Implementation of ITER Fast Plant Interlock System Using FPGAs with cRIO

E. Barrera[1], M. Ruiz[1], A. Bustos[1], M. Afif[2], B. Radle[2], J. L. Fernandez-Hernando[3], I. Prieto[4], R. Pedica[5], J.M. Barcala[6], J.C. Oller[6], R. Castro[6]

[1]Instrumentation and Applied Acoustic Research Group. Technical University of Madrid, Spain; [2]National Instruments, Austin, Texas USA;
[3]ITER Organization, St. Paul-lez-Durance, 13067 France; [4]Iberdrola Ingeniería y Construcción S.A.U., Madrid, Spain;
[5]Vitrociset, SPA, Via Tiburtina, 1020 - 00156 Roma, Italy; [6]Asociación Euratom/CIEMAT para la Fusión, Madrid

Abstract– Interlocks are the instrumented functions of ITER that protect the machine against failures of the plant system components or incorrect machine operation. Regarding I&C, the Interlock Control System (ICS) ensures that no failure of the conventional ITER controls can lead to a serious damage of the machine integrity or availability. The ICS is in charge of the supervision and control of all the ITER components involved in the instrumented protection of the Tokamak and its auxiliary systems. It is constituted by the Central Interlock System (CIS), the different Plant Interlock Systems (PIS) and its networks. The ICS does not include the sensors and actuators of the plant systems but it is in charge of their control. The ITER interlock system shall be designed, built and operated according to the highest quality standards. The international standard IEC-61508 has been chosen as the reference. In both CIS and PIS cases two main architectures are used: a slow architecture, for those functions with response time requirements slower than 100ms (300 ms for central interlock functions), based on PLC technologies, and a fast architecture, based on FPGA technologies, for the functions with faster requirement times. The proposed design for fast PIS is based on the use of RIO (Reconfigurable Input/Output) technology from National Instruments (compactRIO platform). In order to provide a high integrity solution, a FMEDA (Failure Modes Effects and Diagnostics Analysis) has been conducted to analyze the components behavior. According to the output of the FMEDA a set of diagnostics has been defined and additional redundancy was added to the architecture to improve the integrity figures. The defined configuration has been called the "double-decker solution", with two chassis running in parallel, communicated between them using a synchronous high speed serial line, and using redundant modules to implement the input and output measurement/excitations and redundant analog and digital modules to implement the diagnostics of these input/output modules. The integrity figures for the "double decker" solution are obtained from the classification of the failure rates, obtaining for the different configurations a SFF (safe failure fraction) of 85% and a FPH (Probability of dangerous Failure per Hour) of less than 1E-07. The FPGA design includes all the hardware to support the data acquisition from the input modules, the implementation of the diagnostics functionalities for analog and digital modules, the voting schema and the activation/deactivation of digital outputs. The platform includes an external test platform, also based on compactRIO technology, to perform the validation of the system and to register the performance of the different interlock functions implemented. The response times obtained for the TTL input to TTL output interlock function ranges from 5μs to 20μs; for the analog input to TTL output the response time is in the range of 41 μs to 90 μs, and for interlock functions using 24V digital input to 24V digital output, the time can rise up to 643 μs.

