

THE LASER MEGAJOULE CONTROL COMMAND SYSTEM INTEGRATION PLATFORM

J.P. Arnoul, J. Fleury, A Mugnier, CEA, DAM, CESTA, 33116 Le Barp Cedex, France.
J. Nicoloso, CEA, DAM, DIF, F-91297 Arpajon, France

Abstract

The French Atomic Energy Commission (CEA) has just built an integration platform outside the LMJ facility in order to assemble the various components of the Integrated Control Command System (ICCS).

This article provides an overview of this integration platform and the qualification strategy based on the use of equipment simulators, and focuses on several tools that have been developed to integrate each sub-system and qualify the overall behavior of the ICCS.

Each delivery kit of a sub-system component (Virtual Machine, WIM, PLC,..) is scanned by antivirus software and stored in the delivery database. A specific tool allows the deployment of the delivery kits on the hardware platform (a copy of the LMJ hardware platform). Then, the TMW (Testing Management Workstation) performs automatic tests by coordinating the equipment simulators behavior and the operator's behavior. The tests configurations, test scenarios and test results are stored in another database. Test results are analyzed, every dysfunction is stored in an event data base which is used to perform reliability calculation of each component.

The qualified software is delivered on the LMJ to perform the commissioning of each bundle.

THE ICCS ARCHITECTURE

The ICCS architecture has been described in [1]. The global system is achieved by a dozen contractors each of them being responsible for a subsystem. A subsystem is composed of all the equipment provided by the contractor plus all the PLC that drive the equipment plus the subsystem supervisory which authorizes the subsystem operator - in the control room - to perform exploitation and/or diagnostic operations on the subsystem.

The main functions of the high level supervisory subsystem are achieved by other contractors.

Each subsystem is connected to the global supervisory which is designed to dialog with all the subsystem mainly using dedicated software called "sequences".

THE ICCS INTEGRATION STRATEGY AND ASSOCIATED SIMULATORS

The ICCS Integration strategy has been described in [2]. One of the main aspects of this strategy is that global tests are mainly carried out on a dedicated platform next to the LMJ site which is totally representative of the LMJ ICCS except the fact that no real equipment is present in the PFI building: it is replaced by different kind of simulators depending on the interface level you want to simulate according to Figure 1.

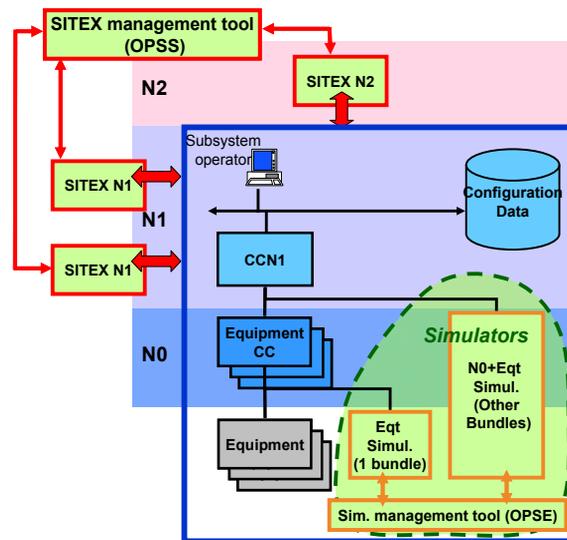


Figure 1: The different kinds of simulators.

You can find on the Integration Platform three kinds of simulators:

- "SITEX" (EXternal InTeface Simulators) which are designed to simulate the high level interfaces between the high level supervisory and the subsystems supervisory (N2-N1 interface), or interfaces between subsystems supervisory (N1-N1 interface). These interfaces are based on a dedicated protocol which is used by all the subsystems.
- "N0+Eqt Simu." is an internal simulator (according to a subsystem) that simulates the N1-N0 interface; this interface is most of the time based on a standard protocol.
- "Eq Simu". is an internal simulator (according to a subsystem) that simulates the N0-Equipment interface.
- Simulators management tools allow test operators to dynamically configure the simulators behaviors.

Each Subsystem Control system is delivered on the Integration Platform and tested in three successive phases:

- Phase 1: the "stand alone" phase in which the other subsystems are simulated by the SITEX
- Phase 2: the integration phase in which the subsystem is connected to the high level supervisory and the other subsystems already installed on the platform. During this phase each N2-N1 and N1-N1 interface of the subsystem is tested.

When enough subsystems have been tested (phase 1 and phase 2) we proceed to the last phase:

- Phase 3: the global commissioning phase. During this phase the global operation of the system is tested using the several subsystems and the sequences.

THE ICCS INTEGRATION BUILDING

A dedicated building has been constructed next to the LMJ site to perform these tests before delivering the ICCS on the LMJ.

This building consists of an office area, an area for control rooms, a computer room, an area for the utilities. Each area has a dedicated access control.

The computer room is designed to accommodate up to 60 computer racks. The cooling system of the computer room is based on the use of hot aisles and cold aisles. It is dimensioned for 240kW. Electric power is maintained and backed by batteries and a generator, with an autonomy of 8 hours.

