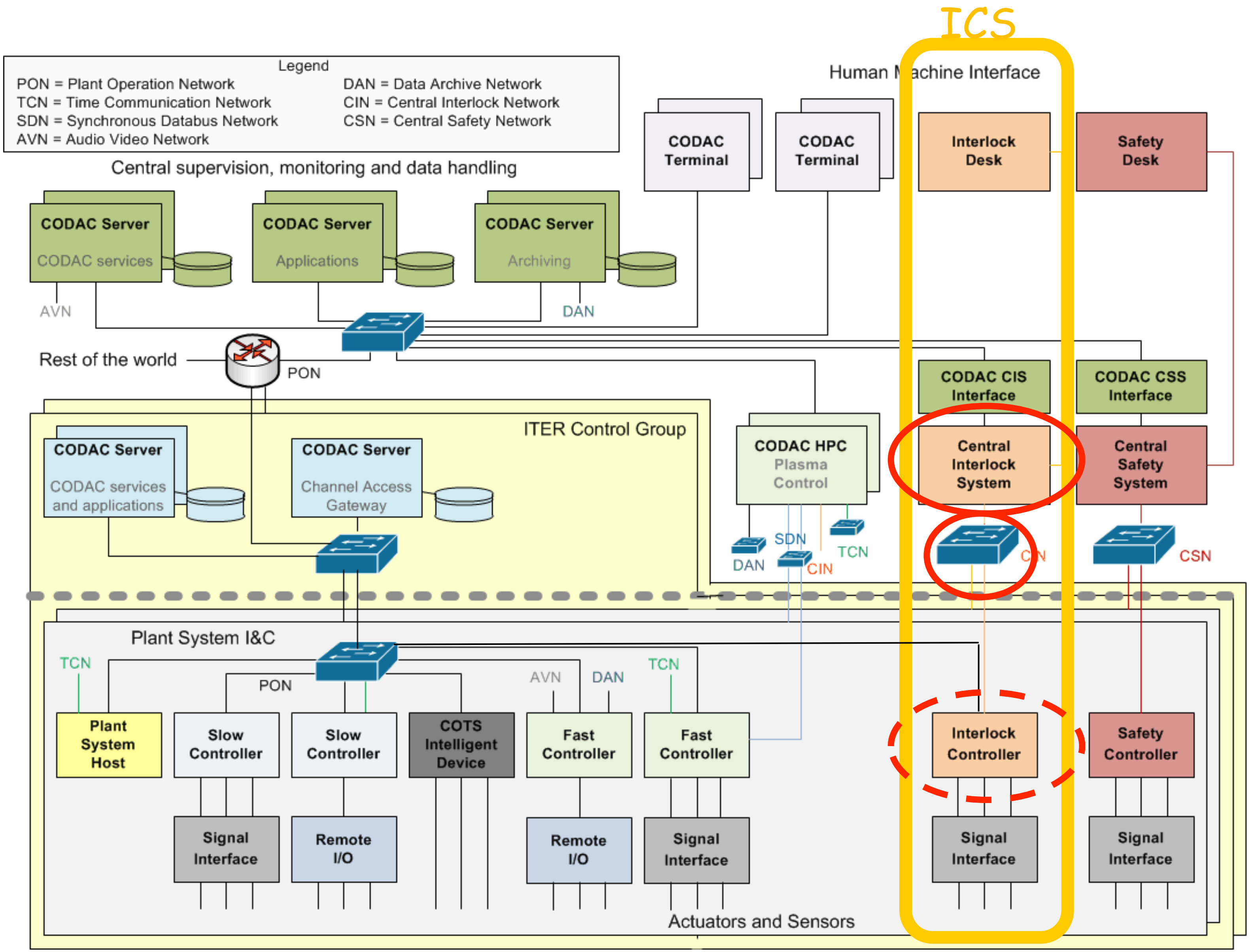
iter

china eu india japan korea russia usa