FAST INTERLOCK SYSTEM REQUIREMENTS

- Interlock action signals < 100 μs following an interlock event
- Overall availability > 99.9 %
- Reliability (over two, 8-hour shifts) > 99.6 %
- Integrity level (SIL3 equivalent – IEC 61508) PFH < 10^{-7}
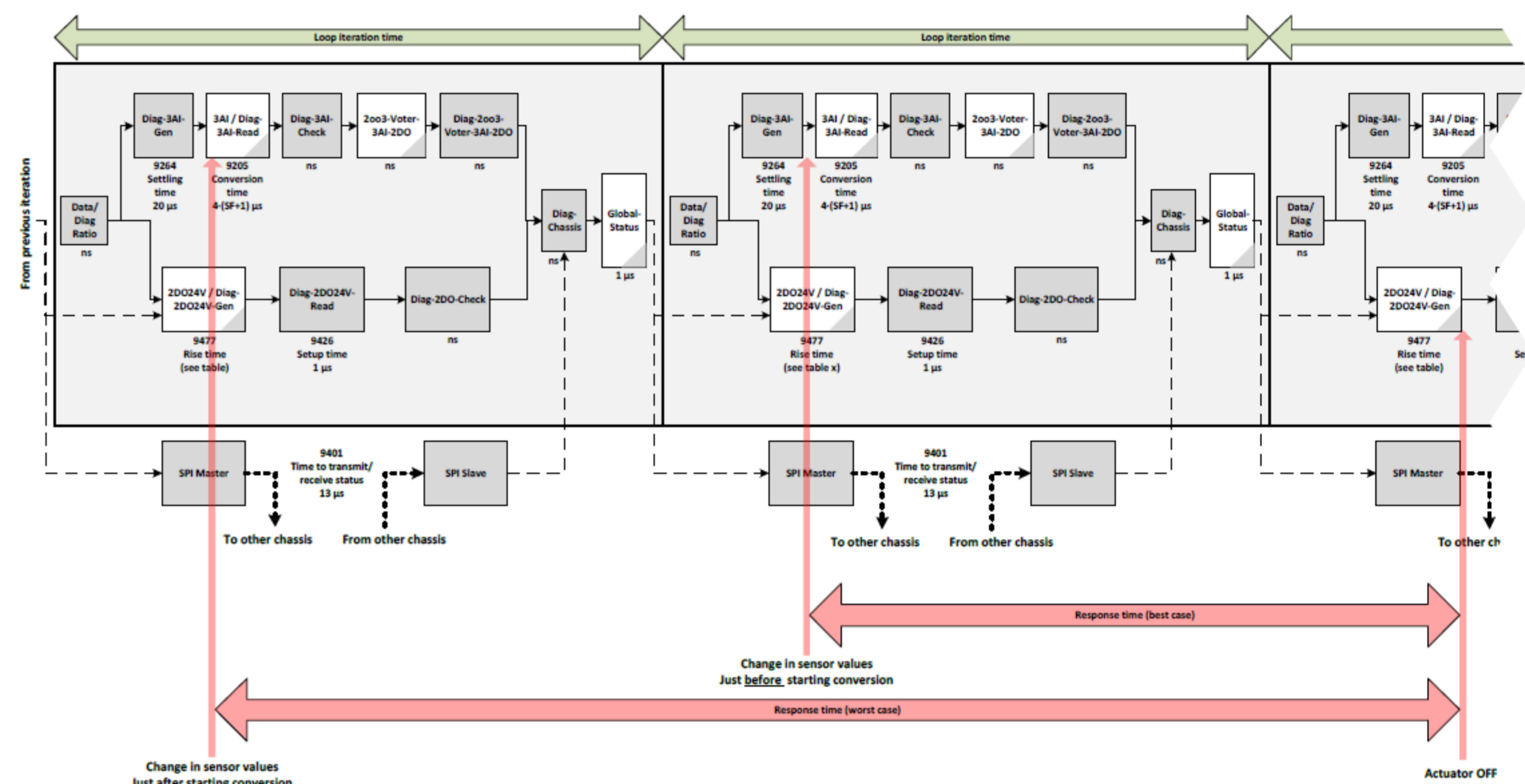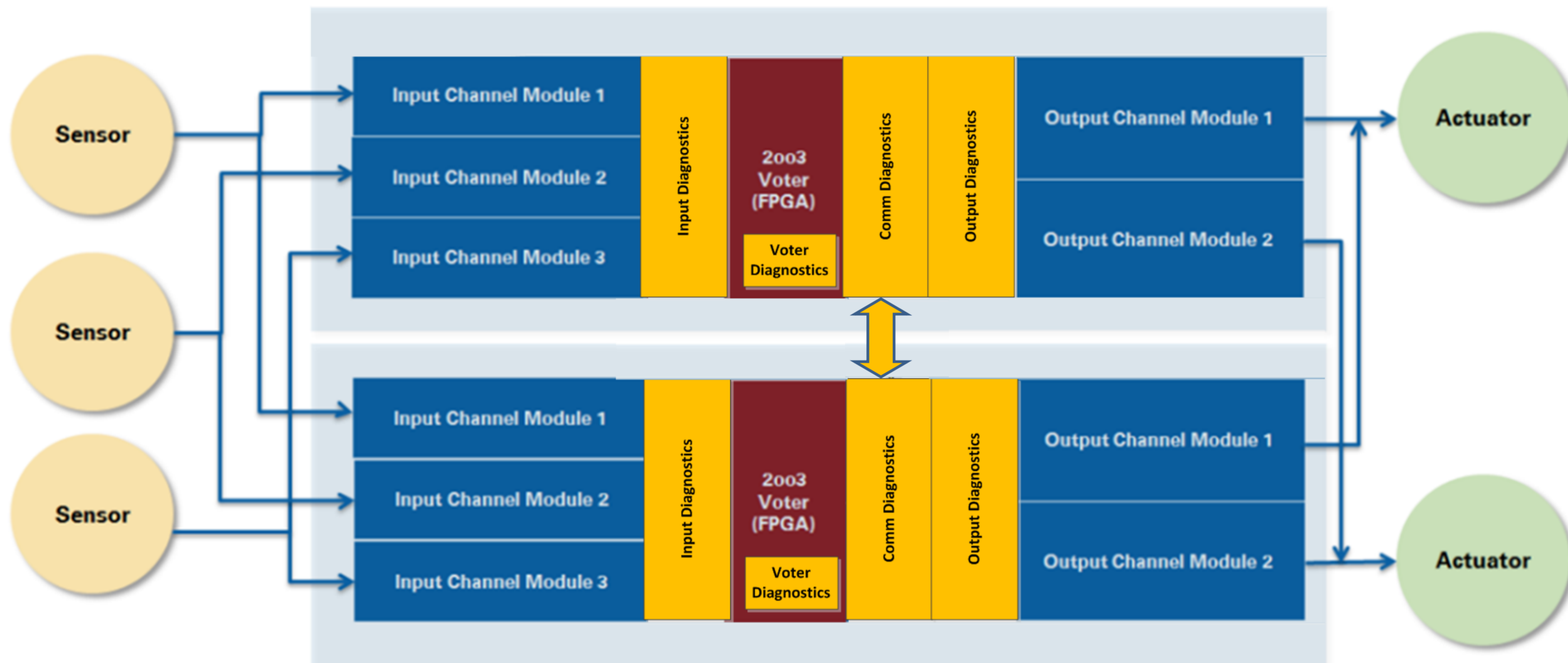- Fail safe solution (deterministic state in case of internal error)
- Harsh environment

