ITER Central Interlock System

Fast Machine Protection ITER

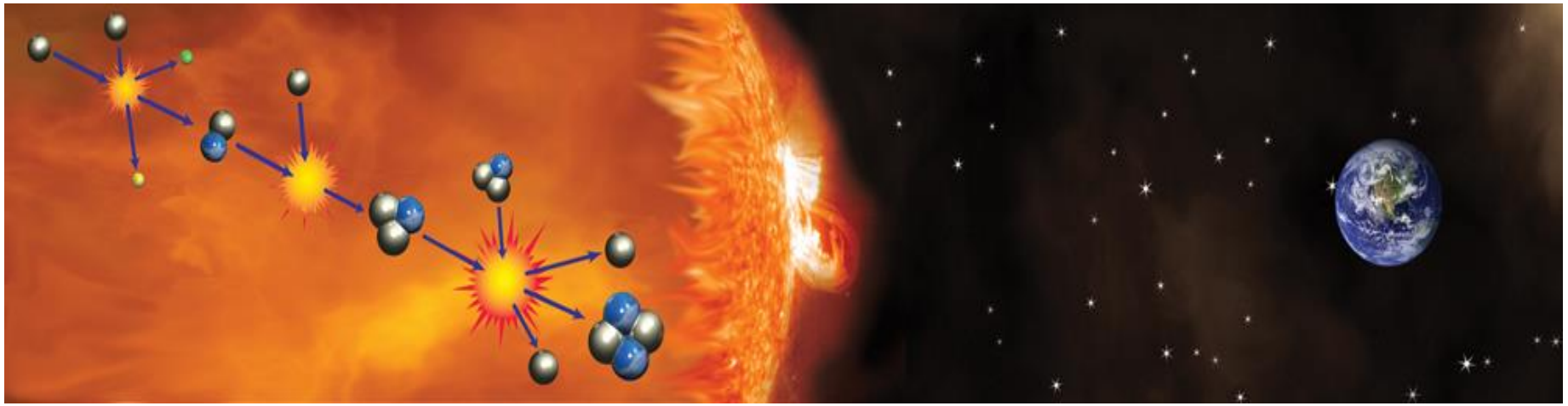
CIS Team

NI Big Physics Summit

February 2016

china eu india japan korea russia usa

the way to new energy…



Attractions:

- unlimited fuel
- no CO_2 or air pollution
- intrinsic safety
- no radioactive ash or long-lived nuclear waste,
- cost will be reasonable ***if*** **we can get it to work reliably**

Disadvantages:

not yet available

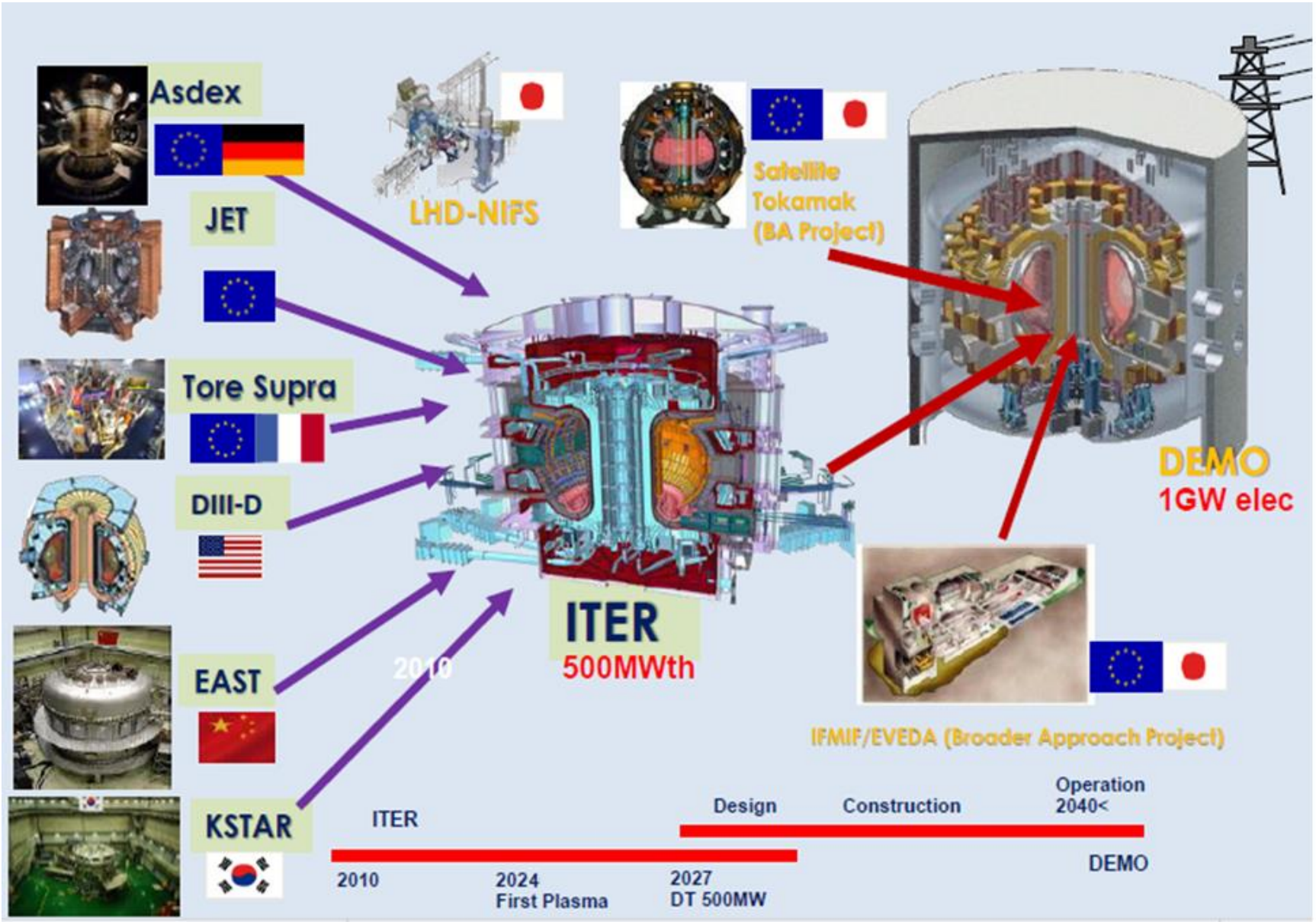
walls gets activated (but could recycle after 100 years)

"*For the benefit of mankind* "

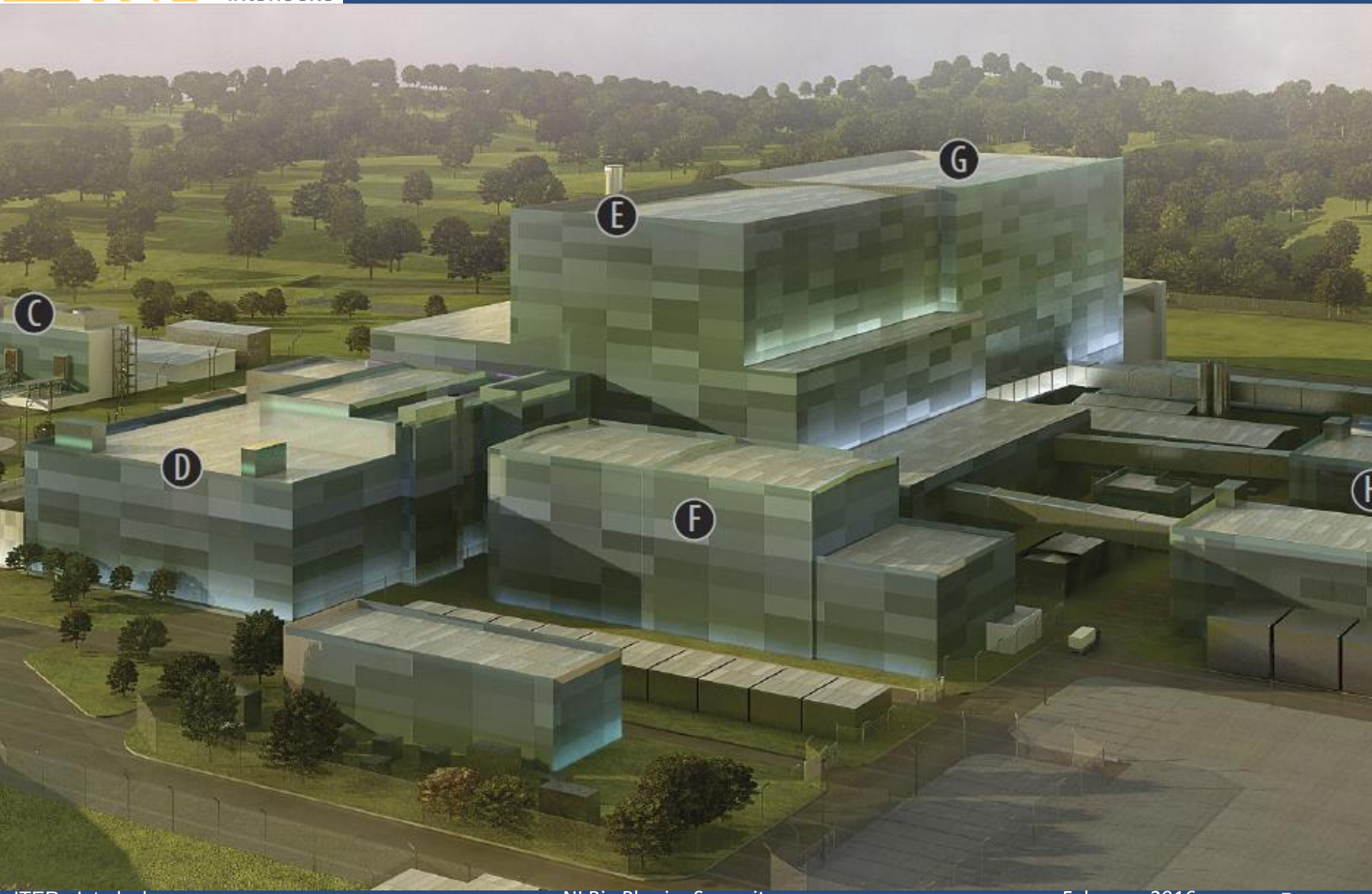
The idea for ITER originated from the Geneva Superpower Summit in 1985 where Presidents Gorbachev and Reagan proposed international effort to develop fusion energy…

…"*as an inexhaustible source of energy for the benefit of mankind*".

China, Europe, India, Japan, Korea, Russian Federation and the United States of America signed the ITER Agreement on 21 November 2006 in the Elysee Palace, Paris


Asdex
JET
Tore Supra
DIII-D
EAST
KSTAR
LHD-NIFS
Satellite Tokamak (BA Project)
ITER
500MWth
2010
DEMO
1GW elec
IFMIF/EVEDA (Broader Approach Project)
ITER
Design
Construction
Operation 2040<
DEMO
2010
2024 First Plasma
2027 DT 500MW

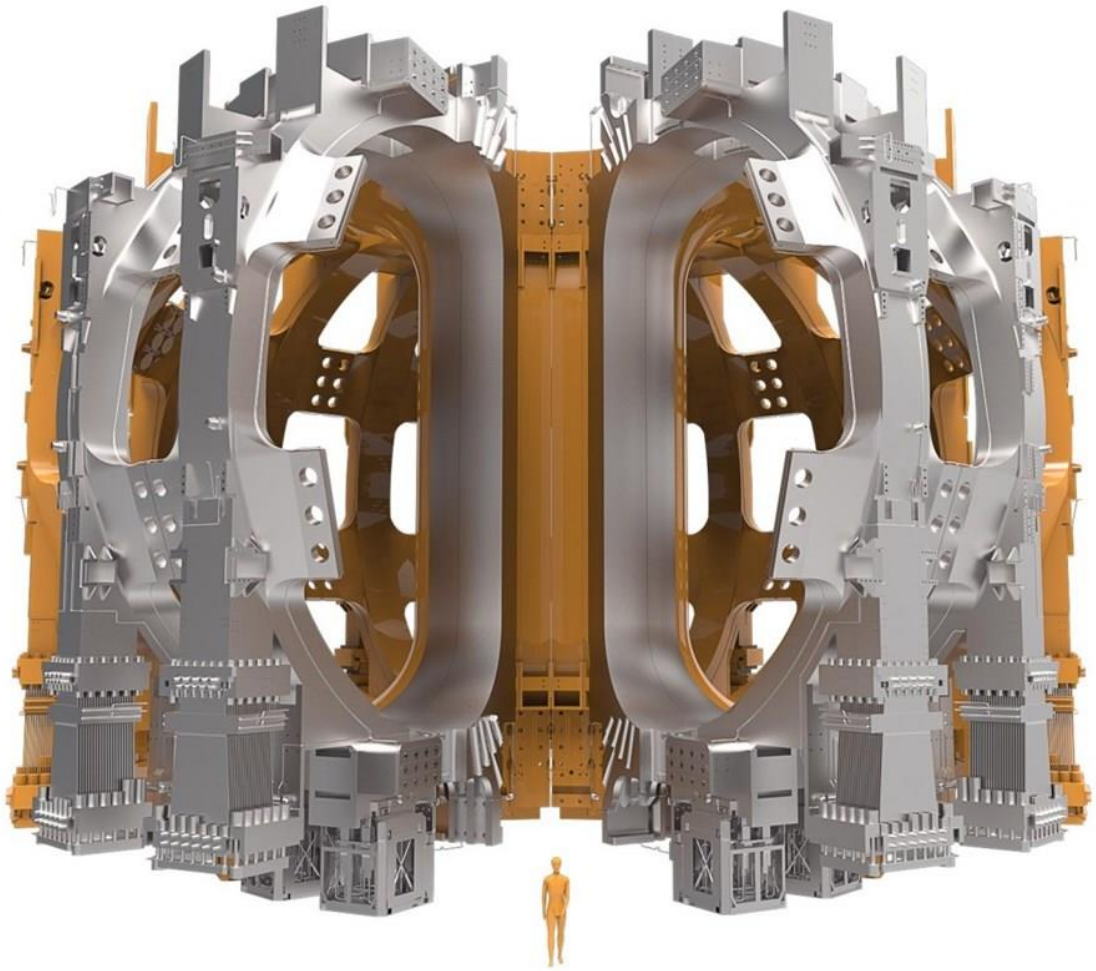
The ITER Domestic Agencies are responsible for implementing the procurement activities under each Member's responsibility


