ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR05

INTEGRATED SUPERVISION FOR CONVENTIONAL AND MACHINE-PROTECTION CONFIGURATION PARAMETERS AT ITER

D. Karkinsky†, W. Van Herck, I. Prieto Diaz, J. Soni, A. Marqueta, ITER Organization, St. Paul lez Durance, France

Abstract

Configuration parameters for ITER's I&C systems are predominantly high-coupled due to the nature of the process under control. Subsequently, I&C re-configuration requires an integrated supervision approach that addresses coupling through abstraction, automation, scalability, changeability, robustness and re-usability. Moreover, high-coupling might manifest at any tier of the I&C, and certainly spans configuration parameters across both conventional and investment-protection I&C.

Stemming from ITER design guidelines, the handling of investment-protection configuration parameters needs to meet the goals of IEC61508. These goals are mostly in congruence with the main concerns of integrated supervision identified above. However they also extend requirements that bind the supervision process with traceability and audit capabilities from sources to final self-test (run-time) diagnostics.

This presentation describes the provisions for integrated supervision at ITER and elaborates how these provisions can be used to handle machine-protection parameters in compliance with IEC61508.

INTRODUCTION

The ITER plant configuration system is a component of the Control, Data Access and Communication (CODAC) Supervision and Automation (SUP) system and is tasked to:

- Derive machine parameters from the central planned experiment information contained in the pulse schedule,
- Conduct a multi-stage engineering verification process involving a wide range of codes (e.g. electromagnetic induced forces on mechanical structures, scarce resource budget management, etc.),
- Convert machine parameters to the number and format representation of the various Plant Systems Instrumentation and Control (I&C), and
- Eventually load machine parameters to the Plant Systems Instrumentation and Control (I&C) as part of the experiment preparation.

The ITER plant configuration system interfaces to ITER machine Operation, to a heterogeneous set of data repositories (e.g. pulse schedule queue, machine geometry and condition, operating limits, live measurements, Plant System self-description data, etc.), and the Plant System Instrumentation and Control (I&C) systems that compose the ITER machine.

† Damien.Karkinsky@iter.org

The ITER plant configuration participates to the ITER defence-in-depth machine protection scheme by ensuring the configuration is as thoroughly verified as deemed necessary before starting lengthy and costly operations.

The baseline design for the Plant System I&C configuration interface is using EPICS records databases and Channel Access (CA). This was challenged during the 2014 CODAC design review. It was then understood that this choice was ill adapted to address the complexity required in the scope of ITER Plant Systems, and in particular in those areas below:

- Large and complex data structures involved.
- Existence of dependencies between parameters.
- Exception handling (e.g. restoration of valid configuration after a failed verification by the Plant System) and reporting.
- Handling of investment protection parameters for the Integrated Control System (ICS).

As a result, the configuration system was designed to support:

- Structured configuration variables,
- Atomicity of loading such, possibly complex, data structures,
- Protection against data corruption.

The protocol for Plant System I&C configuration is defined to follow the sequence outlined in Figure 1. The hash provides protection against data corruption and acts as a digital signature of over a data stream that can encapsulate an arbitrary set of configuration parameters.

In this presentation we report the results from an investigation into how the ITER plant configuration system can integrate with ITERs integrated control system (ICS) for handling investment protection parameters. As per ITER guidelines the ICS needs to meet the goals of IEC61508[1]. We report on the process by which we arrived at an adequate integration point for both systems and the technological solutions that have been put in place in support of this integration.

SUP SYSTEM DESIGN

ITER defence-in-depth principles, and the overall complexity of the machine, dictate that parameters are verified before being loaded to the plant. Distinct verification processes may be used depending on the nature of the task.

Furthermore, high-level operation will define operation goals, from which Plant System parameters must be derived (e.g. required cryogenic cooling capacity derived from predicted thermal loads).