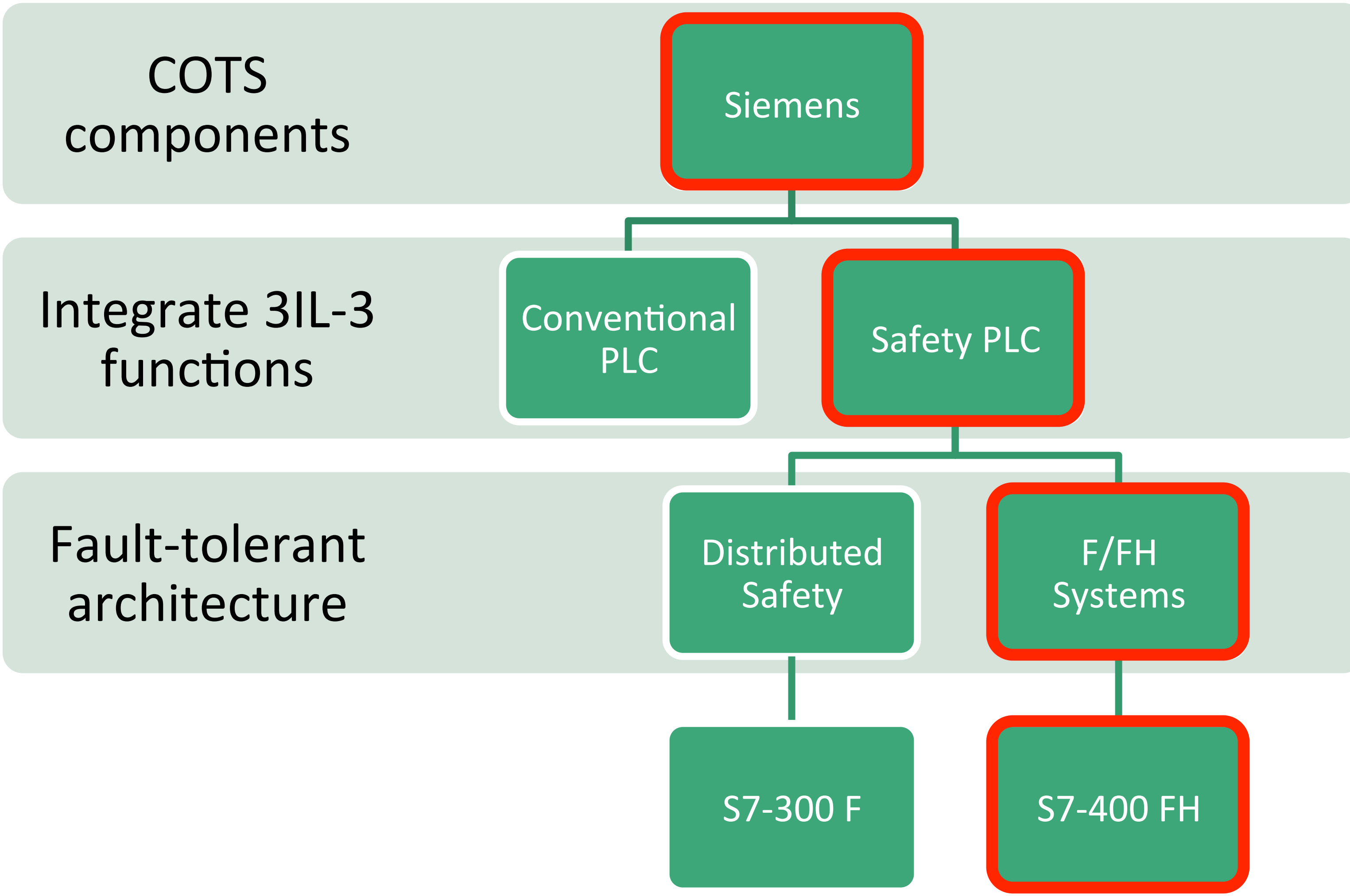
PLC workshop at ESS
29-30 August 2013
PLC systems: Availability & Safety