THE ICCS INTEGRATION PLATFORM TOOLS

To perform the several functional tests of the LMJ ICCS, specific tools have been developed by the contractor in charge of performing these tests. They constitute what we call the PFI Core. We can distinguish:

- the antivirus Tool called SAS
- the Software Configurations Management Tool called OGEKI
- the Test Campaign Management Tool called PGT
- the Bug Management Tool called FFT

A specific hardware platform was also built to install the simulators provided with each subsystem.

The Antivirus Tool (SAS) and its Main Functions

As the LMJ network is totally isolated from the rest of the world the only way to contaminate the network is when you enter new data on it. To lower this risk, each software delivered by a contractor, is first scanned with the antivirus Tool comprising two different antivirus software programs, each of them running on a dedicated computer. These computers are not on the PFI Network, but on a stand alone local network that is automatically connected to Internet each night only during the necessary time, to update the antivirus signatures. In case of a virus contamination is detected by the Antivirus Tool, we can therefore guarantee that the virus has not contaminated the PFI Network. (Fig. 2).

Software is mostly delivered as .rar packages including virtual machine (VM) or WIM, plus other files describing the delivery.

Several types of scanning are performed: a “raw” scanning of the .rar packages, a “cold” scanning after mounting the VM or WIM and a “hot” scanning after starting the VM or WIM, and using the antivirus tool that is already installed on the delivered machine.

Once those several scans are done, the result are archived and the software is copied and signed on a dedicated data transfer hard disk. The signature ensures that no data has

been changed between the copy of data on the Antivirus Tool and the insertion on the OGEKI Tool on the PFI Network. This data transfer hard disk is the only physical external support that can be connected to the PFI Network and it is allowed only on the OGEKI computer. All other USB ports are locked.

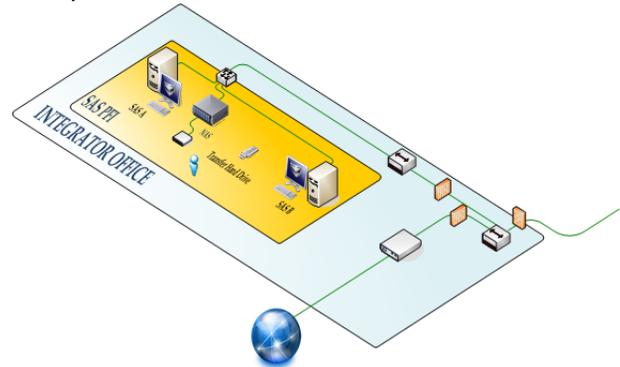


Figure 2: Antivirus Tool hardware architecture.

The Software Configurations Management Tool (OGEKI) and its Main Functions

The OGEKI is a standard computer connected to a data server with high storage capability. On this data server you can find the several databases used by the PFI Core Tools. (Fig. 3)

The first function of the OGEKI is to recognize the data transfer hard disk.

Each software delivery is stored in a database called “management software database” (BDGL ...in French).

A dedicated interface allows the operator to know of which software is made a specific industrial delivery, to know at any time the different versions of delivered software, to know where a particular version of a particular software DVD or BluRay is stored. Each BluRay or DVD is identified with a bar code.

The tool computes (or allows to manually enter) compatibility rules between the various software supplied. These rules are used to build consistent tests: if non compatible software versions are used to perform functional tests then the operator is warned.

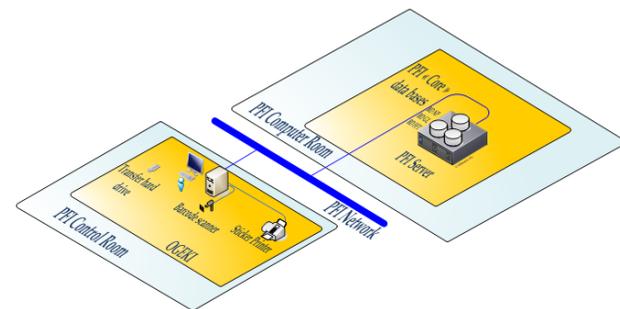


Figure 3: Software configurations management Tool hardware architecture.

The Test Campaigns Management Tool (PGT) and its Main Functions

The PGT can be seen as the heart of the PFI “core”. The PGT main functions are to define test campaigns and conduct the tests included in these campaigns. A test campaign consists of:

- the identification of the campaign (name, person in charge, ...)
- the list and description of the functional requirements to be tested
- the test configuration i.e. the VRF* chosen for the tests, the description of the machines (PCs, PLCs, ...) to use for the campaign (which version) and the sets of data associated with each machine according to the conducted test. Once the configuration test is defined, the PGT requires the installation tools to deploy the selected machines.
- the description of the test sequences. The PGT is based on the Teststand© (National Instrument® commercial product)
- the test results (for each test plus a general report). If a test sequence fails, PGT automatically generate a bug for the FFT tool.