To accommodate these requirements, the SUP configuration framework contains the following subcomponents:

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR05

- Configuration Verification and Validation Framework (CVVF): this framework encapsulates user-defined transformation and verification codes and exposes these as network services; the framework allows for the integration and invocation of codes that were implemented in different programming languages (e.g. C++ or Python);

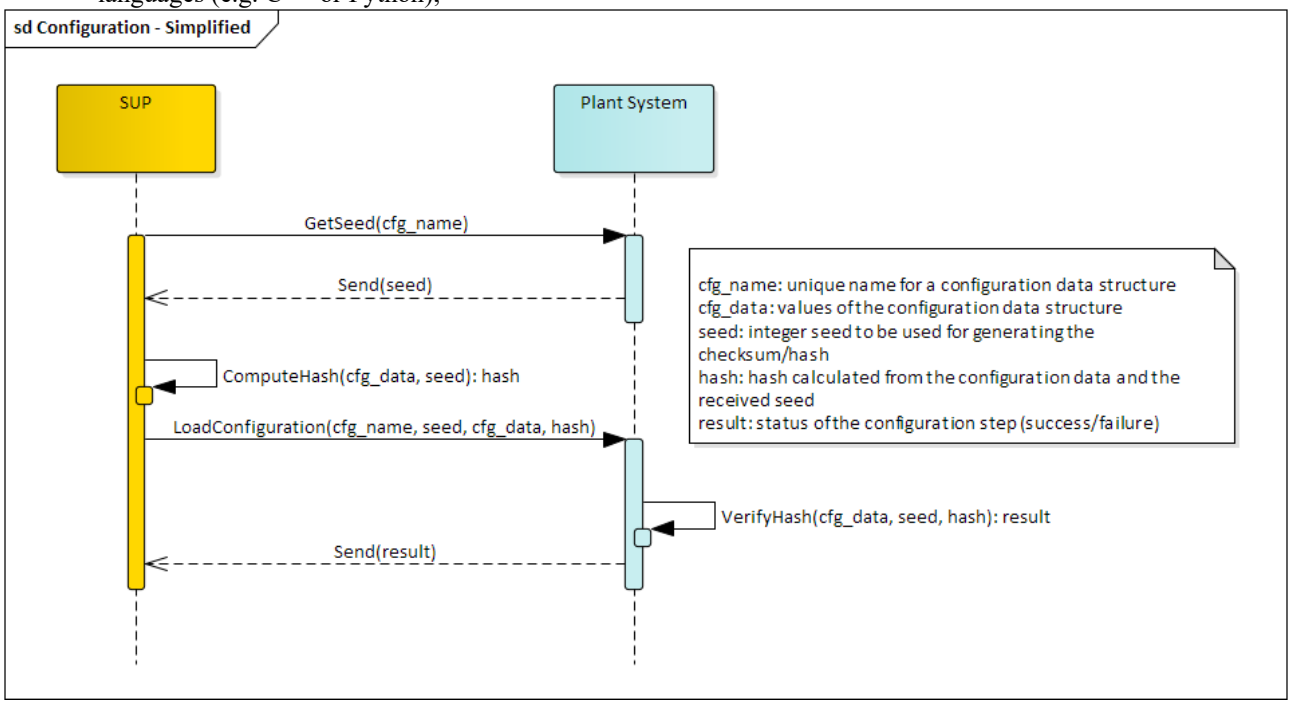

Figure 1: Simplified sequence diagram for Plant System configuration by SUP.

- Chain Data Processing engine (CDP) to define and execute workflows through CVVF applicable to various Plant I&C.

In order to support differentiated workflows for distinct types of users (e.g. operator and expert users), or during distinct life-cycle phases (e.g. testing, commissioning or operation), the configuration process and workflow definition is data driven.

An example of a simple configuration workflow clarifies how different processes in the workflow can depend on one another:

- Retrieve high-level parameters for the current activity;
- Call CVVF service to:
  - verify the authenticity of the received parameters;
  - verify that the high-level parameters of the current activity are within operational constraints;
  - transform high level parameters from the physics/operational domain to the engineering domain (machine specific);
  - verify that the machine specific configuration parameters do not lead to violations of machine or operational limits and constraints;
  - hash the streams of output to each Plant System;
- If all CVVF steps pass without an issue, transmit those parameters to the Plant System I&C in an atomic transaction.

Each of the CVVF processes express the configuration transformation and validation needs, through a set of remote function calls, which are identified using a Uniform Resource Identifier (URI). These function calls are fed with variables from the engine's workspace and result in updating other variables in the workspace.

INTEGRATED CONTROL SYSTEM AND ITS CONFIGURATION

ITER functions for investment protection are implemented in dedicated Plant System I&C called Plant Interlock Systems (PIS). PIS are coordinated by interlock functions of the Central Interlock System (CIS) where transversal investment protection risks are identified. Together these systems form ITER's Integrated Control System (ICS).