G
E
C
D
F

Main Sources of Risk at ITER

Sources of Risk at ITER

Superconducting Magnets

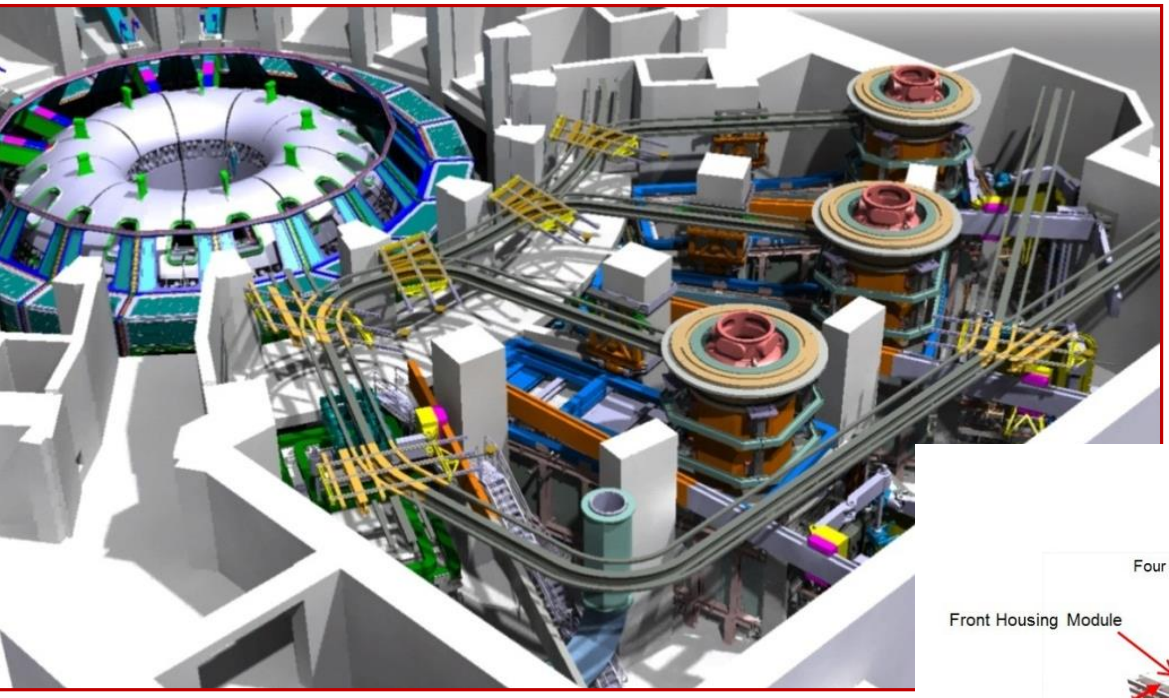


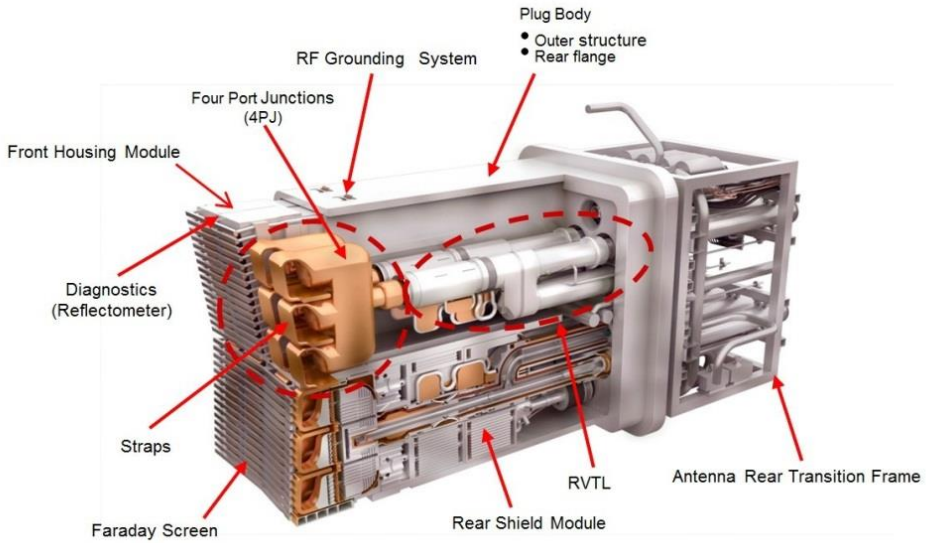
Interaction of strong magnetic fields
5T and up to 17 MA plasma

ITER Interlocks
@ITERinterlocks

Stopping an aircraft carrier at 150km/h in 500m?powering interlocks manage the same energy,51 GJ, to protect #ITER

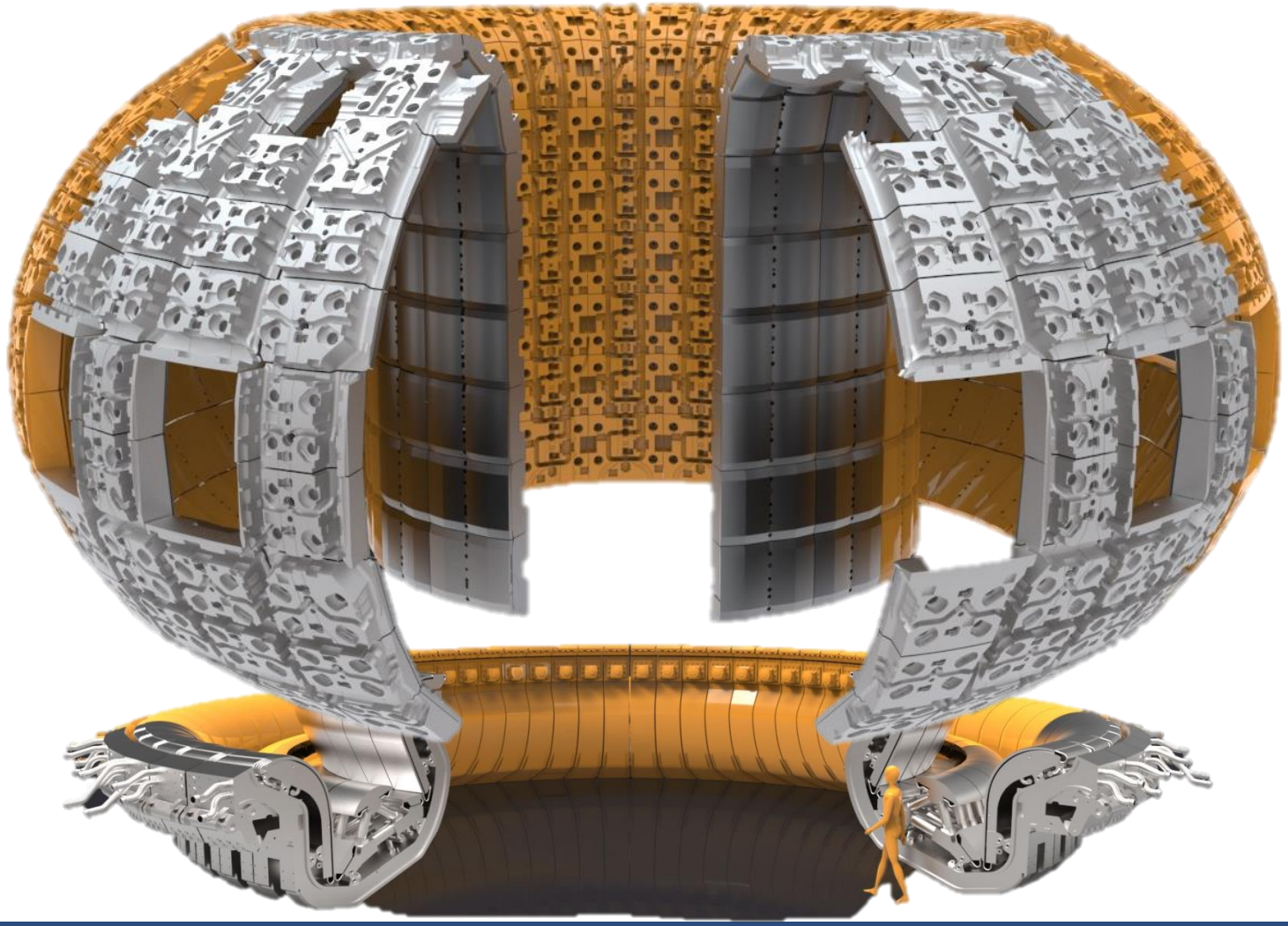
Plasma Heating & FuellingSystems





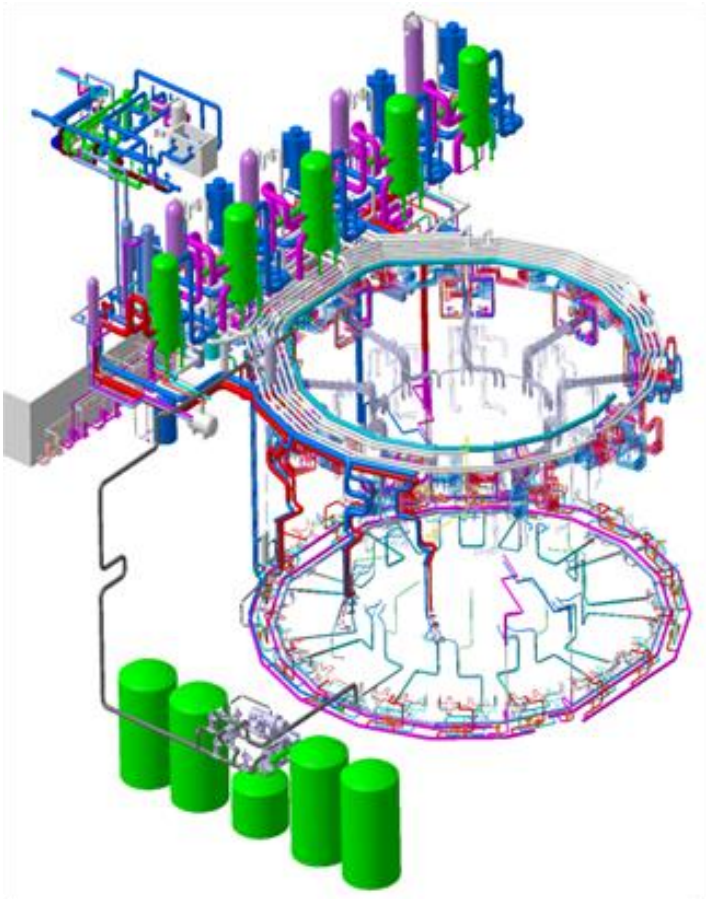
The Plasma

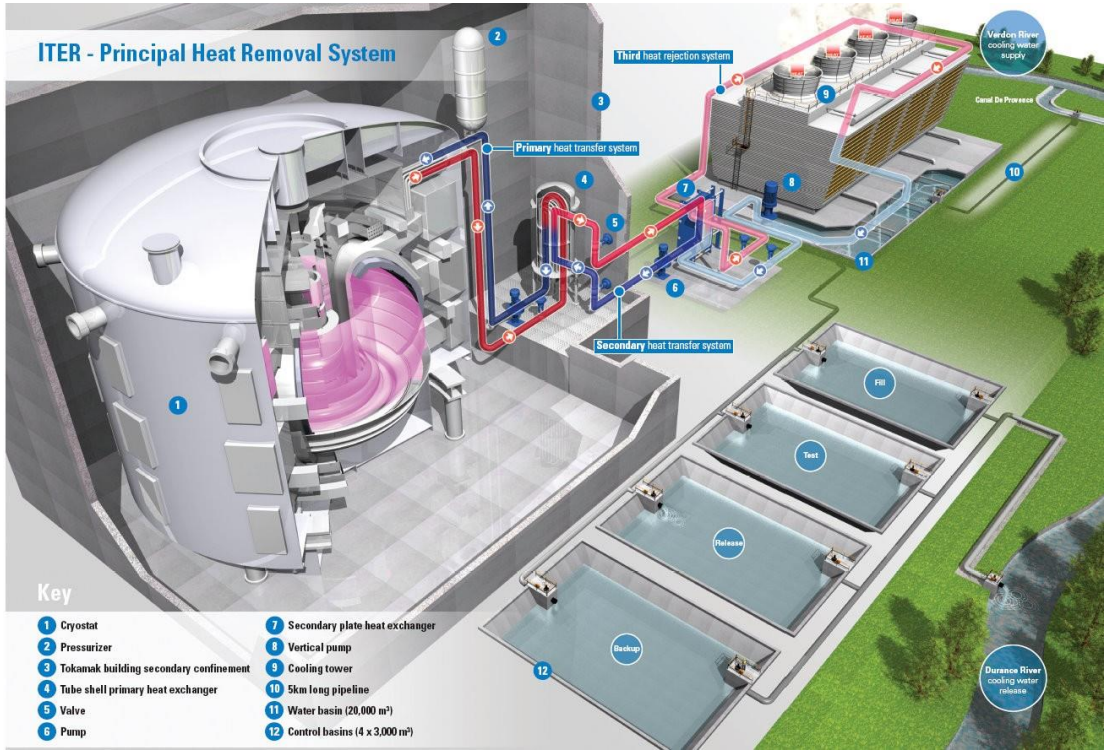
- Energy, Temperature – Internal Components