Adopted solution:

NI CompactRIO - embedded
FPGA-based architecture
with hot-swappable
industrial I/O modules
Redundancy in I/O modules
Diagnostics modules
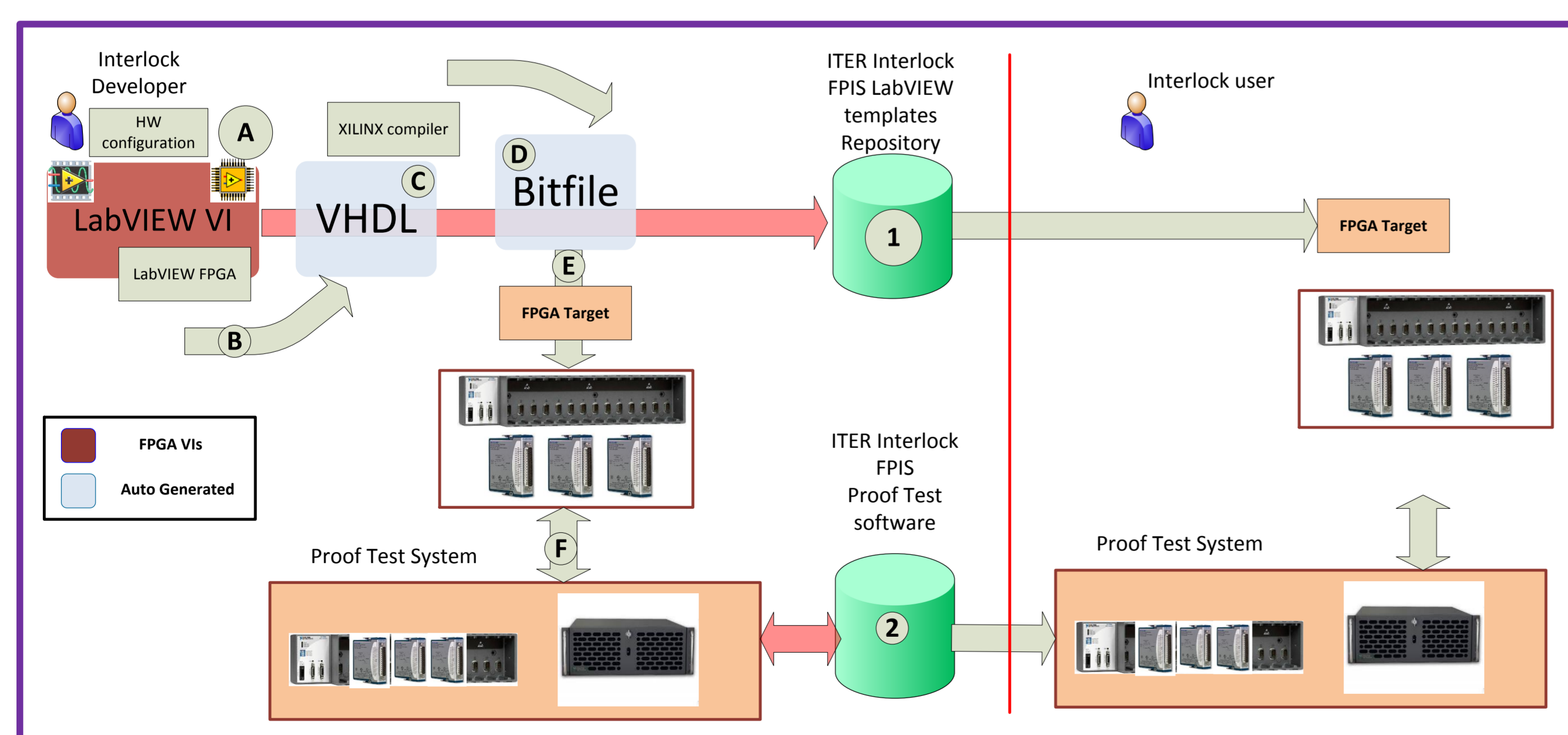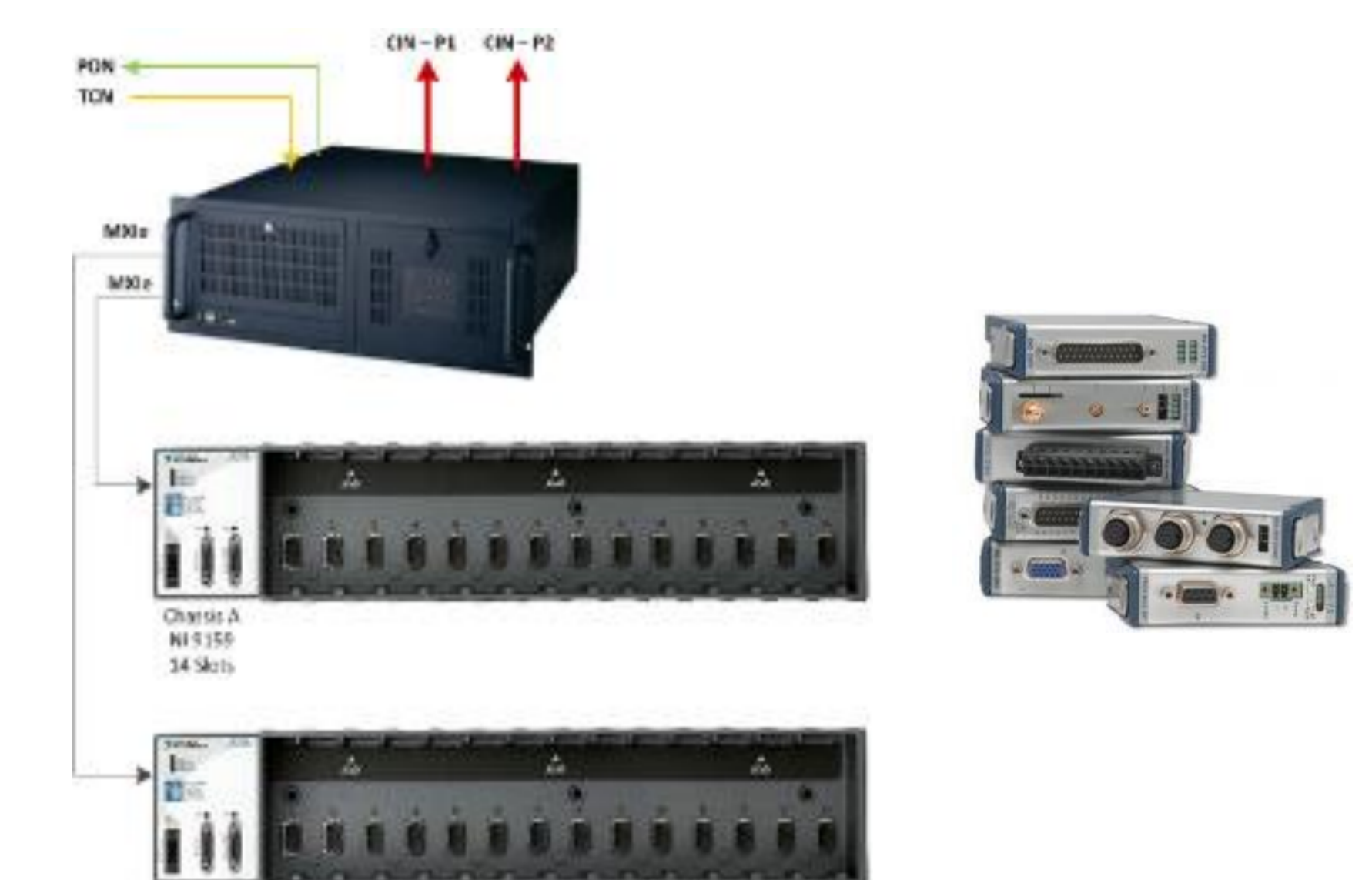2 chassis in a redundant configuration

