Network for Occupational Safety (CSN-OS).

The SCS-OS will implement up to SIL-3 safety instrumented functions. It will be developed according to and be compliant with the IEC 61511/61508. The CSS-OS and several PSS-OS will be developed according to the IEC 61511 lifecycle although other PSS-OS may directly follow IEC 615108.

The CSS-OS is as well in the final design stage. In parallel support is being provided to the first PSS-OS to be installed in ITER. The architecture is based on Siemens S7-400 FH (although some PSS-OS may use S7-300 F) and the SCADA product selected is WinCC-OA.

For each nuclear safety function, ITER CSS (PBS48) prepares the technical specifications in two steps collecting from GIS and GDC the information about sensors and actuators for checking.

OS function is reviewed at each stage of the design phase through Hazard Identification and Risk Assessment (HIRA). Preliminary HIRA report ([RD10]) concludes the possibility that no

OS is needed for GIS and GDC. With the design development, it needs reviewing in the next hold points with the inputs from GIS and GDC design developers.

7 Work Description

This summary covers the technical services to be provided to GIS and GDC under the scope of this contract.

The contract services include:

- **System Engineering services** covering participation to the design of the plant system I&C, performing of I&C functional analysis and specifications, definition and illustration of guidelines for the design, assessment of technical documentation provided by external bodies and integration of Plant System level I&C for GIS and GDC into the ITER project.
- **Interface services** covering the updating of the interfaces of the GIS and GDC plant systems I&C with the central I&C systems. For the physical interfaces, it involves configuration management model tools, like CATIA, See System Design; while for the functional interfaces, Interface Data Sheet is usually used to keep track of the development for plant system I&C.

7.1 Scope of System Engineering services

This part is relevant to the design work on the CODAC, Interlock and Safety System for GIS and GDC.

7.1.1 Task 1: System Engineering for CODAC & Interlock

7.1.1.1 System Design

The scope of this part covers the following aspects:

- Contribution to the development of the functional analysis of GIS and GDC during the PD phase.
- Review and revision of engineering documentation;
- Preliminary HMI design for GDC;
- Technical assessment and report;
- Guidelines for plant systems in order to ease integration;
- Guidelines for plant systems design in accordance with design evolution.

Required competencies are:

- Design of I&C systems, mainly for the plant system I&C layer, in respect of requirements of standards in force on the ITER project;
- SCADA systems based on COTS product (e.g.: Siemens WinCC OA);
- Control System Studio.

7.1.1.2 Functional Specification

The deliverables will be in connection with documentation to specify I&C functions. This spans from the overall process description of the function to the detailed function definition down to the process variable level. The following deliverables will be included in the scope:

- Overall function definition providing a description of the process and the main features of the function,
- Production of logic diagrams.
- Elaboration of the detailed interfaces (exchange tables).

- Determination of the SIL level for interlock functions.

Required competencies are:

- Specification of I&C function,
- Design, commissioning and installations of I&C systems in large scientific projects.

7.1.2 Task 2: System Engineering for Safety I&C design

The Plant System safety I&C system is covered by IO Central Safety System (PBS48). Step 1 and step 2 files are prepared by PBS48 for functional specification and implementation.

The deliverables will be primarily on the review of the design documents to ensure compliance with the PCDH-N and successful integration with the CSS; review of the functional specification files for nuclear and occupational safety.

Required competencies are:

- Specification of I&C safety function,
- Design, commissioning and installations of I&C safety systems in nuclear facilities or large scientific projects.

7.2 Task 3: Interface Services for GIS and GDC

The scope of these services is to develop and maintain physical and technical interfaces between GIS and GDC with the central control systems and other relevant plant systems.

The main deliverables are the Interface Control Documents and corresponding Interface Sheets of GIS and GDC with the central control system including CODAC, PCS, CIS and CSS. The work covers the contents needed for the whole lifecycle including design development, testing and integration.

Relevant skills are:

- Extracting design model from ITER CAD database;
- Processing flow diagram and cabling diagrams.

8 Responsibilities

8.1 Obligations of the Contractor

The work will be performed according to deliverables defined.

8.2 Obligations of the ITER Organization

The ITER Organization shall make available:

- Procedures, information, data and any specialized equipment necessary for the Contractor to perform its functions under this Scope of Work;
- A safe work area which meets the generally-accepted requirements for the satisfactory execution of the Services;
- Any necessary and appropriate safety training;
- IT equipment and access to IO network for the services with a duration on IO-site longer than 6 months if long term working on-site is needed.

9 Deliverables and due dates

The Contractor shall submit all relevant data necessary to demonstrate the performance and outcome of its deliverables to the ITER Organization upon request by IO-RO anytime during the course of the tasks and subtasks.

Documentation which includes all materials (spread sheets etc.) and references (graphs, tables, data sources, etc.) shall be provided in order to allow reproduction and traceability of the results.