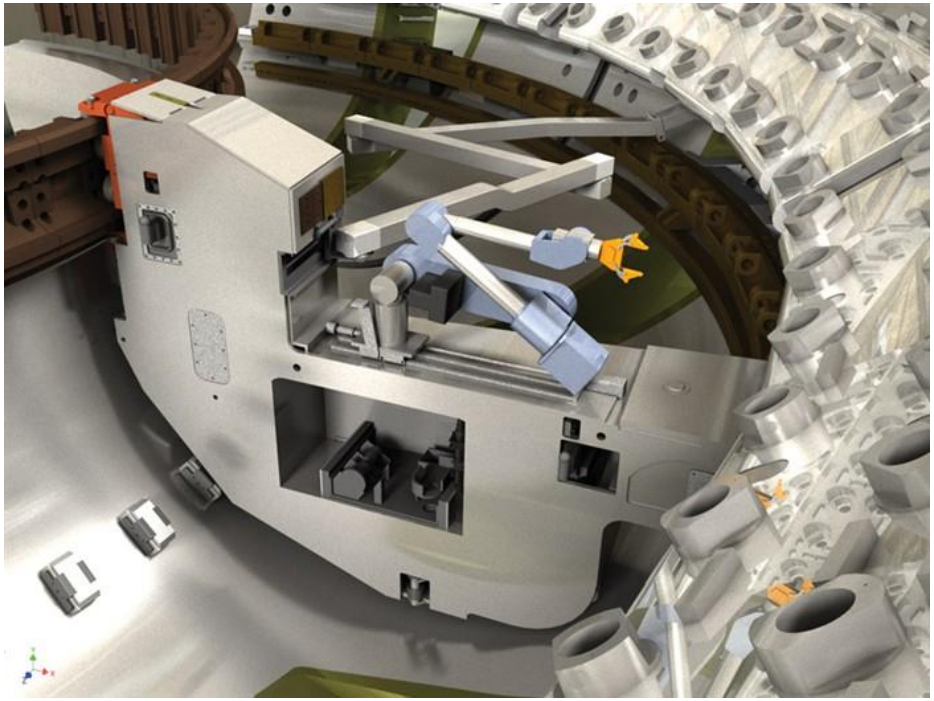
Plasma Disruptions

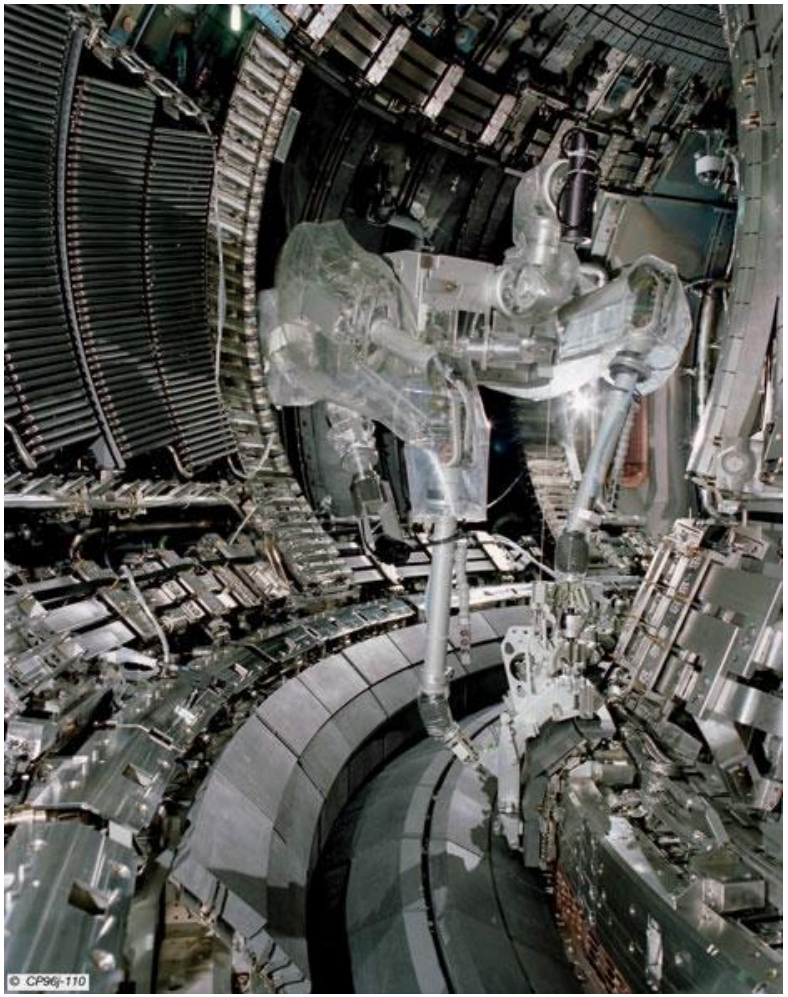
Vacuum, Cryogenic and Cooling Water Systems





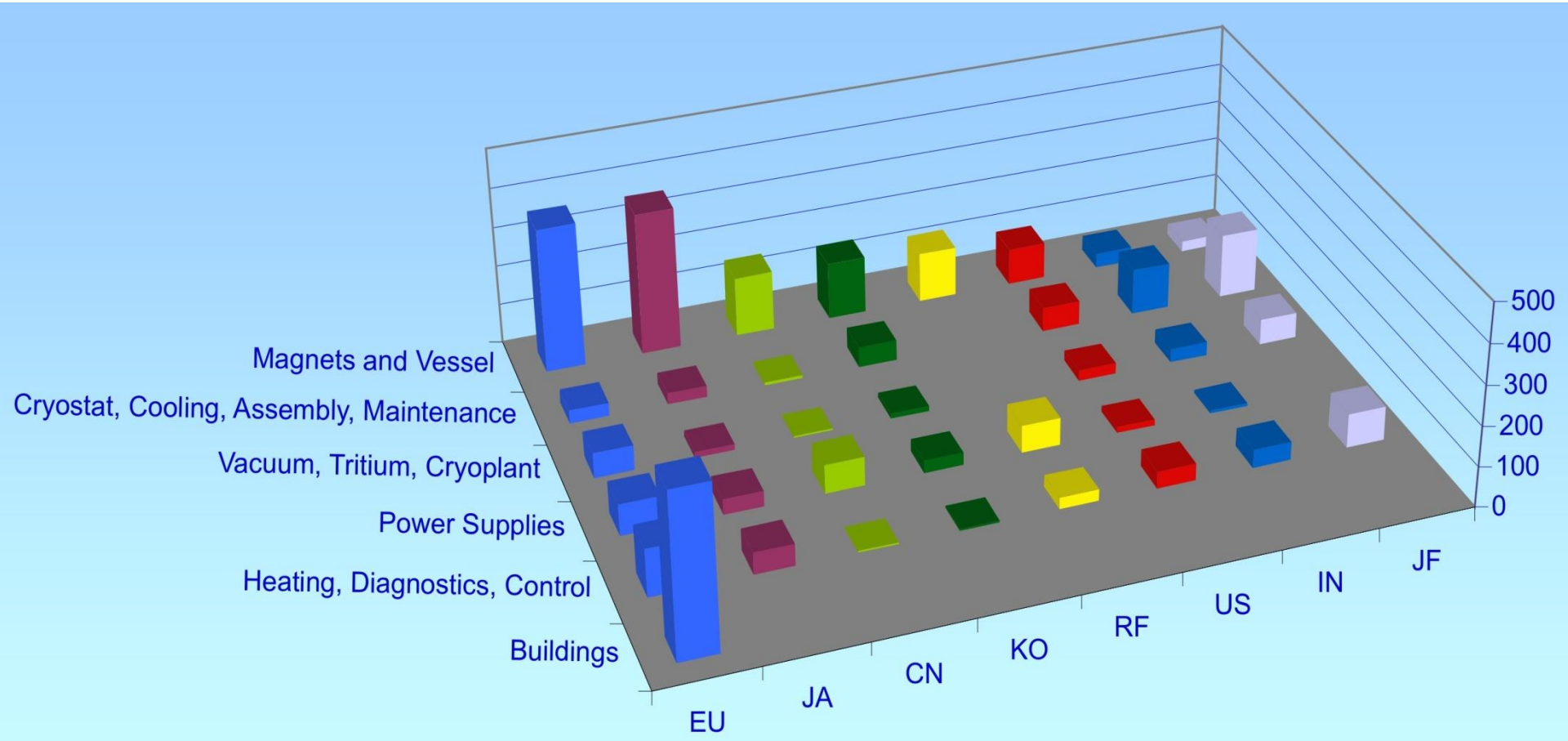
Remote Handling



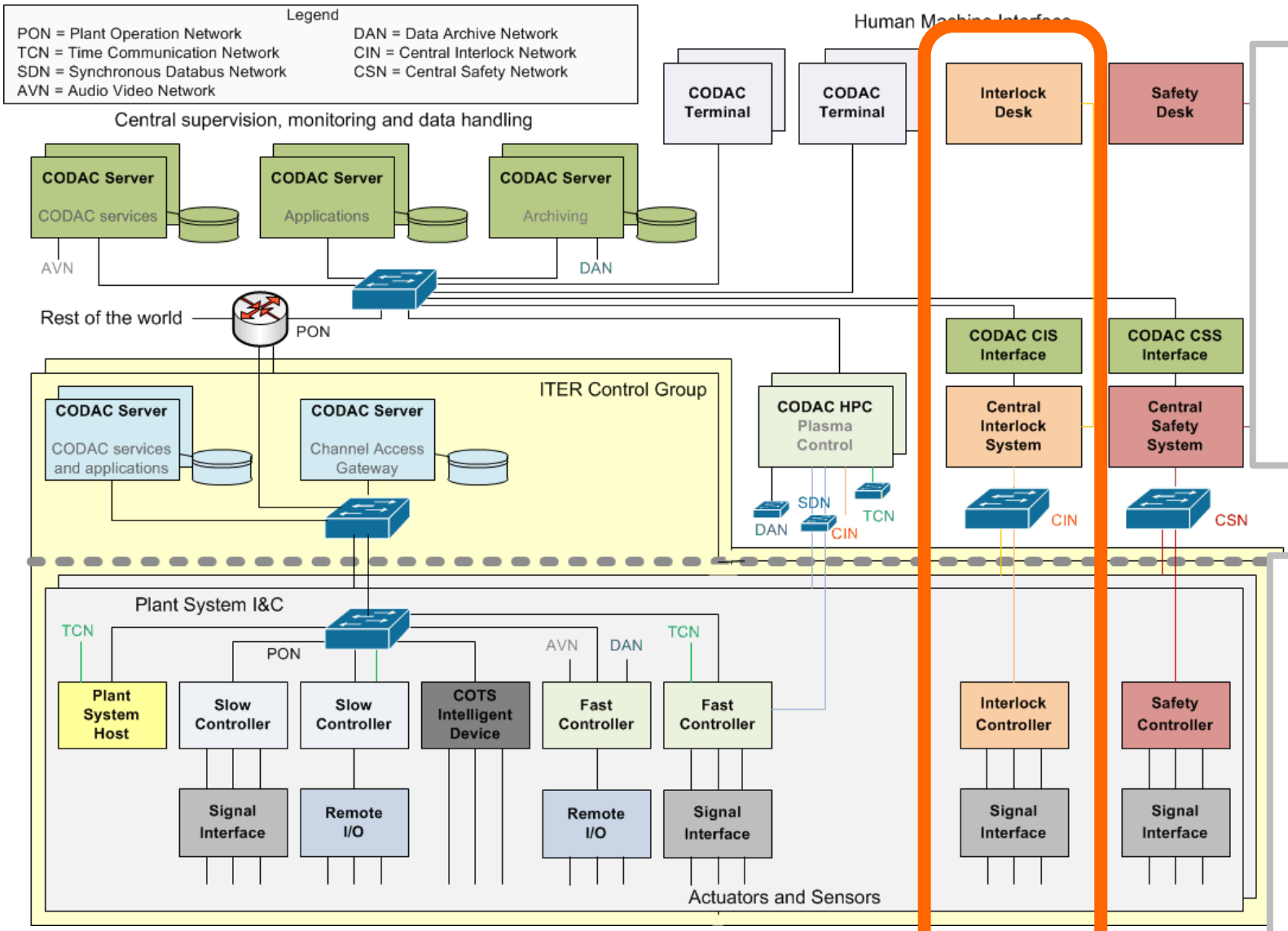


ITER Procurement Strategy

A unique feature of ITER is that almost all of the machine will be constructed through *in kind procurement* from the Members



In-fund and in-kind procurement



Interlocks at ITER

Interlocks at ITER

Future fusion power plants will be only possible if ITER proves that the reactor and associated systems can run **long plasma discharges reliably.**

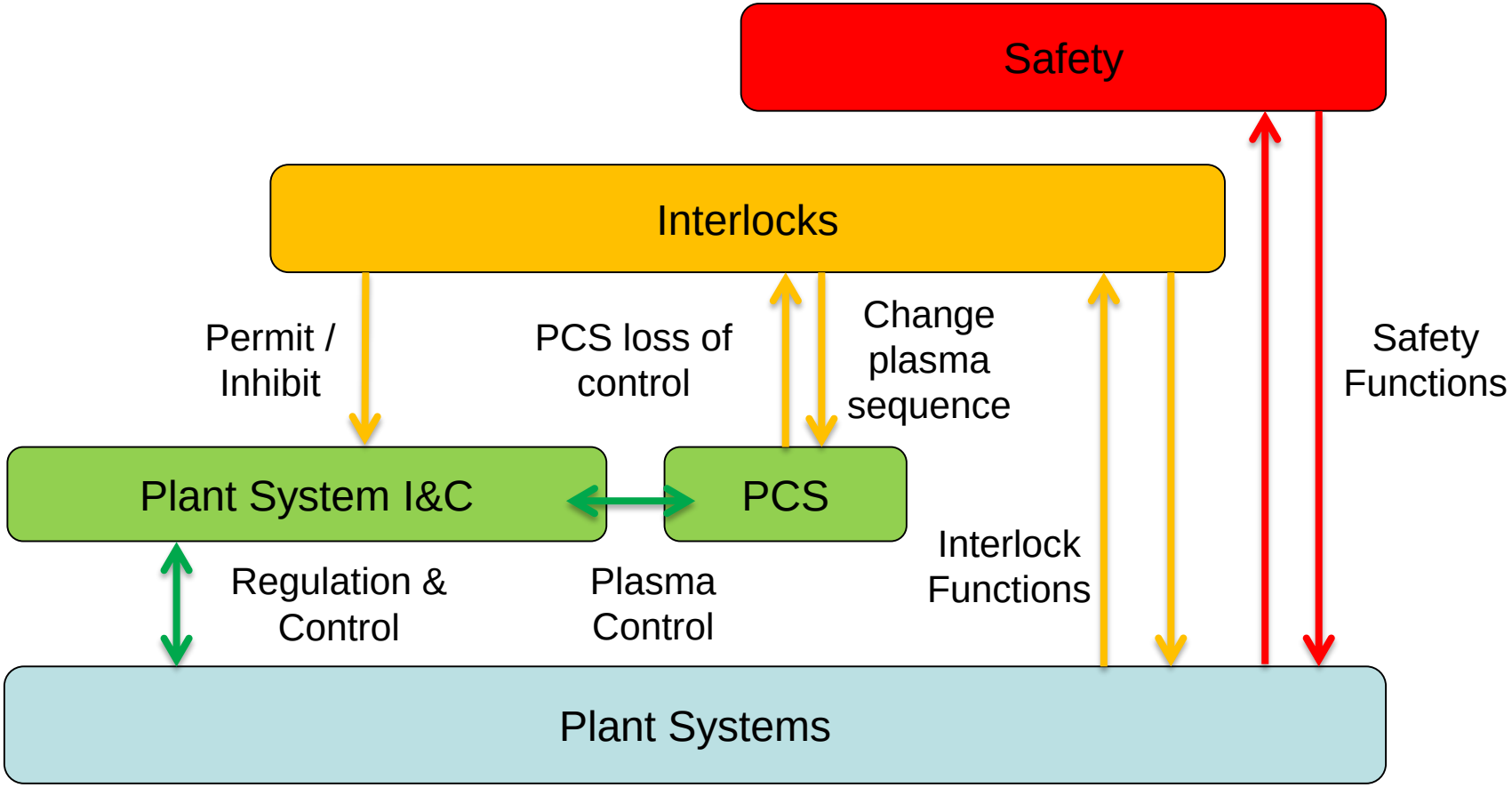
Interlocks are the instrumented functions of ITER that protect the machine against failures of the plant system components or incorrect machine operation.