Reconfigurable HW system

2oo3S Double Docker with Diagnostics

Results

Config.	Inputs	Outputs	SFF	PFH (17 months)	SIL consumption (IEC 61508)	# Safety Functions	Response time	Max. FPGA resources used
A	3 x AI	2 x 24V	85.47 %	1.324 E-8	13.2% of SIL 3	1 to 11	41 – 89 μs	49.9 %
B	3 x 24V	2 x 24V	85.47 %	1.322 E-8	13.2% of SIL 3	1 to 11	143 - 643 μs	32.0 %
C	3 x TTL	2 x TTL	85.47 %	1.597 E-8	16% of SIL 3	1 to 7	5 - 20 μs	32.5 %

SFF: Safe Failure Fraction
PFH: Probability of dangerous Failure per Hour (high demand system)
SIL: Signal Integrity Level

- ✓ NI 9159 14-slot CompactRIO chassis (Virtex-5 FPGA)
- ✓ NI 9205 analog input (AI) module; 32-Ch ±200 mV to ±10 V, 16-Bit, 250 kS/s
- ✓ NI 9264 analog output (AO) module; 16-Ch ±10 V, 16-Bit, 25 kS/s
- ✓ NI 9477 sourcing digital output (DO) module; 32-Ch 24 V, 8 μs, Sinking
- ✓ NI 9425 sinking digital input (DI) module; 32-Ch 24 V, 7 μs
- ✓ NI 9476 sourcing digital output (DO) module; 32-Ch 24 V, 500 μs
- ✓ NI 9426 sourcing digital input (DI) ; 32-Ch 24 V, 7 μs
- ✓ NI 9401 digital I/O (or DIO) module; 8-Ch, 5 V 7-Ch TTL high-speed bidirectional

Development cycle of FPIS apps:

Interlock users only need to retrieve bitfiles from Interlock repositories (preconfigured templates)

Conclusions

- ✓ Generic fast PIS controller solution
- ✓ Integrity figures estimated according to IEC 61508
- ✓ Preconfigured and tested templates/bitfiles (additional possible)
- ✓ Integration with the central system (critical and non critical comm.)
- ✓ First ITER real applications: Correction Coils (2015), Poloidal field coils, central solenoid and toroidal field coils power converters (2016)