In the baseline design, the configuration of CIS is performed at the CIS desk through a custom High-Integrity Operator Commands (HIOC) [2] application layer protocol based on an OPC-UA interface. This interface is independent from SUP and the configuration of the PIS. Stemming from high-coupling, in almost all situations concerning PIS configuration, SUP configuration is the only realistic solution. This results in a gap of requirements for the ICS on handling critical configuration parameters. For instance, PIS modification without central coordination at the level

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR05

of ICS can lead to un-intended side-effects that can affect fault-tolerance claims and the ability of ITER to remain in a given operational state. Additionally, even in the case of some CIS functions it has become clear that certain parameters need to originate from the pulse-schedule, traverse a SUP workflow, and be communicated to the CIS desk with the necessary degree of assurance.

For this reason CIS needs to play a role during PIS modification, if only to ensure that the pre-conditions during PIS-modify actions are met. This justified a need to seek closer integration between HIOC and SUP and to develop a centralised policy for handling configuration parameters.

IEC61508 COMPLIANCE AND SUP

Investment protection function reliability implemented in ICS is commensurate to integrity targets in the SIL-1 to SIL-3 range according IEC61508. The goal of IEC61508 compliance for investment protection at ITER, is to demonstrate assurance within IO that these functions meet the identified reliability target. In order to drive the requirements for HIOC and SUP integration, we performed an analysis of IEC61508 requirements w.r.t. handling configuration parameters and matched these to SUP requirements.

From the perspective of investment protection, SUP generates outputs which can directly contribute to the executable code of a PIS and therefore, it was considered to be a T3 off-line support tool (see IEC61508-3 7.4.4) for the ICS. There are two main clauses of the standard that we need to respect with regards to such tools:

a) Treat SUP as a software element of the ICS where the level of reliance that is placed is assessed, failure mechanisms identified and mitigation measures taken (see IEC61508-3 7.4.4.1 and 7.4.4.5),
b) Define and meet criteria for coherency of this tool in the system development (which includes configuration) activities (see IEC61508-3 7.4.4.2).

In the case of a) only the workflows for storing, verifying and generating the configuration parameters for a PIS are of interest. Moreover, not all software components in a given workflow will need to be of integrity commensurate to the investment protection integrity target. Where parameters pass untrusted software components, adequate trusted measures can be added to close the vulnerabilities introduced from untrusted elements. In the context of PIS configuration, we aim to classify CVVF transformation and verification steps in three tiers:

1. Untrusted, where no guarantees can be placed on the step's correctness or it can introduce errors in the configuration parameters
2. Trusted with low-confidence, where the integrity of the step is not as required by the integrity target or there are intrinsic failure mechanisms in the technique on which the step is based, which cannot be mitigated.
3. Trusted with high-confidence – the integrity of the step is as strict as required by the integrity target and all failure mechanisms have been mitigated.

Confidence is directly related to the systematic capability (see IEC61508-4 3.5.9) with which a step was developed, verified and change managed. For instance; lack of separation of techniques, development teams or the presence of un-mitigated intrinsic vulnerabilities in the implemented method, reduce confidence in the step. However, low-confidence trusted steps can be combined into higher confidence following the constraints placed by systematic capability over elements (see IEC61508-2).

In the case of b) we set the criteria for structured configuration parameters from IEC61508-3 7.3.3.12-13, 7.4.2.14 and (guide) Annex-G. In a broad sense these require:

a. Verification of the consistency, completeness and compatibility of; data structures, operational parameters and interfaces.
b. Full transparency over the workflow and in particular identification of all items needed to replay any step in the process of loading configuration parameters.
c. Detection of unauthorised changes,
d. Detection of corruption at run-time.

Item a) is partially met from the design requirements of SUP. To meet the requirement fully it is necessary that PIS ROs and ITER Operators take formal steps in determining which configuration parameters pose investment protection risks (e.g. risk assessments) and to drive the specification for the workflows of trusted/untrusted steps within CDP from the identified risks.

In contrast, item b) was identified as a new requirement for SUP. This requirement is not immediately obvious from the perspective of conventional Plant I&C. The requirement requests SUP to ensure that inputs, step configuration, outputs and roles involved in executing each CVVF step at a point in time and in a given workflow, be recorded so that the chain can be audited from the source to destination. The ability to replay CDP workflows gives the ability to identify the source of a fault and drive a policy of continuous improvement.

Items c) is within the domain of ICS, where a central method is necessary to inhibit unauthorised changes, and item d) is in the domain of each PISs which needs to perform run-time verification over static-data as part of its self-check diagnostics.