No.	Relevant Task No.	Clause in the document	Deliverable Name	Requirements	Due Date from T0*
D1	-	11.1	Detailed implementing plan	Reports on working plan synchronizing to the design activities in the PD stage.	+2m
D2	T1	7.1.1	Specifications (GIS, GDC)	It should include the followings: a) GIS CODAC I&C control philosophy, CODAC and interlock I&C functional specification for operation and protection, system operation states at the PD level. b) GDC CODAC I&C control philosophy, CODAC and interlock I&C functional specification for operation and protection, system operation states at the PD level.	+6m
D3	T1	7.1.1	Design (GIS, GDC)	PD level System Architecture Design Description. It should include the followings: a) GIS Functional Architectures (signals and interface data) b) GIS Physical Architectures (components, cubicles) c) GDC Functional Architectures (signals and interface data) d) GDC Physical Architectures (components, cubicles)	+6m
D4	T1	7.1.1	GDC HMI design	PD level (Consolidation of interface systems and logics)	+6m
D5			Verification and validation (GIS, GDC)	Report of DA I&C design activities on the conformity to the PCDH and consistency with the central I&C and PCS.	Monthly
D6	T1		Verification and validation (GIS, GDC)	Review deliverable documents required by PCDH from supplier.	+8m
D7	T3	7.2	Interface services	Review IS vs 45, 46, 47 and 48	+8 m
D8	T2	7.1.2	Safety I&C Systems design	Review nuclear function technical specification document files jointly prepared with the central safety system, Occupational safety related documents	+8 m
D9	T1,2,3		Final Report	Final report during Preliminary Design stage, and this includes: a) Executive summary of all the activities conducted by the Contractor under this contract; b) List of produced documents and reference; c) List of activities made by the Contractor.	+11m

*T0 is the date of kick of meeting to be held by both parties.

10 Acceptance criteria

The IO-RO shall review the deliverables and reply, within the 15 following days, a commented version of the deliverables. The Contractor shall perform all the necessary modifications or iterations to the deliverables and submit a revised version. The Contract will be considered completed after ITER has accepted the last deliverable.

All the reports must meet every relevant part of technical requirements specified in this technical specification document and referenced documents.

Deliverable is considered to be approved:

- when it has been fully approved by IO in ITER document management system (IDM) for all the deliverables except D6, D7 and D8, and
- when it has been accepted by IO RO by email or in writing for D6, D7 and D8.

11 Contract Execution & Organisation

11.1 The detailed work plan

In order to ensure the required quality required in this service, the Contractor shall develop, plan, implement, and execute the contract based on their work plan.

After the kick off meeting with the IO, the Contractor shall first prepare the detailed implementing plan synchronizing the design activities in the PD stage. This should include the following items:

- The detailed schedule and project milestones
- The methodology and organization to execute the works
- The risks and opportunities identified in execution
- Potential measures to mitigate identified risks

11.2 Contract Follow-up

Progress of the deliverables will be monitored during weekly meetings with the IO Contract Manager and concerned other IO staff, including short-term schedules and new and on-going Task Orders.

The minutes of these meetings shall be written by the Contractor in the simplified form of a table of action items and archived in IDM.

The Contractor shall submit written progress reports to the IO Responsible Officer every month. The progress report shall be in .doc(x) format and include at least the following information for the reporting period:

- Summary of the work carried out for all on-going Tasks.
- Description of any problems encountered for all on-going Tasks.
- References to any produced deliverables for all on-going Tasks.
- Status and schedule of all on-going Tasks.

The progress report shall be submitted three working days before a regular weekly meeting and discussed there.

The progress report shall be approved by the IO- RO.

11.3 Meeting Schedule

The following meetings and submissions of progress reports should be foreseen.

Scope of meeting	Point of check progress or final report	Place of meeting
Kick-off Contract	Work program (within ten days after signature)	ITER site
Progress meetings	Progress check and further work definition (every 4 weeks)	ITER site or Video Conference
Summary presentation	Summary presentation about I&C work for PDRs. (12 months after signature)	ITER site

12 Quality Assurance Requirement

Contractor should have ISO 9001 accredited quality system. Otherwise the Contractor shall have QA Program approved by the IO.

Prior to commencement of works, Quality Plan which comply with Procurement Requirements for Producing a Quality Plan (ITER_D_22MFMW) shall be submitted to IO for approval with evidence of the above. The Contractor's Quality Plan shall describe the organisation for tasks; roles and responsibilities of workers involved in; any anticipated sub-contractors; and giving details of who are the independent checkers of the activities.

Where any deviation is requested or non-conformity happens from Technical Specification, for Non Conformity the procedure in ITER_D_22F53X shall be followed, which for Deviation Request the IO procedure in ITER_D_2LZJHB shall be followed for the management of Deviation Request.

Documentation developed as the result of works shall be retained by the Contractor for a minimum of five (5) years and then may be discarded at the direction of the IO.

IO will monitor implementation of the Contract's Quality Plan through surveillance. Where condition adverse to quality is found during monitoring, IO may request to the Contractor to take corrective action. The use of computer software to perform a safety basis task activity such as analysis and/or modelling, etc. shall be reviewed and approved by the IO prior to its use, in accordance with Quality Assurance for ITER Safety Codes (ITER_D_258LKL). Where applicable, Software Qualification Policy (ITER_D_KTU8HH) shall be taken into consideration to ensure quality and integrity of software prior to application.

In the case of the Nuclear Safety Control System (SCS-N), Contractor shall perform the works on the basis of I&C Nuclear Safety Control System - Overall Quality Plan (ITER_D_48Y3CS).

13 Safety Requirements

ITER is a Nuclear Facility identified in France by the number-INB-174 ("Installation Nucléaire de Base").

For Protection Important Components and in particular Safety Important Class components (SIC), the French Nuclear Regulation must be observed, in application of the Article 14 of the ITER Agreement.

In such case the Suppliers and Subcontractors must be informed that:

- The Order 7th February 2012 applies to all the components important for the protection (PIC) and the activities important for the protection (PIA).
- The compliance with the INB-order must be demonstrated in the chain of external contractors.
- In application of article II.2.5.4 of the Order 7th February 2012, contracted activities for supervision purposes are also subject to a supervision done by the Nuclear Operator.

For the Protection Important Components, structures and systems of the nuclear facility, and Protection Important Activities the contractor shall ensure that a specific management system is implemented for his own activities and for the activities done by any Supplier and Subcontractor following the requirements of the Order 7th February 2012.