23rd IEEE-NPSS Real Time Conference 1-5 August 2022

Verification and Validation of ITER Interlock System Fast Architecture according to IEC 61508 standard

I. García-Siguero[1], A. Carpeño[1], E. Barrera[1] , D. Karkinsky[2] , Ignacio-Prieto Diaz[3], and A. Marqueta[2]

[1]Instrumentation and Applied Acoustic Research Group (I2A2), Universidad Politécnica de Madrid, Madrid, Spain; [2]ITER Organization, St. Paul-lez-Durance, 13067 France; [3]F4E, Torres Diagonal Litoral Edificio B3, C/ Josep Pla 2, 08019 Barcelona, Spain.

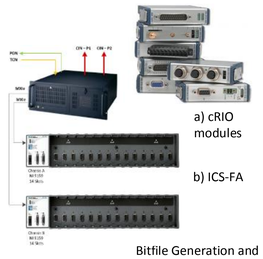
Email: i.gsiguero@i2a2.upm.es

Abstract

The ITER Interlock Control System (ICS) requires the application of the IEC 61508 standard for all mission-critical (known as investment protection) control functions. Such functions must detect the events of the integrated physical processes and distribute them to the actuators with hard real-time constraints on the order of milliseconds or even microseconds. Systems able to achieve these timing requirements are often bespoke FPGA-based solutions, which are a well-known challenge to IEC 61508 processes. However, to minimize the variety of components and simplify the procurement process for an international supplier base, ITER decided to standardize the use of Commercial Off-The-Shelf (COTS) devices. The COTS selected for the ICS was the FPGA-based CompactRIO NI 9159 chassis (and several adapter I/O modules), provided by National Instruments (NI). This COTS requires the use of a high-level language (LabVIEW-FPGA) and the associated integrated development tools to develop the FPGA functionality. Therefore, it is necessary to ensure the required assurance that a COTS device is of enough quality, fit for purpose, and can be properly integrated into an investment protection control loop with the necessary level of systematic capability during the development process. This paper describes in detail the method ITER uses to perform the verification and validation process, according to the IEC 61508 standard recommendations, of the logic configuration generated by the LabVIEW-FPGA for the FPGA inside these COTS, after the compilation of high-level language sources designed during the development.

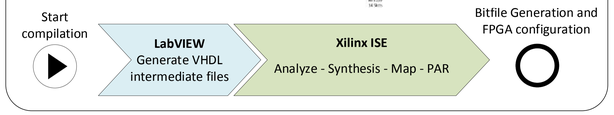
1. ITER Interlock Fast Architecture

- Interlock action signals <100 µs following an interlock event
- Integrity Level equivalent to SIL3 – IEC 61508
- FPGA-based COTS CompactRIO NI 9159 and its pluggable modules
- Fast Architecture based on "Double-Decker" solution
- LabVIEW FPGA programming tool



a) cRIO modules

b) ICS-FA

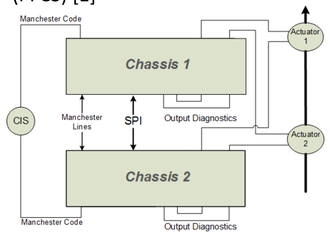


2. Current V&V approach

The application of the IEC 61508 standard for this system must be made carefully because it is not fully adappted to this solutions. The standard offers compliance directives for E/E/PE system developed with HDL, not for graphical languages as LabVIEW. LabVIEW generate a VHDL code but it is not accesible by the user. For this reason, ITER formalized a category 2 chit and subsequently transitioned into ITER risk. Afterward, ITER started the investigation of the feasibility of applying the IEC 61508 standard to ICS-FA developed by LabVIEW FPGA tool.

3. Research Done

- Selected previous developed PIS (PFCS) [1]



PFCS PIS-FA

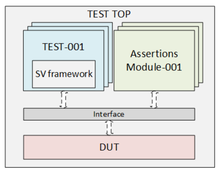
- Preliminary V&V plan based on the V-model
- Annex-B and Annex-F of IEC 61508 as reference

Item Group	A	NA	NS
P. Management	2	0	0
Design A & Doc	10	0	0
Tools compliance	6	4	1
Semi-formal	7	0	0
Formal	5	2	4
Simulations	8	2	0