Consequences

The ITER interlocks shall:

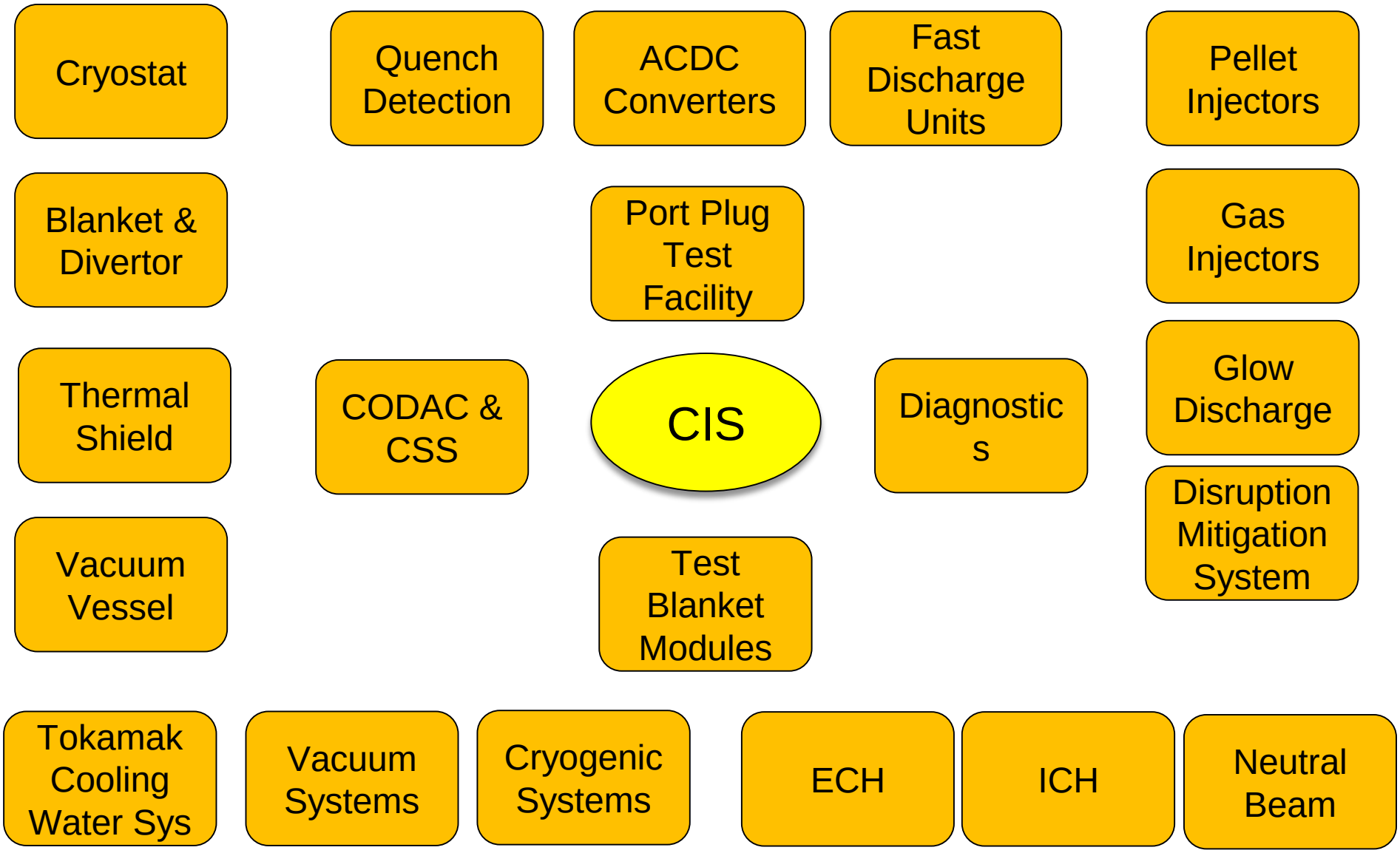
1. **Protect the tokamak integrity**
2. **Maximize scientific operation time**
3. **Anticipate and test interlock solutions for future industrial fusion reactors**

ITER Defense-in-depth Approach

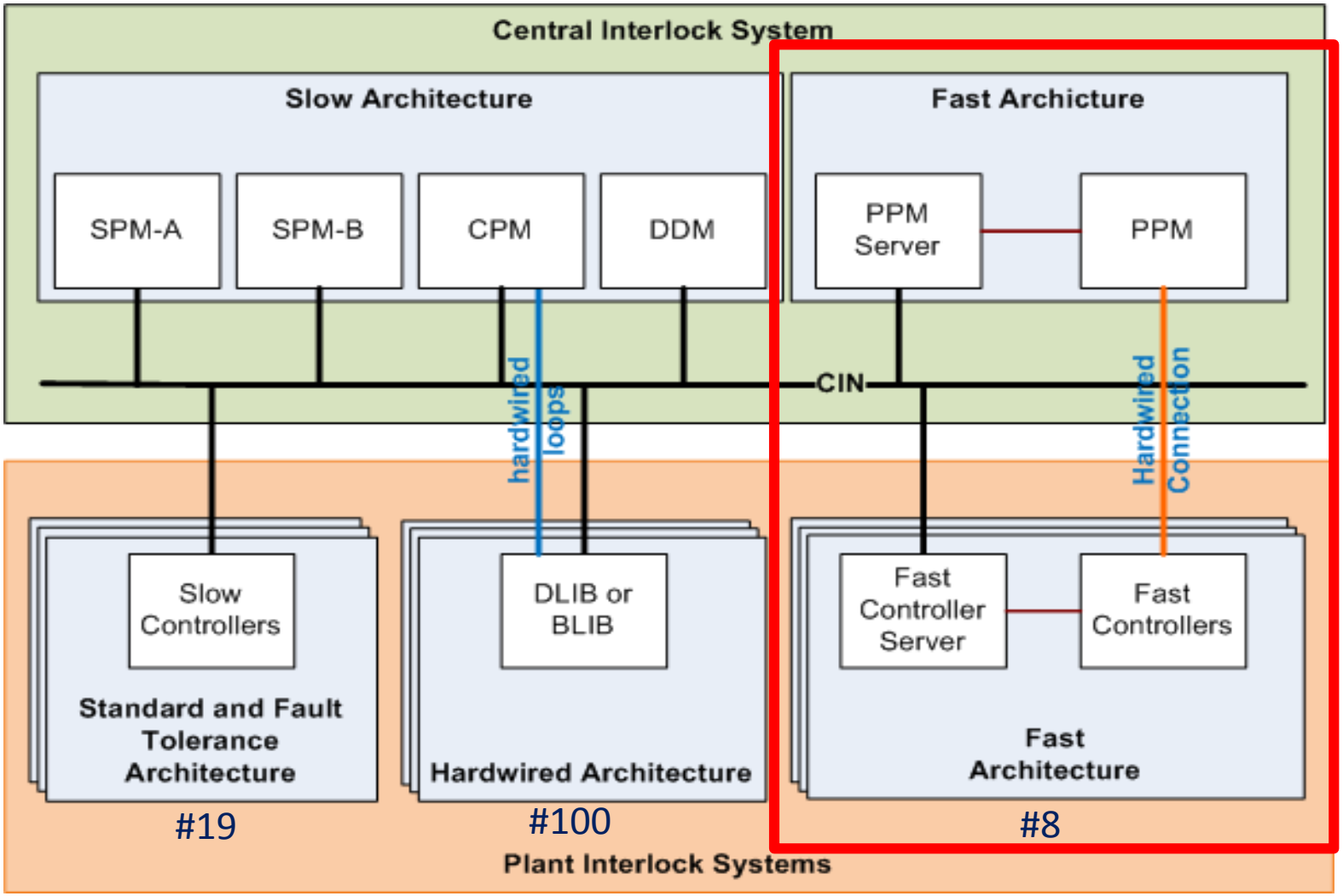


The Interlock Control System ensures that no failure of the conventional ITER controls can lead to a serious damage of the machine integrity or availability.

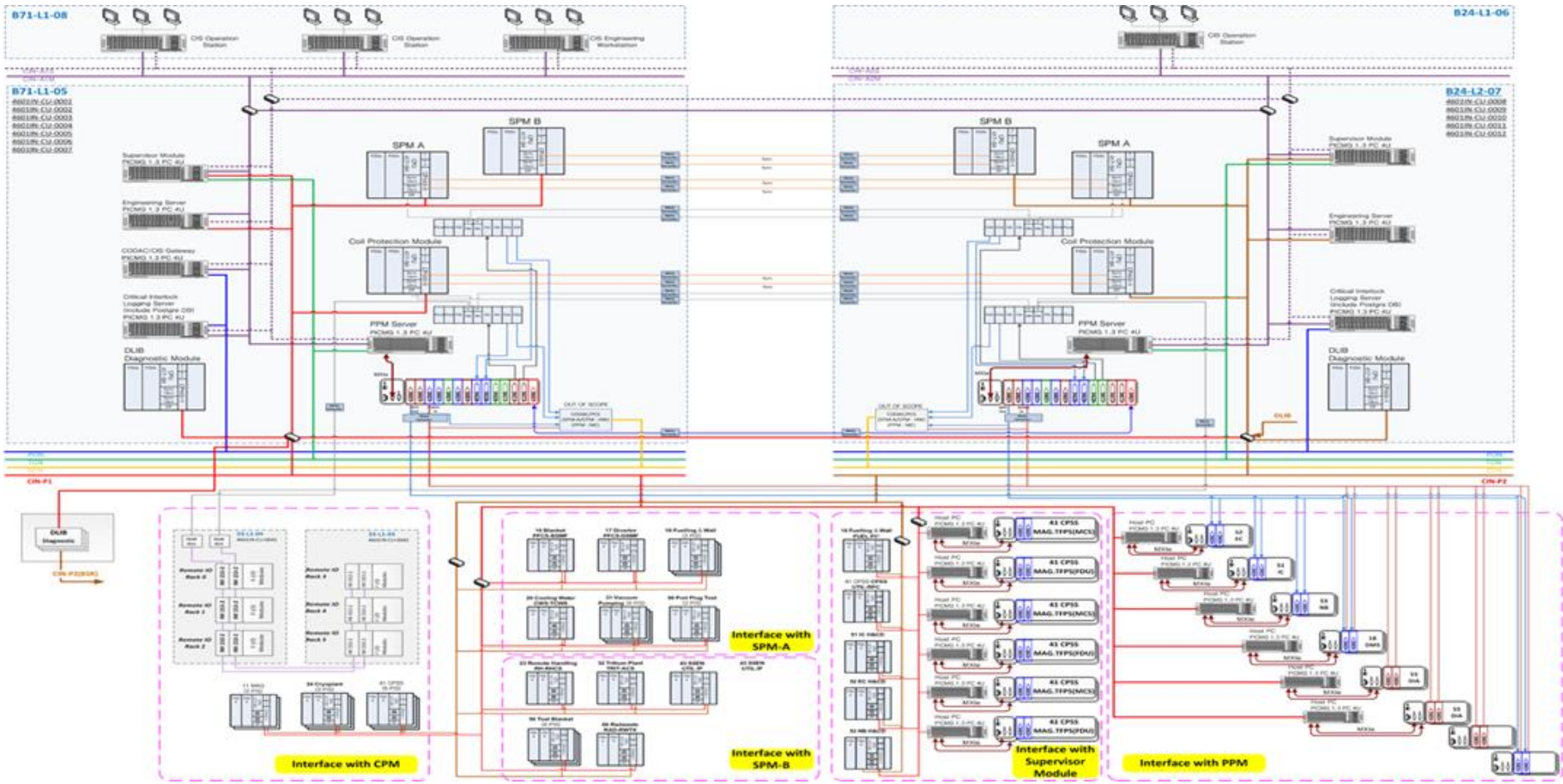
Central Interlocks: Plant Systems



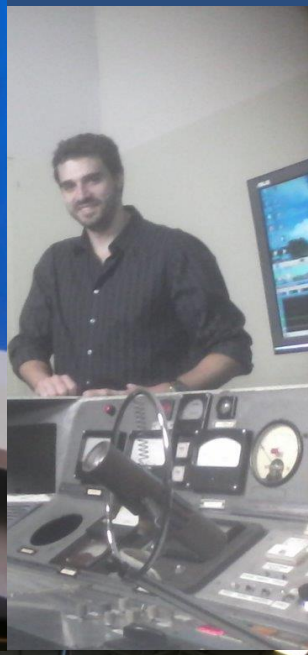
The CIS


Central Interlock System
Slow Architecture
Fast Archicture
SPM-A
SPM-B
CPM
DDM
PPM Server
PPM
CIN
hardwired loops
Hardwired Connection
Slow Controllers
Standard and Fault Tolerance Architecture
#19
DLIB or BLIB
Hardwired Architecture
#100
Fast Controller Server
Fast Controllers
Fast Architecture
#8
Plant Interlock Systems

ICS – Complex architecture



Domestic Agencies



How to integrate the most complex machine ever?Communication is the Key! a good interface to soften problems #ITER

ITER Interlocks
@ITERinterlocks

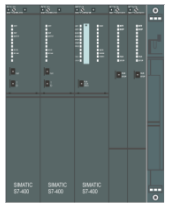
Fast Machine Protection

PIS Controllers

Integrity	Performance	Availability	Technical Solution	Configuration
Up to 3IL-3	> 100ms	Standard	Siemens S7-400-F	Standard PIS
Up to 3IL-3	> 100ms	High Availability	Siemens S7-400-FH	Fully Fault-Tolerance
Up to 3IL-3*	< 100ms	???	???	???