Alvaro Marqueta – IFMIF
Antonio Vergara – ITER

ITER Central Control Systems



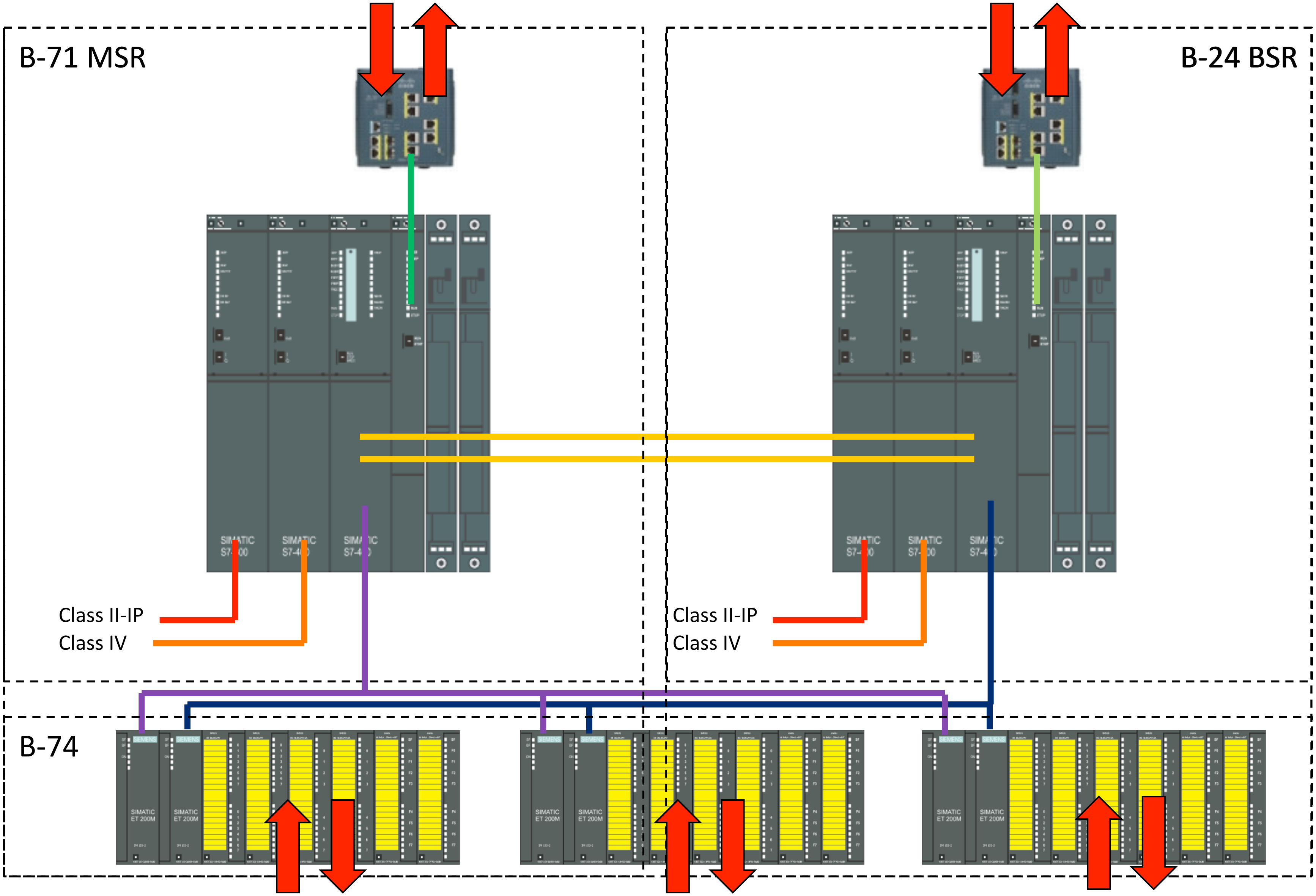
Slow controller selection



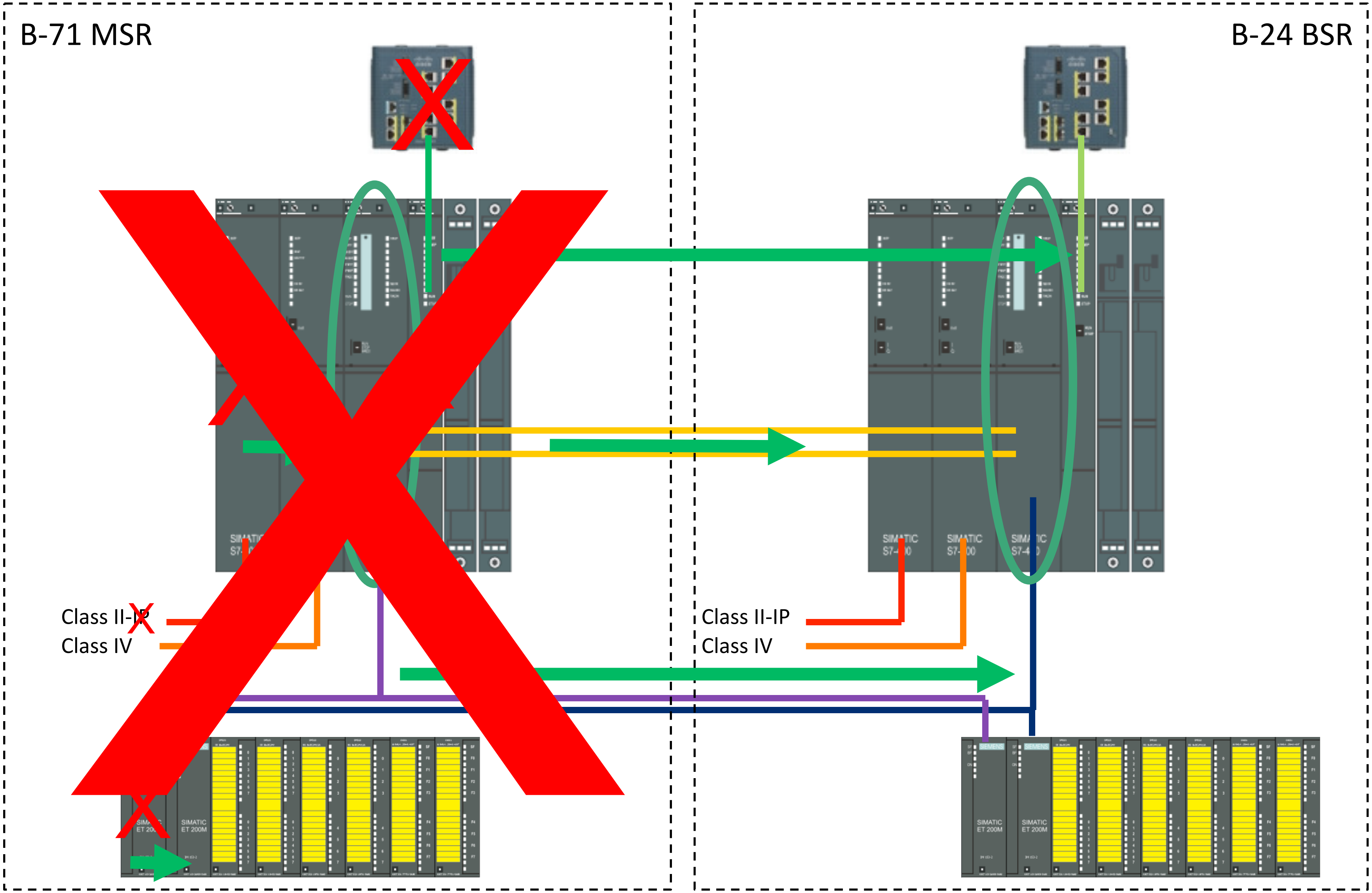