A = Applicable
NA = Not Applicable
NS = Non Selected

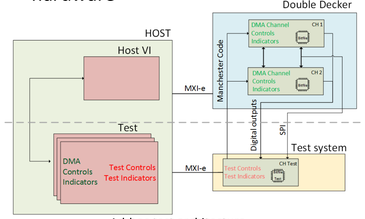
- Replicate the FPGA configuration bitstream autogenerated by LabVIEW using only Xilinx ISE
- Formal analysis of constraints file
- Study of VHDL autogenerated code architecture
  - Clock and reset domains
  - Synchronization mechanisms
  - Finite State Machines
  - Encrypted VHDL
  - Xilinx Advisory compliance
  - Hierarchical structure os CompactRIO code

- Coding guidelines by DesignChecker tool
- Design Rule Check by Xilinx ISE
- Static Timing Analysis by TRACE (Xilinx ISE)
- Verification unit simulations
  - Questa Advanced Simulator
  - System Verilog



Testbench architecture

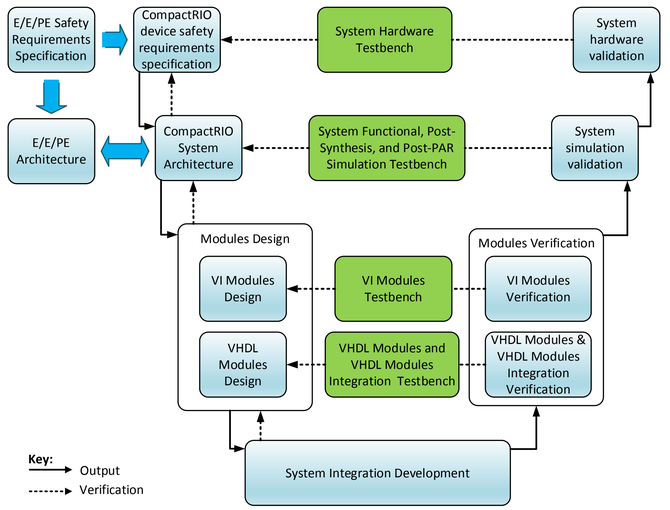
- Validation simulations
  - Simulation of the complete system
- Ad-hoc test system over the real hardware



Ad-hoc test architecture

- Study of the probability of SEU affect the FPGA correct operation
- Feasibility of designing and integrating SEU detector and mitigator
- Feasibility to integrate ChipScope into CompactRIO
- Feasibility to control FPGA placement
- Feasibility to isolate a critical part in CompactRIO
- How to verify the isolated FPGA section

4. New V-model Proposed



5. Results

- CompactRIO Virtex-5 shows a nominal 165 FIT/Mb for the configuration cells
- CompactRIO Virtex-5 has 4,801 FIT or an MTBF of 23.8 years
- It is possible to develop and integrate an SEU detection and mitigation system.
- It is possible to integrate user-defined constraints that affect the placement of LabVIEW graphic code
- It is possible to isolate a user VHDL module from the rest of the LabVIEW logic
- It is possible to verify the correct isolation of an FPGA region by using the IVT
- The table summarizes all the cumulated information about all IEC61508-2 items. The items marked as "Partial" cannot be fully evaluated due to the lack of information about some NI internal components.

Item Group	Compliance	Partial	Non Compliance	Not Applicable
P. Management	1	0	1	0
Design A & Doc	7	1	0	2
Tools compliance	6	0	0	0
Semi-formal	6	0	1	0
Formal	3	1	0	1
Simulations	2	3	3	0

CONCLUSIONS

The main conclusion is the set of possibilities and limitations of the application of the Verification and Validation process according to the IEC 61508 standard on ITER ICS-FA.

- **V&V of the system has been possible with some limitations**
- **It has not been possible to cover all the items of the standard**
- **The effort required to understand, manage and implement this process is tremendously high**

Additionally:

- **Research demonstrated the necessity and possibility of integrating an SEU detection and mitigation**
- **It discovered how to control the placement of the FPGA and isolate a VHDL module**

REFERENCES

[1] E. Barrera et al., "Methodology for the deployment of ITER Fast Plant Interlock system. Use case: ITER Poloidal Field and Central Solenoid coil's power converter protection system," Fusion Engineering and Design, Volume 129, 2018, Pages 73-77, ISSN 0920-3796

ACKNOWLEDGEMENTS

This work was supported under grant PID2019-108377RB-C33 funded by MCIN/AEI/ 10.13039/501100011033