Siemens S7-400-FH

Single CPU



CPU + 2 CP

Fully Fault-Tolerance

Red CPU + CP

If the mitigation of the event requires an active coordination of the actions.

No COTS meets the requirements

Requirements

Some central interlock functions require a response time which cannot be implemented by the chosen PLC architecture.

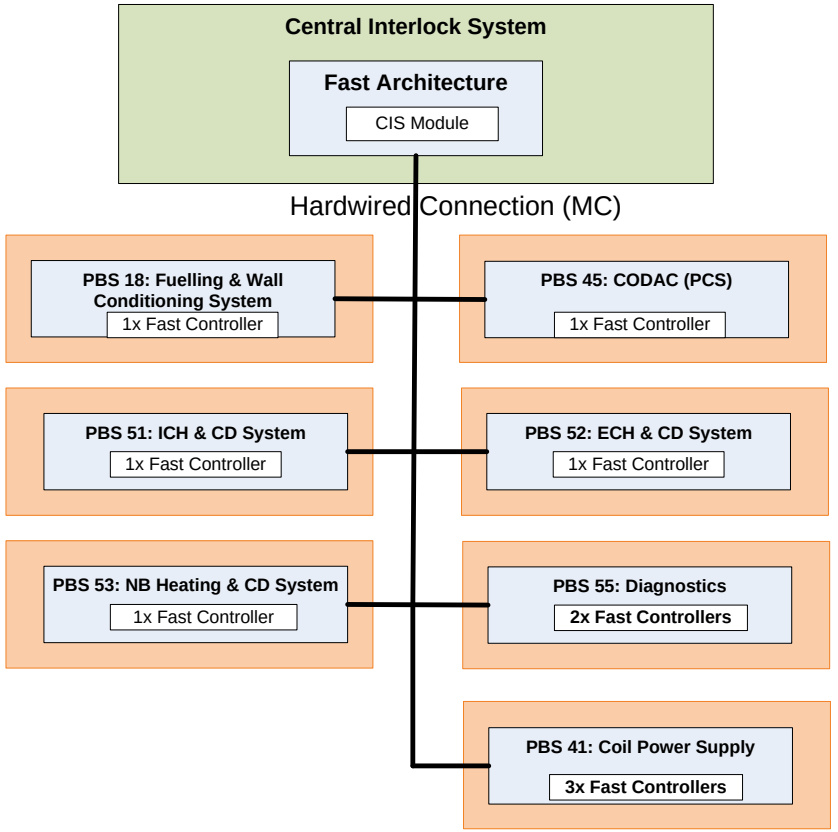
Fast Local functions

Standardized architecture
Standard sensors
Custom electronics

Central functions

Flexible solution
Fiber Optics Comm.

- **Response time below 1ms**
- **Availability (99.9%)**
- **reliability (99,6% in 16h)**
- **Integrity level up to PFH < 10^{-7}**
- **Fail-safe solution**
- **Harsh environment**



Plant Interlock Systems
Fast architecture

Fast Interlock Controller

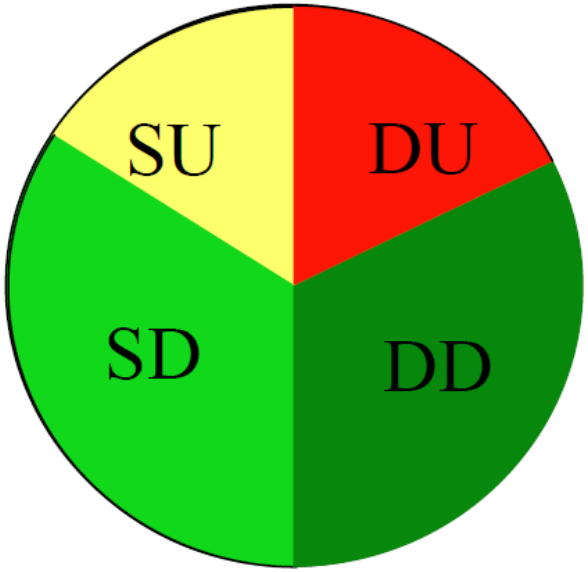
- Highly reliable and available
- Facilitate redundancy
- Magnetic and radiation environments.
- Requires different kinds of I/O :
  - 24 V digital signal
  - Accessible from the same FPGA
- Reaction time doesn't require extremely fast FPGA loops

NI Compact RIO

Category NI CompactRIO Product	MTBF @ 25 °C (Hours)
Controllers	
NI cRIO-9025	293 538
NI cRIO-9074	322 849
NI cRIO-9075	1 065 385
Chassis	
NI cRIO-9118	815 216
NI cRIO-9159	826 266
NI cIRO-9144	458 557
I/O Modules	
NI 9205	2 419 708
NI 9476	1 091 425
NI 9477	5 793 372
NI 9425	3 090 576
NI 9426	3 125 291
System	
NI cRIO-9159	556,746
NI 9205	
NI 9477	

Integrity

Hardware Integrity Architecture



IEC 61508

Total Failure rate λ

Safe Detected	Dangerous Detected
Safe Undetected	Dangerous Undetected

$$SFF = 1 - \frac{\lambda^{DU}}{\lambda^{TOTAL}}$$

IEC 61508 Part 2 Table 3

Architectural constrains on "complex" devices

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.

NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.

NOTE 3 See annex C for details of how to calculate safe failure fraction.

PFH Calculation

Failure Mode, Effects, and Diagnostics Analysis (FMEDA)

Classifies each failure mode discovered as:

- Dangerous or Safe
- Detectable or Undetectable.

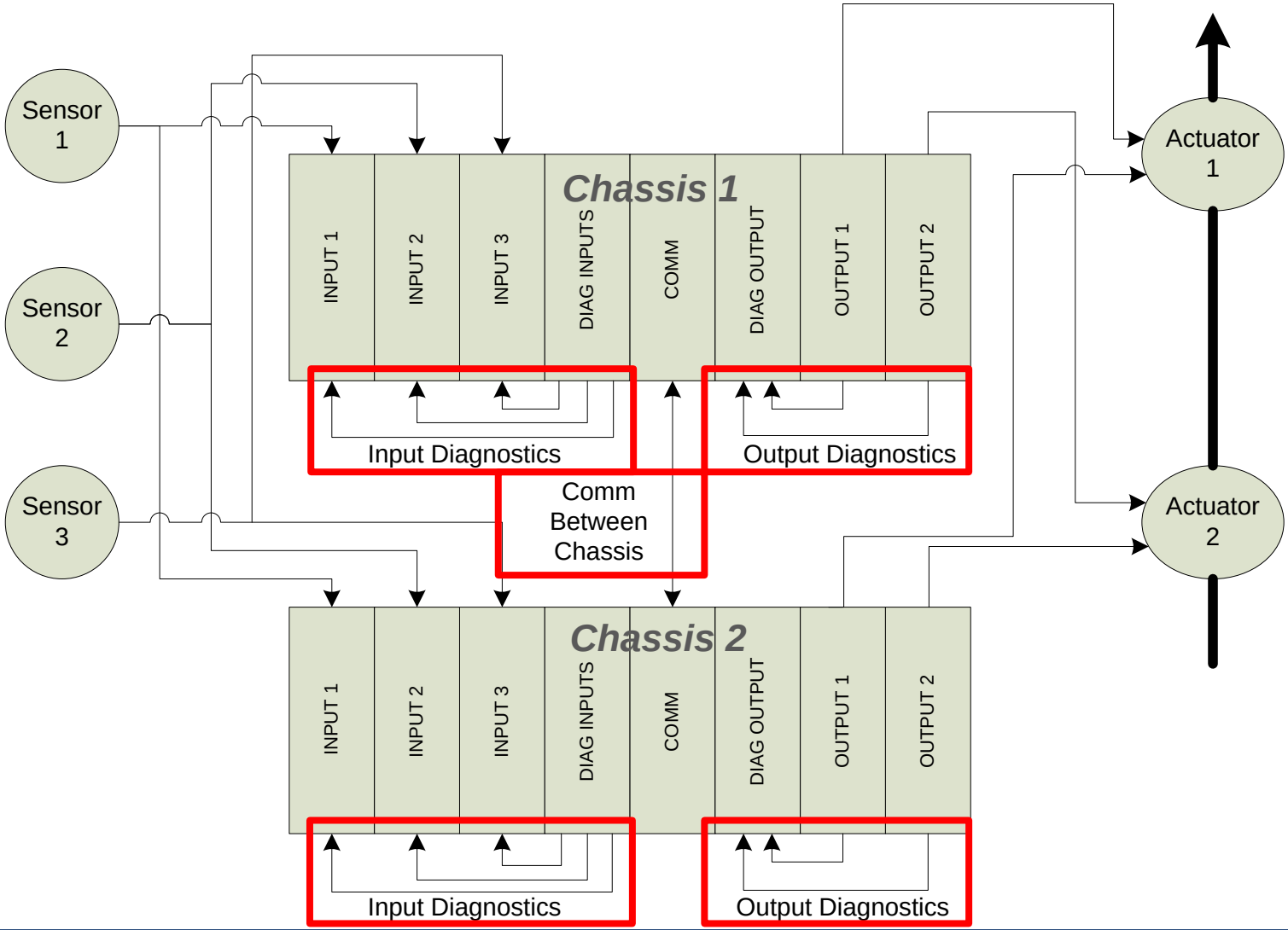
Determine

- Safe Failure Fraction
- Diagnostics Coverage
- Probability of Failure per Hour

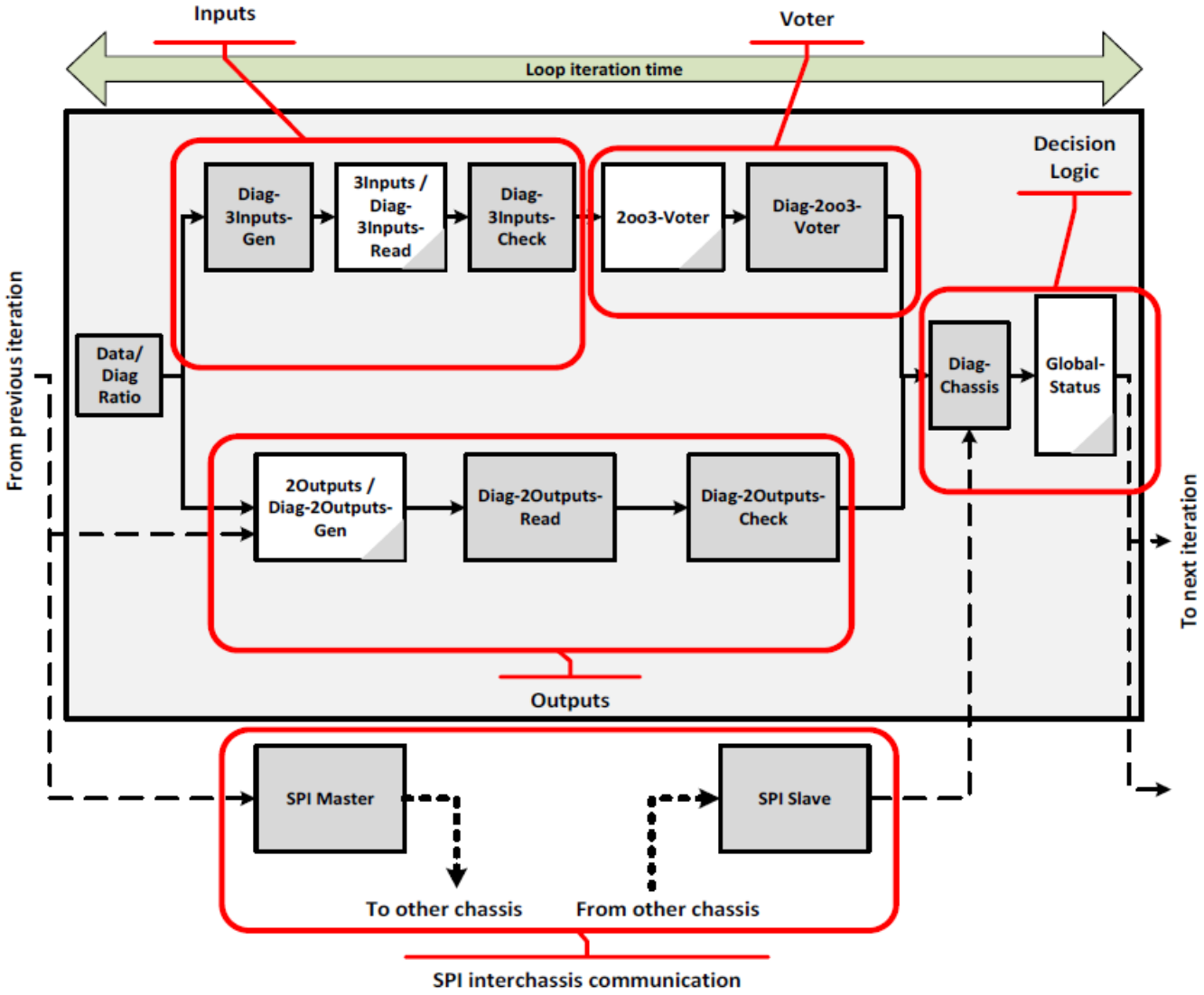
Metric	NI 9205	NI 9425	NI 9401	NI 9477	NI 9159
$\sum \lambda_S$	1.877E-08	3.858E-08	4.308E-09	2.510E-08	8.873E-09
$\sum \lambda_D$	3.966E-07	4.943E-07	2.545E-07	1.656E-07	1.078E-06
$\sum \lambda_{DD}$	0.000E-00	0.000E-00	0.000E-00	0.000E-00	5.735E-07
$\sum \lambda_{DU}$	3.966E-07	4.943E-07	2.545E-07	1.656E-07	5.048E-07
SFF	4.25%	7.24%	1.66%	13.16%	53.57%
DC	0.00%	0.00%	0.00%	0.00%	53.19%
PFH	3.966E-07	4.943E-07	2.545E-07	1.656E-07	5.048E-07