Given these requirements, the interface point for HIOC and SUP was set at c) and d) and additional measures that will permit a configuration change to be traced to a workflow execution within SUP.

HIOC AND SUP INTEGRATION

The development of HIOC, followed IEC61508-2 requirements for a "black-channel" interface where measures necessary to ensure the failure performance of the communications process were implemented. IEC61784-3[3], which contains broad risks & measures guidelines for com-

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR05

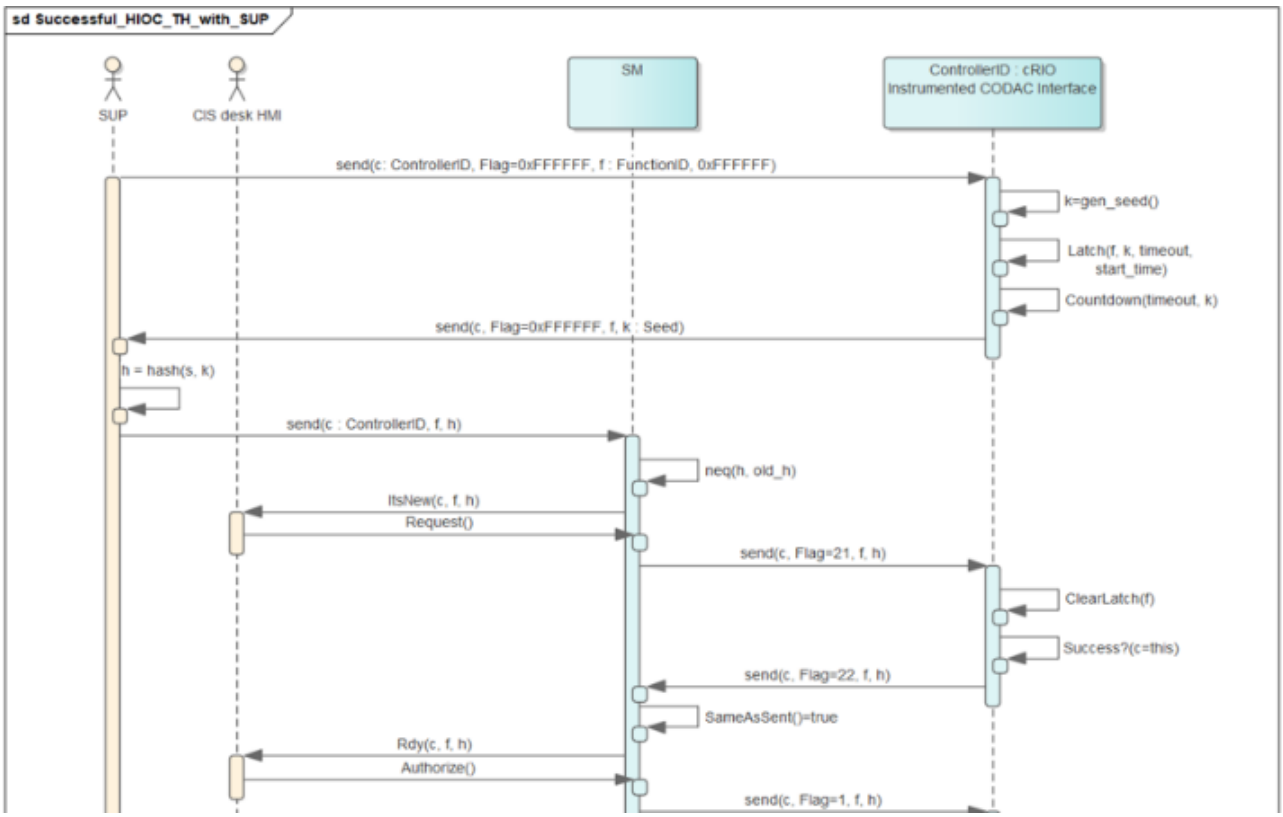

Figure 2: Interaction sequence in HIOC with SUP.

munication channels, was used as the source of requirements. The software elements that have been developed support up-to SIL-3 on PLC and SIL-2 on FPGA types of hardware.

HIOC involves a three-stage configuration process that aims to verify;

1. The controller identity (*ControllerID*) that is being modified is as intended by the operator.
2. The function identity (*FunctionID*) on the controller being modified is as intended by the operator.
3. The configuration parameter value (H) that is being changed is as intended by the operator.

These guarantees are provided at application level, meaning lower level components in the communications hierarchy can be of arbitrary integrity. If one of the three stages fails, HIOC aborts the configuration process which means that the parameter is not loaded into the critical path of the target function's control loop.