The chosen solutions

Siemens S7-400-FH for slow interlocks

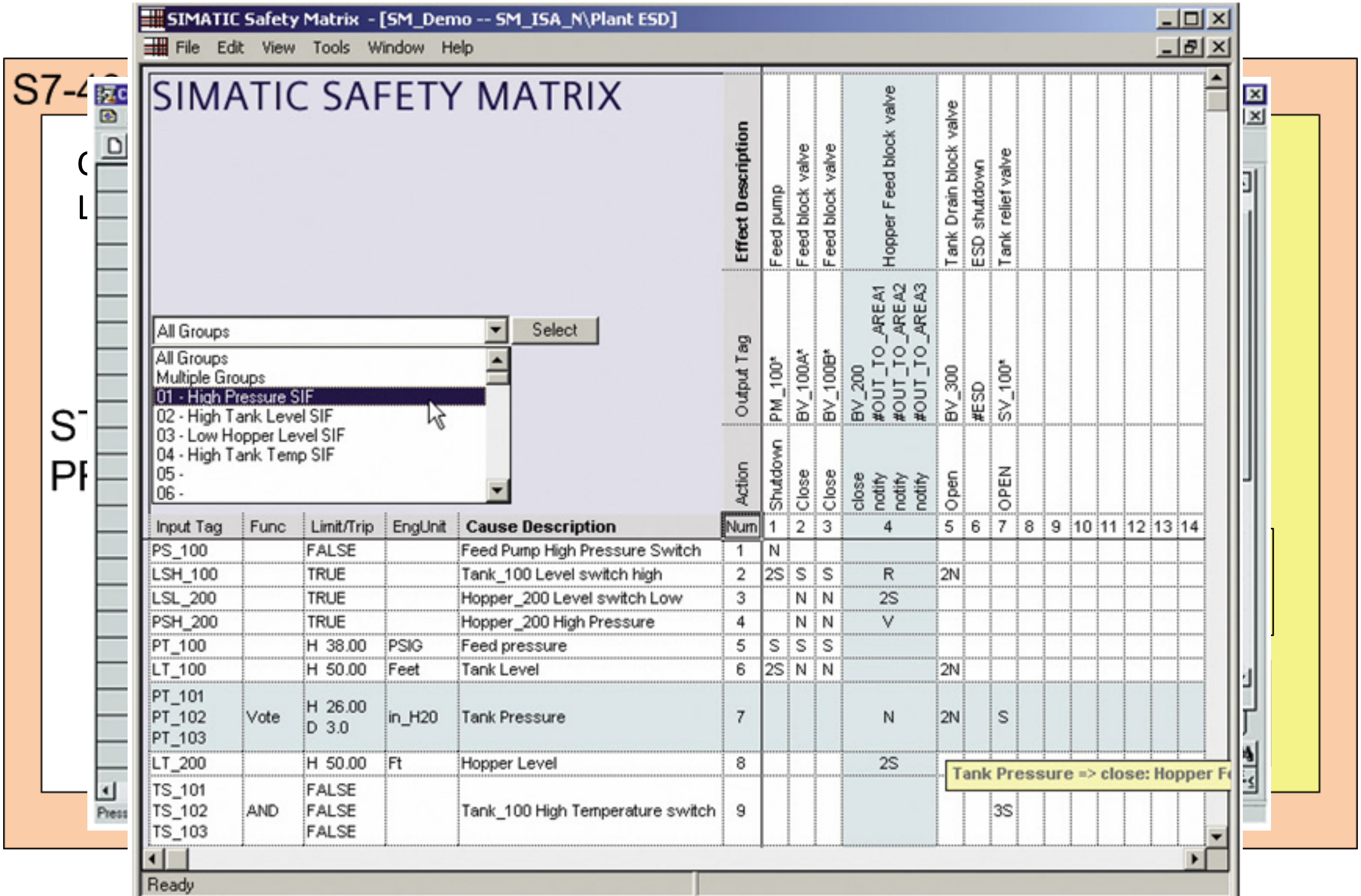
Hardware architecture



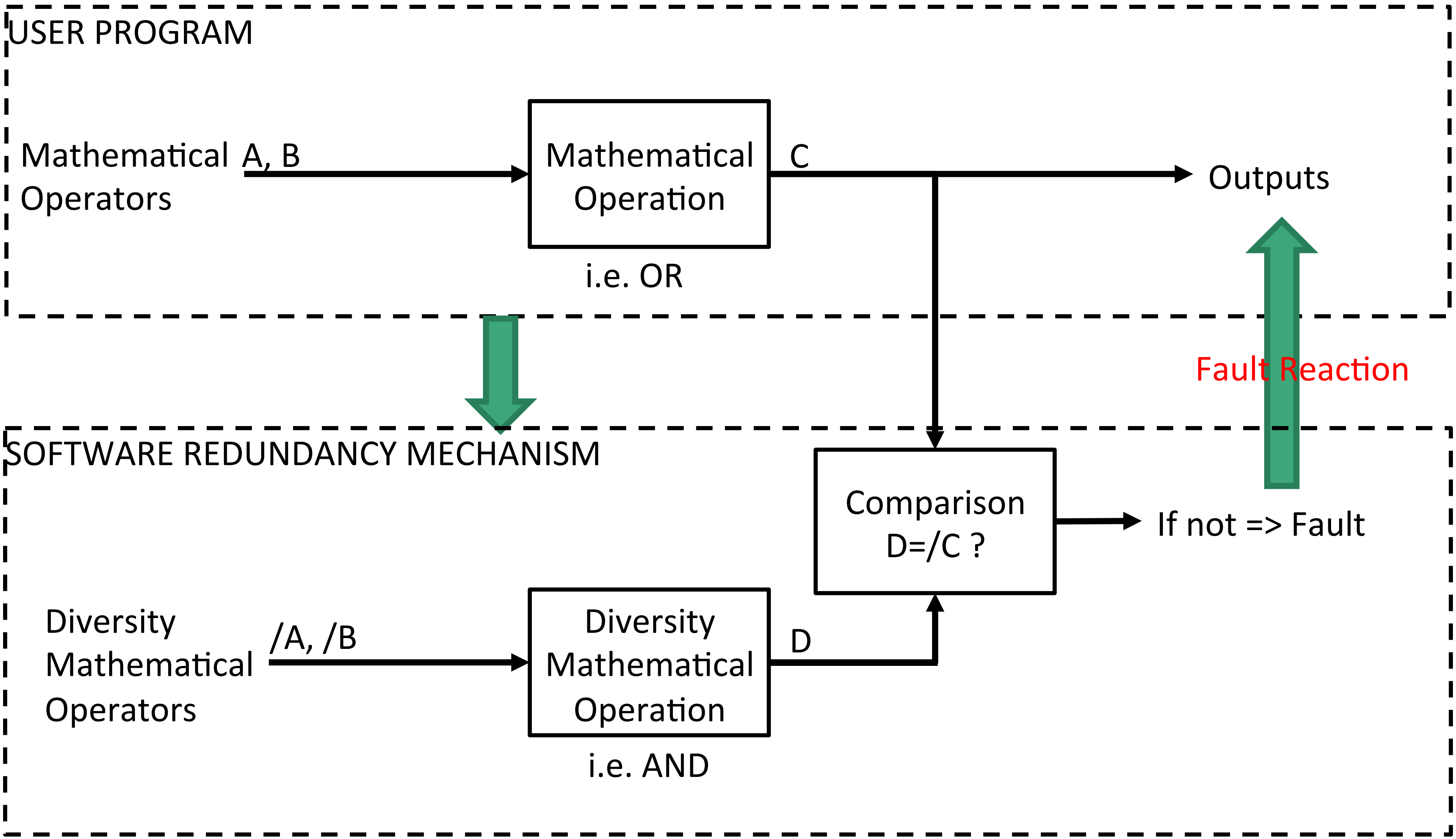
Redundancy mechanisms