Fast Controller Solution

Double Decker

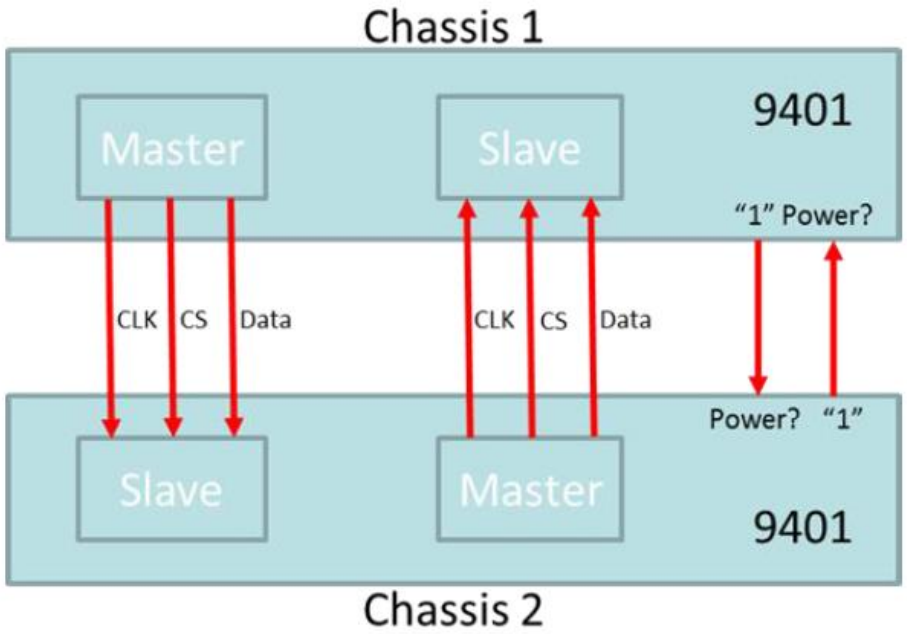


Fast PIS – FPGA core application



Inter-chassis Communication

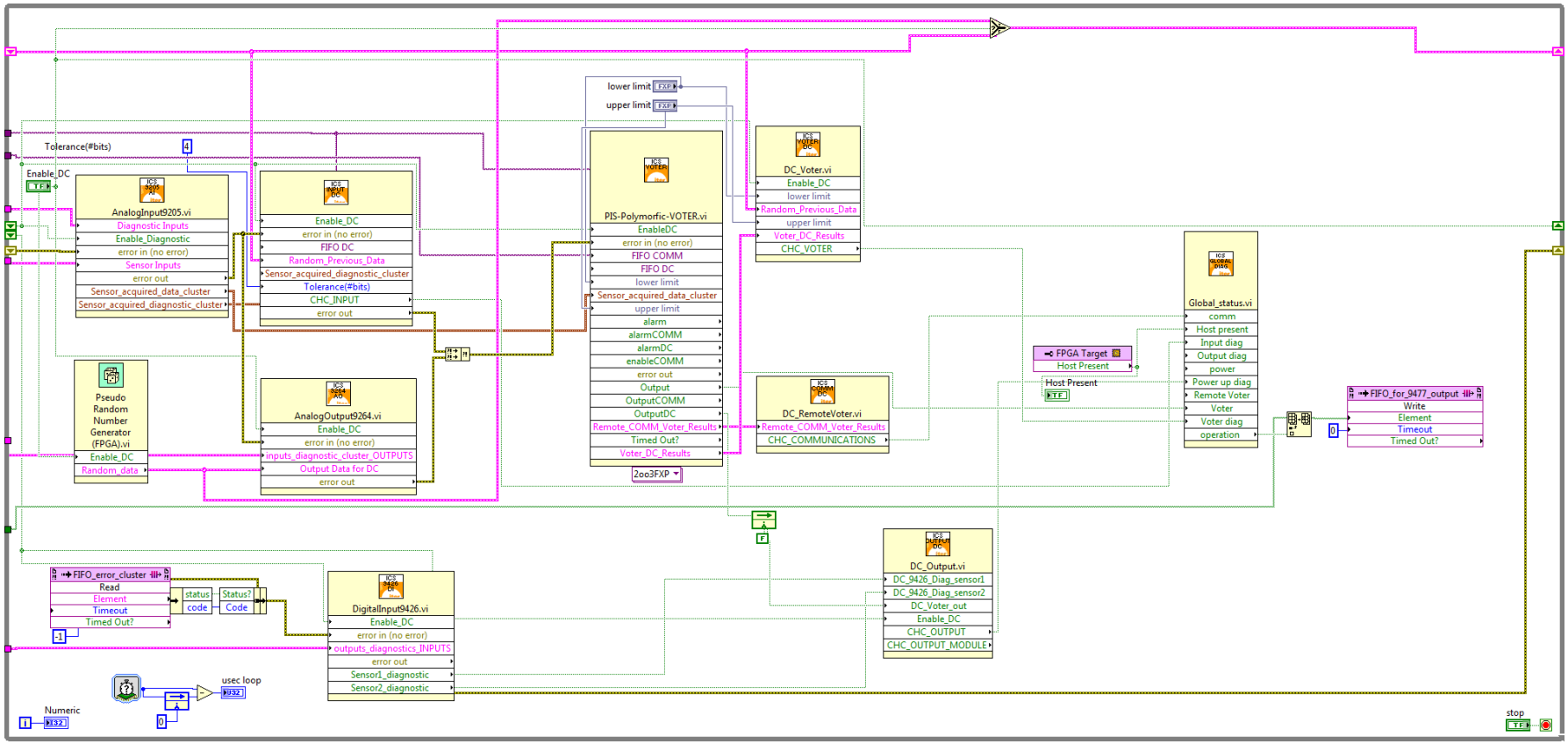
- SPI communication
- 64 data frame
- Status:
  - Inputs
  - Outputs
  - Voter
  - Diagnostics
- Integrity measures:
  - Consecutive number
  - CRC 16 bits



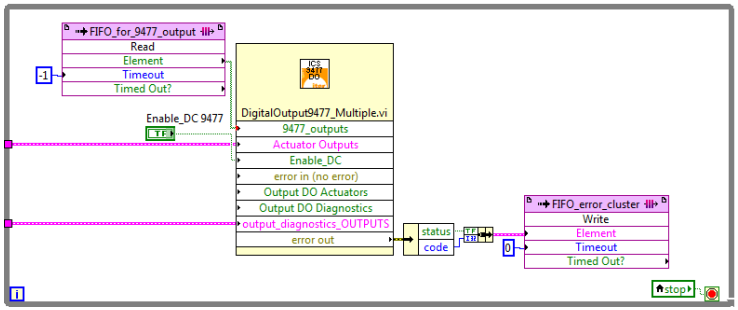
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Consecutive number (5 bits)					PU	CH	CC	RP	I1	I2	I3	O1	O2	TE	VO1
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
VA1	VD1	VO2	VA2	VD2	VO3	VA3	VD3	VO4	VA4	VD4	VO5	VA5	VD5	VO6	VA6
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
VD6	VO7	VA7	VD7	VO8	VA8	VD8	VO9	VA9	VD9	VO10	VA10	VD10	VO11	VA11	VD11
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
CRC (16 bits)															

Legend:	
Consecutive number	CN (5 bits)
Power Up DC	PU
Comm Host	CH
Comm chassis	CC
Remote Power	RP
Input DC1	I1
Input DC2	I2
Input DC3	I3
Output DC1	O1
Output DC2	O2
Temp	TE
Voter Output n	Von
Voter Alarm n	Van
Voter DC n	VDn

Fast PIS – Labview Code



https://svnpub.iter.org/codac/iter/codac/dev/units/m-cis-pisfc



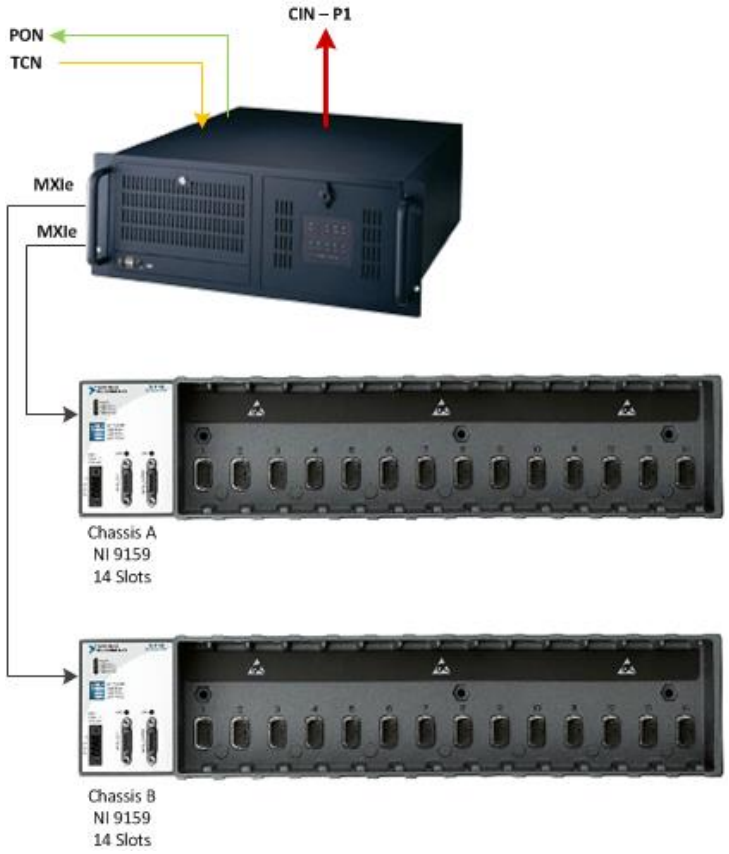
Fast PIS – PC Host

The interlock critical data of the F-PIS or F-CIS module will be transmitted via hardwire links.

The interlock non-critical data (diagnostics) and the communication with both interlock desk and engineering workstation would be done using ethernet CIN-P connected to an attached Fast Controller Server.

The server will be also used to send all the field data to CODAC (e.g. via PON)

The time synchronization for the fast controller will used the TCN



Reference Documentation:

FMEDA Analysis for the 2oo3SD Double Decker Diagnostic and Improvement of the Safe Failure Fraction Figures (SFF) (N62LS6)

Fast PIS – Features

Generic fast PIS controller solution:

- Hardware configuration according to IEC 61508
  - Reliability and integrity figures available
  - PFH calculation tool available for integrity

- Software preconfigured and tested
  Additional configuration can be defined and tested if requested

- Integration with the central system
  - Critical signal: FPGA to FPGA, using Manchester coding via fiber optic
  - Non critical communication with CIS and CODAC via a PC HOST – OPC UA

Conf.	Inputs	Outputs	PFH	SIL consump. (IEC 61508)	SFF	Response Time (min / MAX)
A	3x AI	2x 24V	1.324 E-8	13.2% of SIL 3	85.47 %	41 / 89 µs
B	3x 24V	2x 24V	1.322 E-8	13.2% of SIL 3	85.47 %	143 / 643 µs
C	3x TTL	2x TTL	1.597 E-8	16% of SIL 3	85.47 %	5 / 20 µs

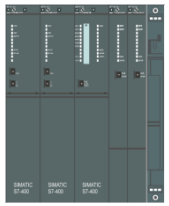
Note: the requirement for SIL-3 according to IEC 61508 is SFF>90%,
There is no SIL-3 COTS with a response time below 1 ms

PIS Controllers

Integrity	Performance	Availability	Technical Solution	Configuration
Up to 3IL-3	> 100ms	Standard	Siemens S7-400-F	Standard PIS
Up to 3IL-3	> 100ms	High Availability	Siemens S7-400-FH	Fully Fault-Tolerance
PFH $<10^{-7}$	< 100ms	Standard	NI Compact Rio	Double Decker

Siemens S7-400-FH

Single CPU



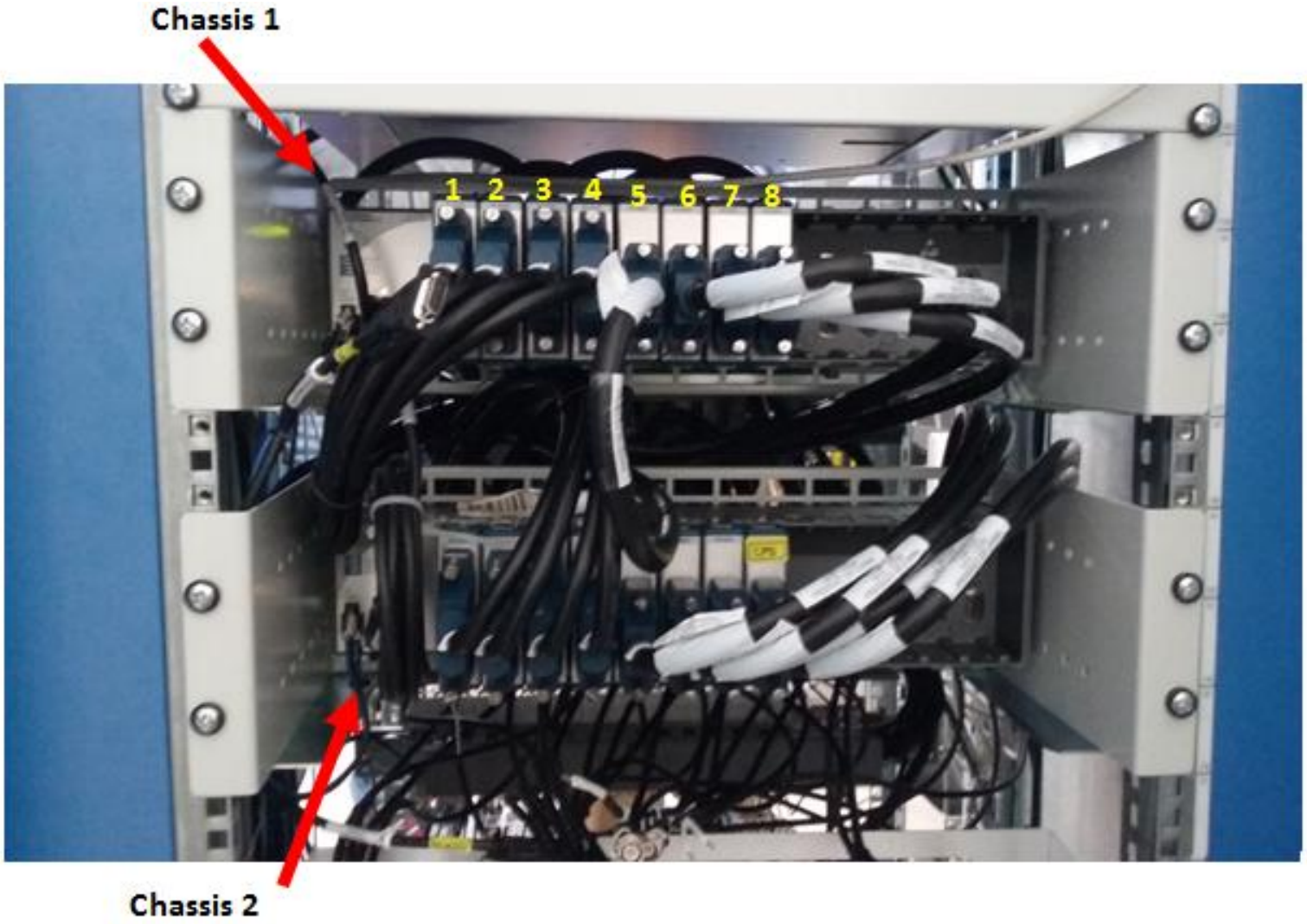
CPU + 2 CP

Fully Fault-Tolerance

Red CPU + CP

If the mitigation of the event requires an active coordination of the actions.