The main use-case of HIOC is to modify single value Boolean and Threshold parameters. Such parameters can be used to gate PIS special states e.g. mask the PIS response to a hard or a soft reset or set the maximum plasma current threshold for a given experiment.

In the case of HIOC with SUP integration, the Threshold use-case was re-purposed as an 8-byte SHA-1 hash of a configuration stream. Major assumptions in the use of HIOC is that it shall be utilised within a secure network where all entities are known and are non-malicious. It is within this assumption that HIOC provides a trusted mechanism to preload this hash and set the PIS's SUP interface in a state where the PIS can accept new parameters.

Each hash is valid for a specified time period and is based on a random seed value generated by the PIS. SUP requests the seed from the PIS on protocol initiation and generates the new hash (Figure 1). It then makes a request to the CIS Supervisor Module (SM in Figure 2). The CIS-SM initiates a HIOC interaction with the PIS to retrieve the seed and authorise the new hash. The first goal is to enter the hash, seed and time into the ICS logs. This permits the HIOC transaction to be traced to the outcome of the CDP workflow execution that produced the hash. The second goal of CIS-SM is to verify that given the current ICS state, the PIS can be modified. This can be done by asking for confirmation from the CIS desk (i.e. manually) or automatically. Rules on when PISs must be fully or partially available result from operator instructions. A fully automatic process is not possible as PIS operating rules vary.

Transmitting the hash through the remaining HIOC steps indicates an authorization to load the particular configuration stream that corresponds to the hash/seed pair.

On obtaining authorization to load new parameters, the PIS enters a wait-state for the parameter stream from SUP. During this state, the PIS might override the relevant investment protection functionalities (e.g. placing the outputs in a known disabled state to avoid a spurious trigger of ICS). If it receives this stream within the allocated timeout it can generate its own hash and compare the result against the hash received via HIOC. If the two hashes

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR05

match the PIS can proceed to load them into the critical control loop, which will then re-establish the investment protection outputs to their computed state. The result is reported to the CIS-SM in an abort or a success identifier which is also logged.

Additionally, the PIS can use the hash inside its self-test diagnostics loop to check if the parameters remain unmodified during runtime. Depending on the technology used to store these parameters, they could be susceptible to various forms of memory corruption (e.g. single event upsets).

This approach requires PISs to integrate with HIOC over a separate interface from SUP. The level of separation is dictated by the level of confidence that is required. At the extreme end a different hardware interface can be used. For instance, PIS typically integrate with SUP over the Plant Operations Network (PON). HIOC is normally executed over the Central Interlock Network (CIN), but it can be utilised on PON since the integrity is achieved at the application layer. Additionally EPICS and OPC-UA adaptors have been developed for the common frameworks used in PIS development [4].

CONCLUSION

In this presentation we reported on a central policy for handling investment protection configuration parameters of arbitrary complexity that arises from interfacing the ITER plant configuration system and the ITER integrated control system.

The requirements from this integration were derived from the IEC61508 standard as required by ITER guidelines. The presentation also outlined the technical design that supports this integration.

A number of open questions remain, such as the need of PIS developers to determine which parameters pose investment protection risks to drive workflow definition requirements and the need to incorporate runtime checks over the consistency of these parameters as part of self-test diagnostic routines.

The use of a central policy for handling configuration parameters and special state gate-keeping will eventually target the realisation of central rules over the level of readiness of components within ICS that govern the effective ITER Operational State or a proposed transition to a new state. In the present baseline, each PIS and CIS are preparing individual concepts of operation, and these plans are an important preliminary step towards identifying central rules for ITER operation.

REFERENCES

[1] IEC61508 “Functional safety of electrical/electronic/programmable electronic safety-related system”, 2010.

[2] Fernández Adiego, Borja & Blanco Viñuela, Enrique, (2017). “Applying model checking to critical PLC applications: An ITER case study”, in *Proc. ICALEPCS2017*, Barcelona, Spain, Oct. 2017, pp. 1792-1796. doi:10.18429/JACoW-ICALEPCS2017-THPHA161

[3] IEC61784-3 “Part 3: Functional safety fieldbuses - General rules and profile definitions”, 2010.

[4] A. Neto, F. Sartori, B. Bauvir, “Interfacing MARTe2 to the EPICS Channel Access and pvAccess protocols”, presented at EPICS collaboration meeting, Cadarache, France, Jun. 2019, unpublished.