The Teststand© test sequences can be defined using MaTeLo©. MaTeLo© is a product from the All4Tech® company which allows to generate Teststand© test sequences according to a test strategy called DOT (Dynamic Optimized Testing). The DOT aims at optimizing tests duration and is based on the objective to reduce system failure during a predicted operational use.

Three different operators can work simultaneously on three different test campaigns. A PGT workstation is a four-screen workstation that allows the test operator to simultaneously use the PGT GUI and to observe the GUI of the subsystem under test.

The PGT software is implemented on two virtual machines under windows 7©. All the PGT campaigns are stored in the BDNP Database on the PFI Server. (Fig. 4)

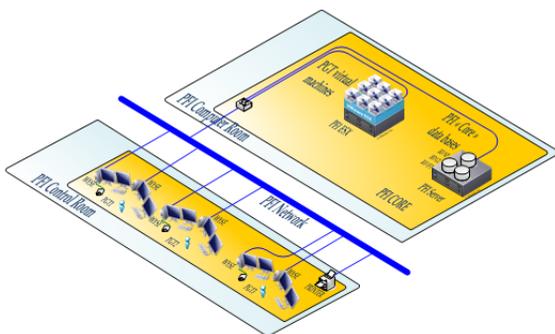


Figure 4: Test Campaigns Management Tool hardware architecture.

* Virtual Routing Forwarding. On the PFI we have defined three test contexts based on the VRF principles. It allows us to conduct simultaneously tests on three Subsystems control system avoiding coactivity problems.

The Bug Management Tool (FFT) and its Main Functions

The Bug management Tool is a specifically configured JIRA© of the Atlassian® company. This product allows defining workflows for bug tracking or, more generally, any kind of data. The bugs are stored in a database called BDFFT.

Each Subsystem is considered as a JIRA© project. Each discovered bug is analyzed and sent, if necessary, to the contractors. A specific module, based on the discovered bugs and the duration of the tests conducted with the PGT, has been added to calculate each subsystem reliability.

One of the goals of the PFI is to compute the expected ICCS reliability improvement between the beginning of PFI tests and the end of the PFI commissioning.

We can access the FFT from any computer of the PFI control room and we also have two dedicated workstations to access this tool and prepare specific reports using JIRA© reporting functions. (Fig. 5)

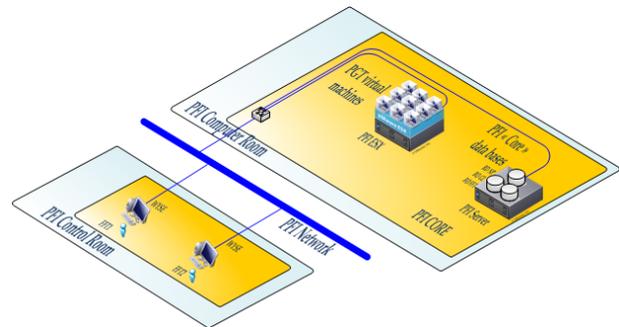


Figure 5: The Bug management Tool hardware architecture.

The Simulator Hardware Platform (PHS) and its Main Functions

A hardware platform has been defined to be able to install the simulators delivered by the several contractors as virtual machines. This allows us to have a standardization of the hardware used on the Integration Platform and therefore ease the maintaining and increase the availability of the Platform. During the integration phase each subsystem simulators has a dedicated hardware configuration but in a few years the simulator platform servers will be totally pooled between all the subsystems. The Platform is composed of 24 servers: R415, R515 and R715 Dell® computers (Fig. 6).

As a part of this platform, we developed a commutation tool that dialogs with the Vcenter and makes it possible to move all the simulators of a subsystem from a test context to another according to the test configurations needed by the PGT.

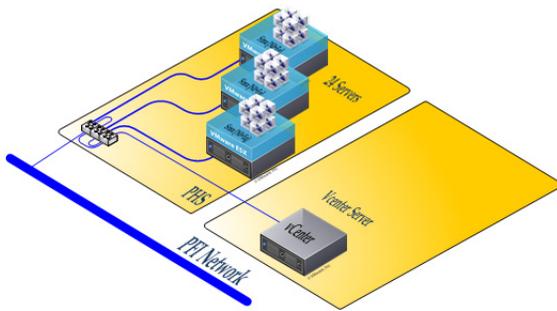


Figure 6: The PHS hardware architecture.

PFI ROADMAP

We received a first version of each laser control command subsystem (except PEPC which is scheduled oct. 2013).

We are currently integrating these control command with the high level supervisory: each interface is being tested.

We have delivered on the LMJ the first control command subsystem: laser diagnostics.

We are about to complete the first three shot sequence development (end of 2013) that will be used to start the global commissioning process for the laser part of the ICCS in Feb. 2014.

REFERENCES

- [1] J.-P. Arnoul, F. Signol, J. Nicoloso, "Laser Megajoule Facility (L.M.J.) Control system status report", ICALEPCS 2011, October 2011.
- [2] J.-C. Picon, F. Signol, P. Bétrémieux, J.-J. Dupas, J. Nicoloso " Strategy for the Integration of the LMJ (Laser Megajoule) control system", ICALEPCS 2009, October 2009.