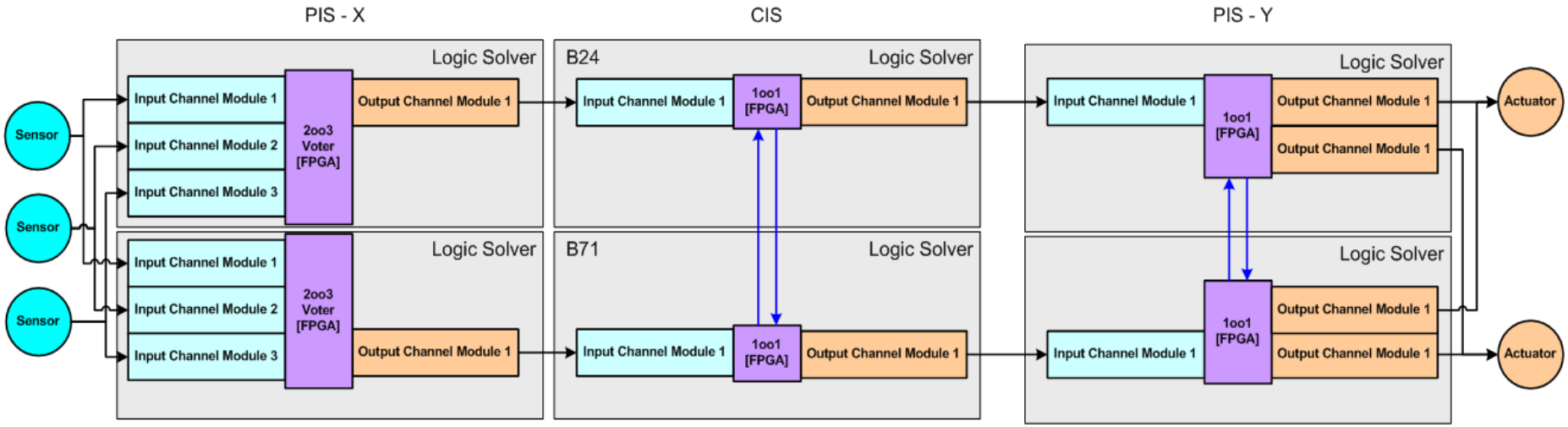
Fast interlock for SC circuits



Central Fast Controller

Fast Architecture

Central Functions: Hardwired connections using CIN-P infrastructure

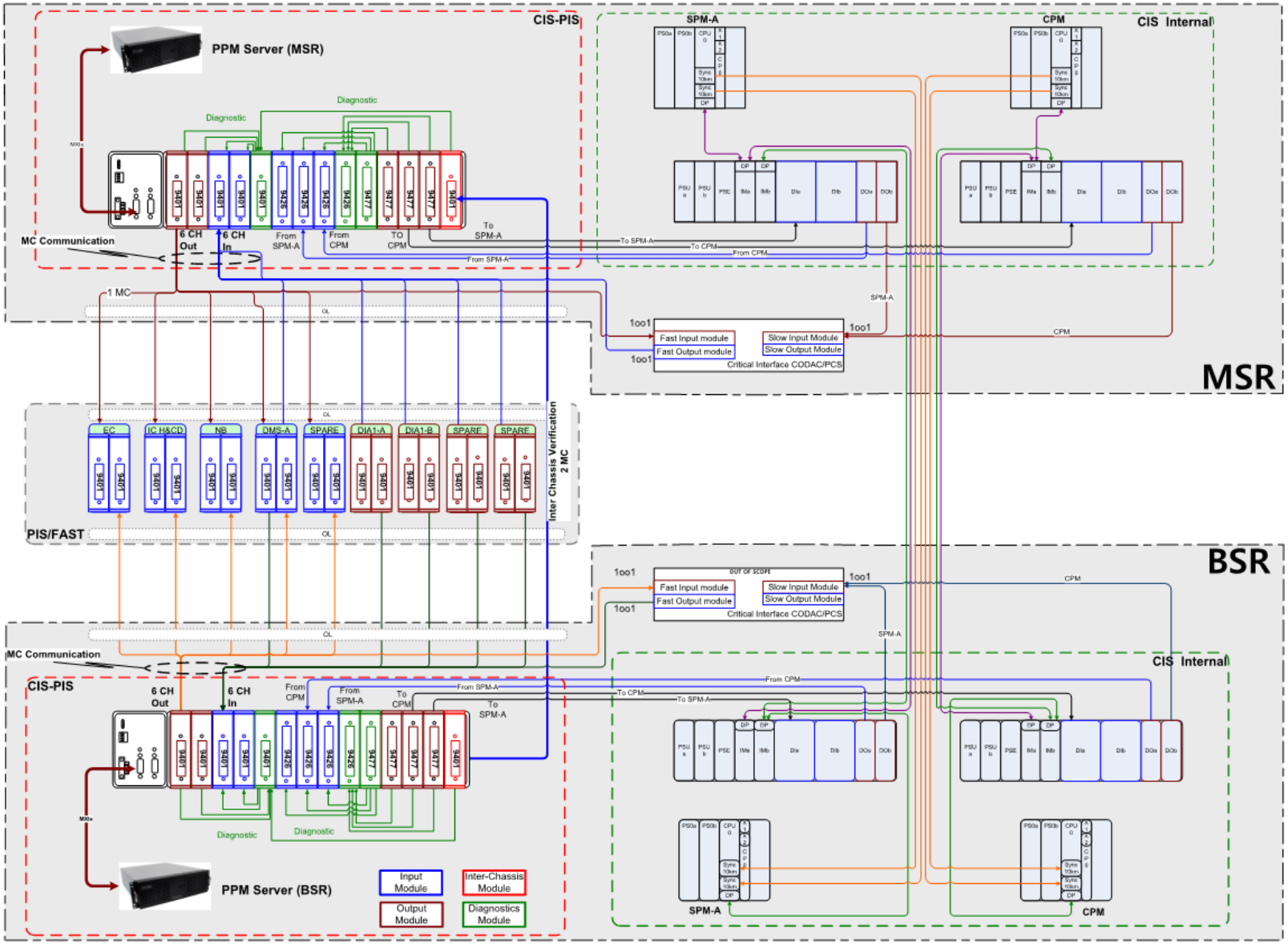


Module	λ_{DU}	λ_{DD}	λ_{D}	λ_{S}
9159 Voter	1.6080E-07	8.7790E-07	1.0387E-06	6.8440E-08
9401 Comm	2.7880E-08	1.9480E-07	2.2268E-07	3.6180E-08
9401 TTL MC Input (from PIS)	1.7350E-08	1.6070E-07	1.7805E-07	2.7250E-08
9401 TTL MC Output (to PIS)	2.6580E-08	1.5580E-07	1.8238E-07	2.7630E-08
9401TTL DI/DO Diag	2.8450E-08	1.7120E-07	1.9965E-07	0.0000E+00
Cumulative	2.89420E-07	1.73160E-06	2.02102E-06	1.59500E-07

PFH	% 3IL-3	%3IL-2
1.540E-08	15%	1.5%

MC transmission time (2 times of encoding, 2 times of decoding)	25.6 µs
Time delay of FO cable (Distance = 1 Km, Round trip)	9.8 µs
Time delay of FO converters (2 for path from PIS to CIS, 2 for path from CIS to PIS)	0.28 µs
Time to process input/output and Diagnostics	5 µs ~ 55 µs
Response time	40.68 µs ~ 90.68 µs

Fast ICS architecture



Central Function Communication - MC

- Manchester Code communication
  - 96 bit for Inter-chassis comm
- Standard frame for plant systems:
  - 64 bits data frame

- Media Converter TTL – FO
  - MTBF 185529 hours

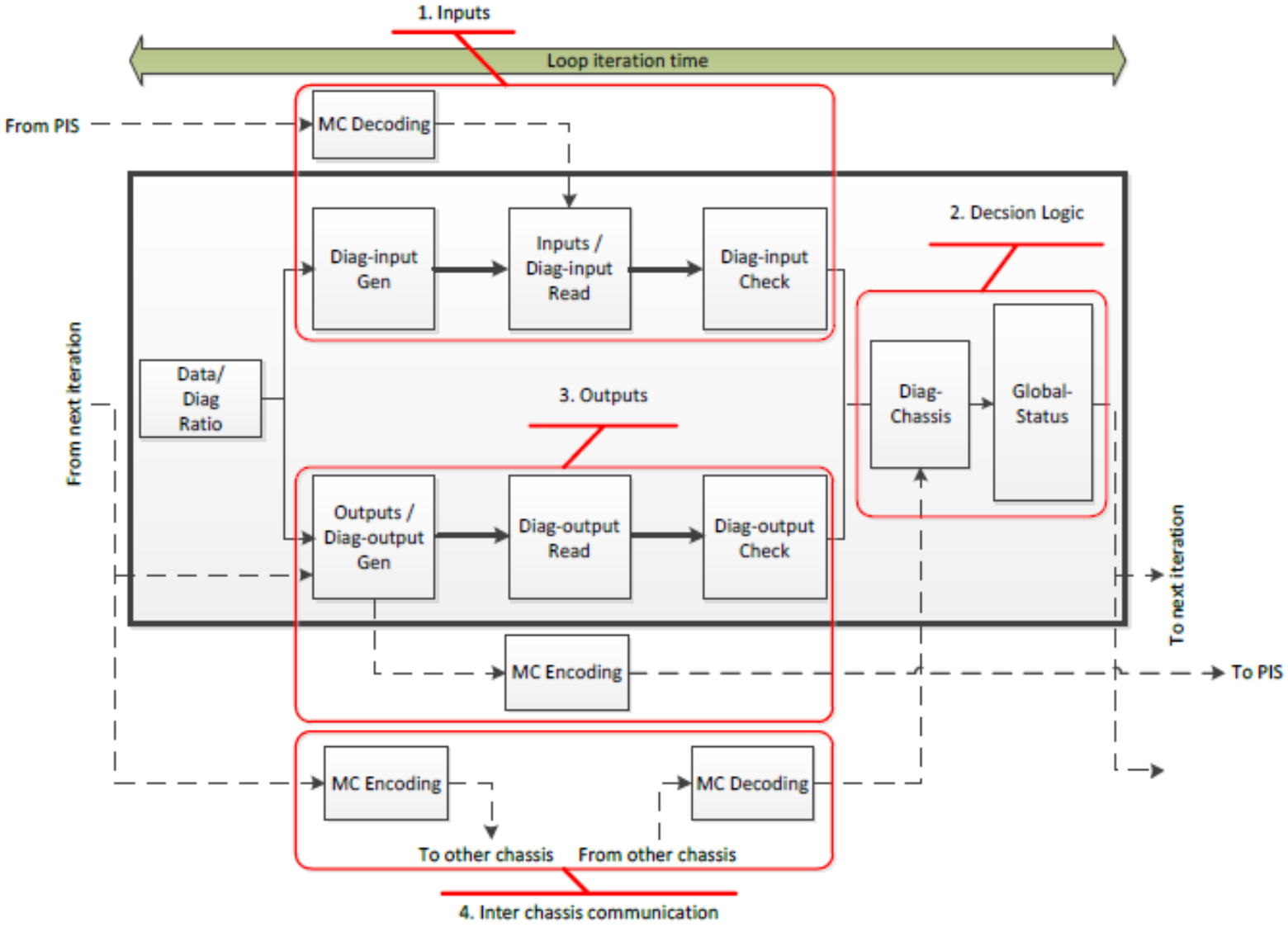
Analogue Value Communication

	Bits	Real data bits
Start Of Frame	2	X
Counter	5	5
Type	3	3
Number of the signal received	8	8
Value	32	32
CRC-16	16	16
Total	66	64

Digital Value Communication

	Bits	Real data bits
Start Of Frame	2	X
Counter	5	5
CBS Level 1	8	8
CBS Level 2	8	8
# of Event or Action	24	24
Reserved	1	X
CRC-16	16	16
Total	64	61

PPM - FPGA core application



Conclusions and Outlook

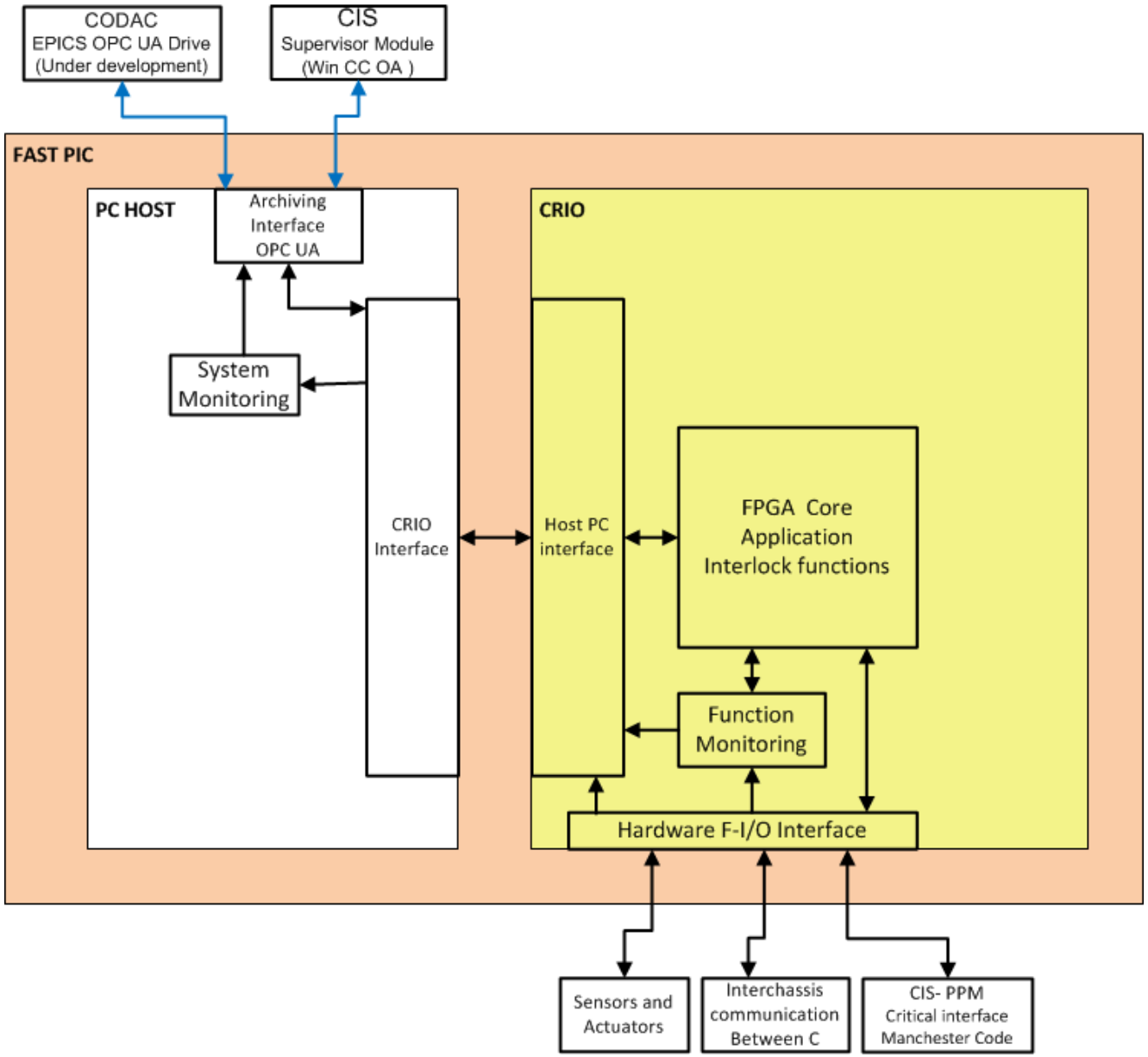
- The project launched in January 2013 has so far produced a PIS controller design over the base of the National Instrument's cRIO with the required capabilities:
  - Availability (99.9%) and reliability (99,6%)
  - Integrity level up to PFH < 10-7
  - Fail-safe solution (deterministic state in case of internal error)
  - Response time of 100µs

- First real applications:
  - Fast interlock for the superconducting coil power supplies (FAT of the Correction Coils Master Controller in December 2015 and for the poloidal field coils, central solenoid and toroidal field coils power converters during 2016)
  - CIS v1

Thank you...

@ITERinterlocks

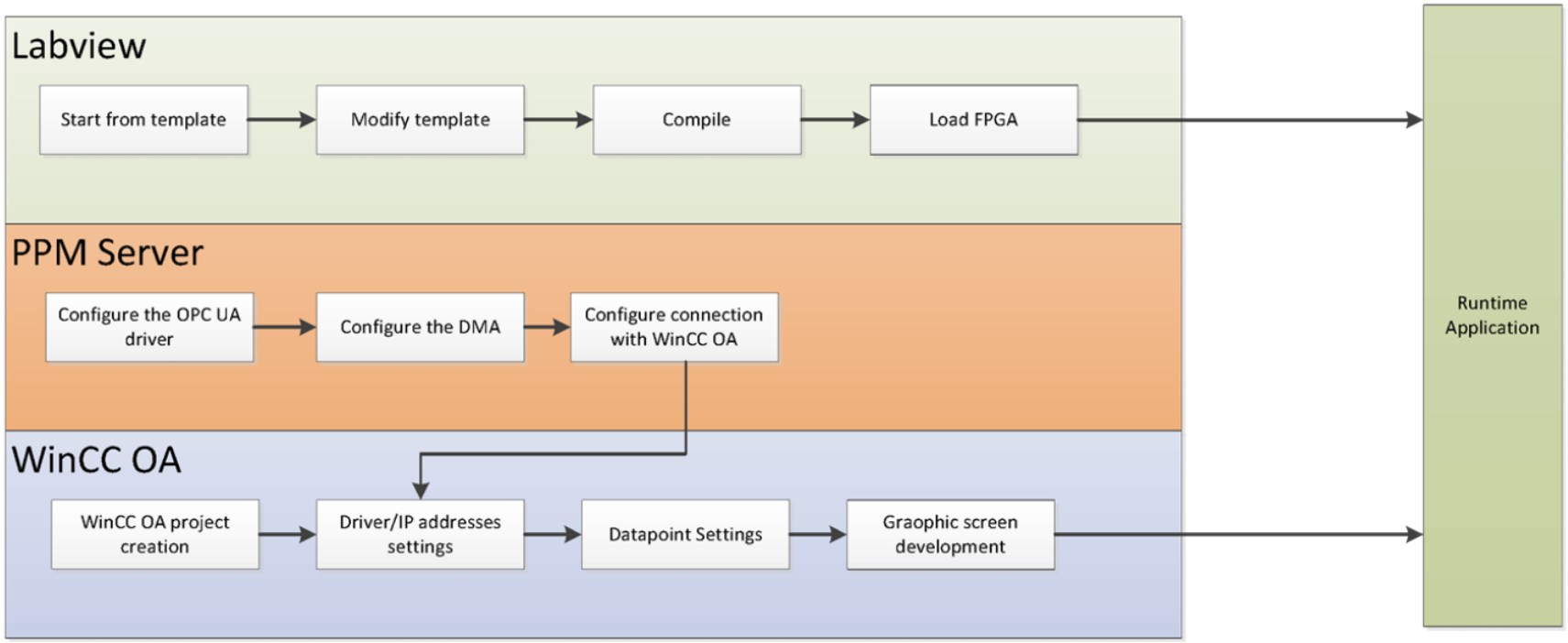
Fast PIS – Software Architecture



Fast-PIS Development Cycle

Several development tools are involved into the development of fast CIS runtime Application:

- LabVIEW for FPGA is used to develop and compile the FPGA code
- The OPC UA driver and the DMA FIFO for the data exchange between the FPGA and Win CC OA are configured under Linux environment with the necessary tools.
- Win CC OA is used to implement the archiving and monitoring of the CIS Fast controller from CIS Desk

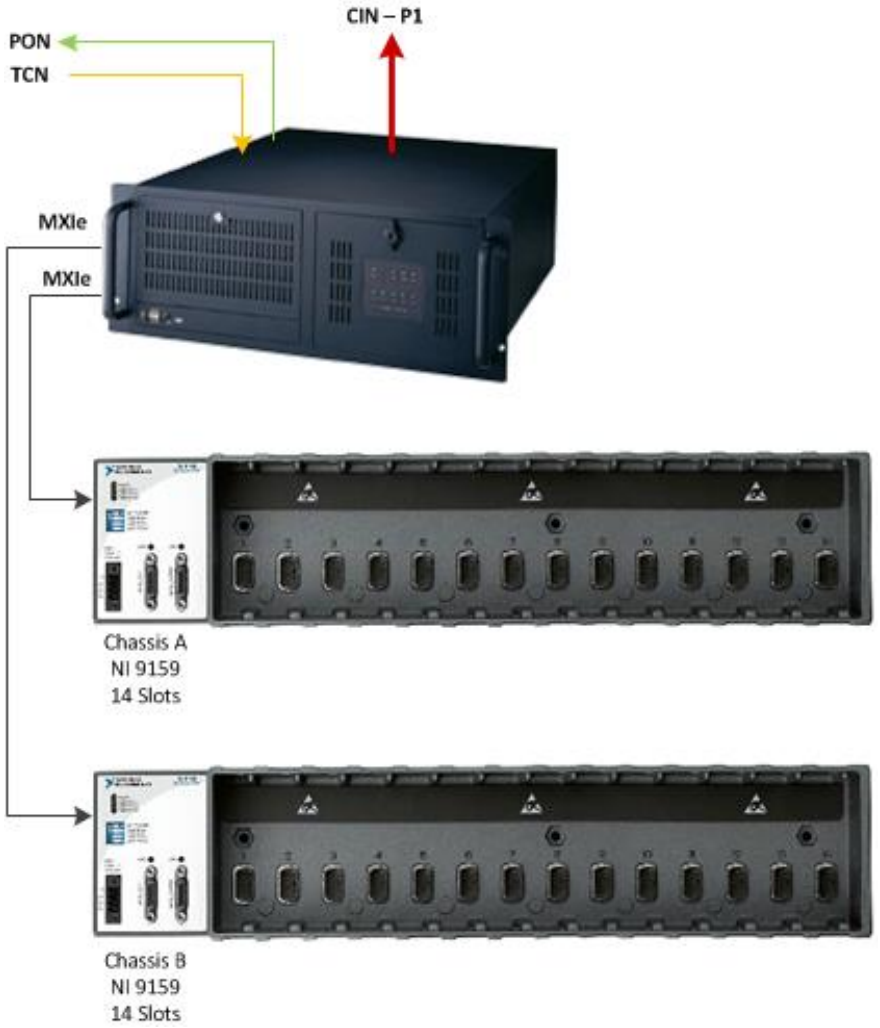


Fast PIS Hardware Architecture

Generic fast PIS controller solution:

Double-Decker System

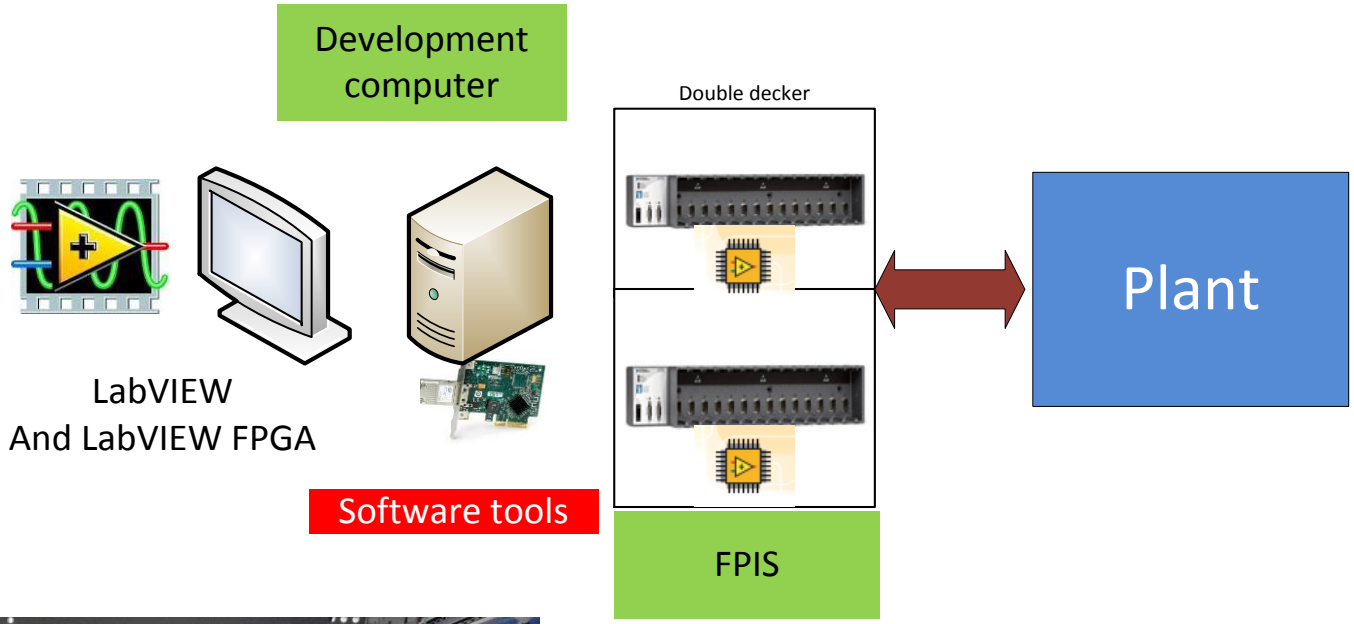
The 2oo3 Double Decker architecture showed the best overall performance in terms of availability and reliability. The voter is implemented in the FPGA; hence it does not require en external voter unit and thus enables capabilities that can provide a higher level of safety. The two chassis allow for a diagnostic strategy that will increase the SFF. Also, this solution can be adapted as a F-CIS module solution.



Compact Rio Modules for Fast Interlock Controllers

Description	Reference
NI 9159, 14-slot CompactRIO Chassis, LX 110 FPGA, MXIe	781315-01
NI 9205 32-Ch ±200 mV to ±10 V, 16-Bit, 250 kS/s AI Module	779357-01
NI 9264 16-Ch ±10 V, 16-Bit, 25 kS/s Analog Output Module	780927-01
NI 9477 32-Ch 24 V, 8 µs, Sinking DO Module	779517-01
NI 9425 32-Ch 24 V, 7 µs, Sinking DI Module	779139-01
NI 9476 32-Ch 24 V, 500 µs, Sourcing DO Module	779140-01
NI 9426 32-Ch 24 V, 7 µs, Sourcing DI Module	780030-01
NI 9401 8-Ch, 5 V/TTL High-Speed Bidirectional Digital I/O Module	779351-01

Prototypes



PPM Inter-chassis Communication

Field	Bits
Start Of Frame	2
Counter	5
PU	1
CH	1
RP	1
TE	1
MDn	14
On	55
CRC-16	16
Total	96