Software architecture



CPU Software redundancy



Safety-related communication

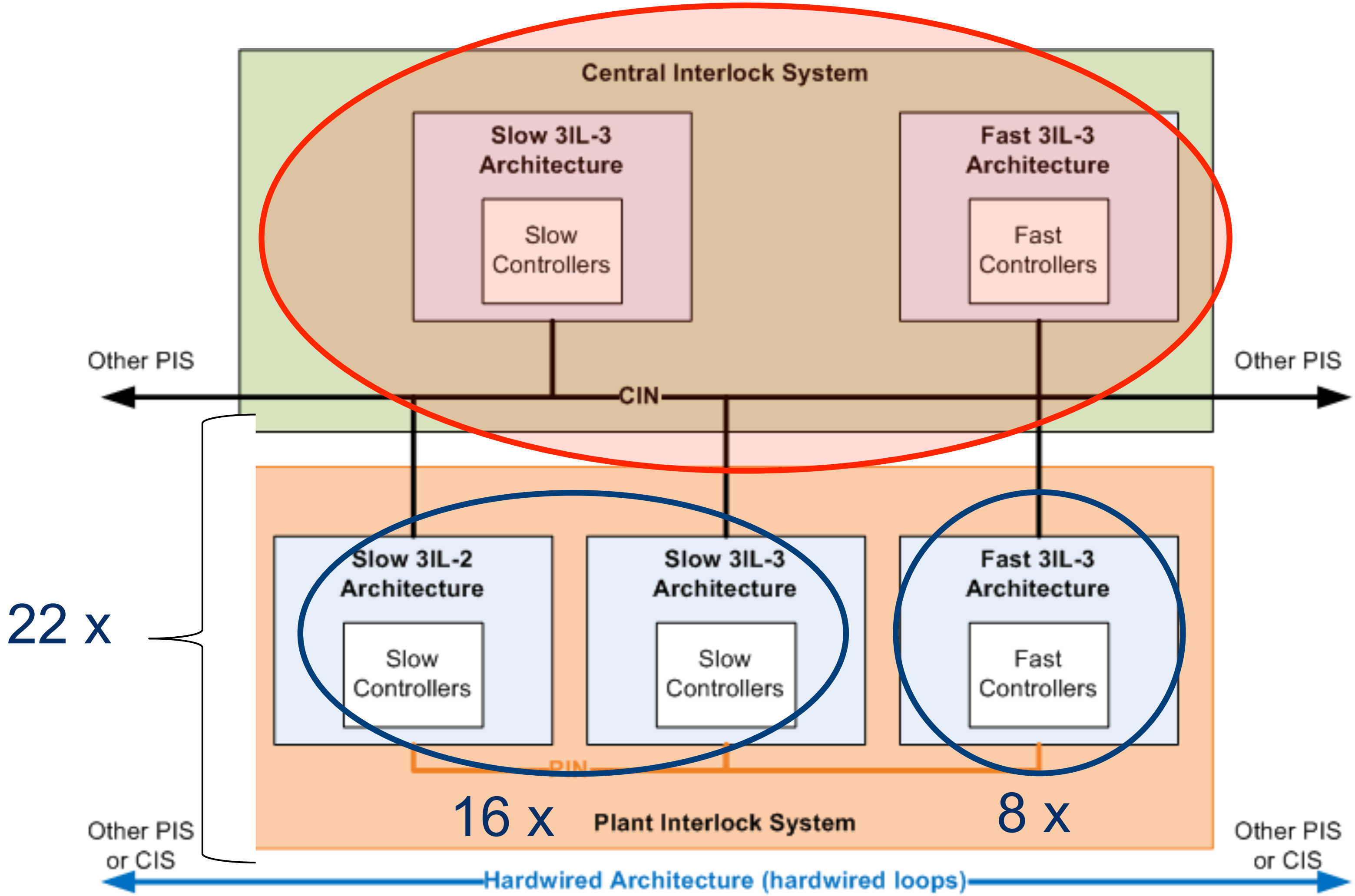
- ✓ Between F-CPU and F-I/O
  - ➢ Profibus protocol
  - ➢ Additional safety shell on top: PROFIsafe
- ✓ Between two F-CPU
  - ➢ Standard protocol (Ethernet, Profibus-DP/PA)
  - ➢ Additional safety shell on top

Threats	Protective mechanisms
Repetition	Sequence number
Deletion	Sequence number
Insertion	Sequence number
Incorrect sequence	Sequence number
Corruption	CRC signature
Timing errors	Periodically sent messages Watchdog
Masquerade/Usurper	Identification procedure

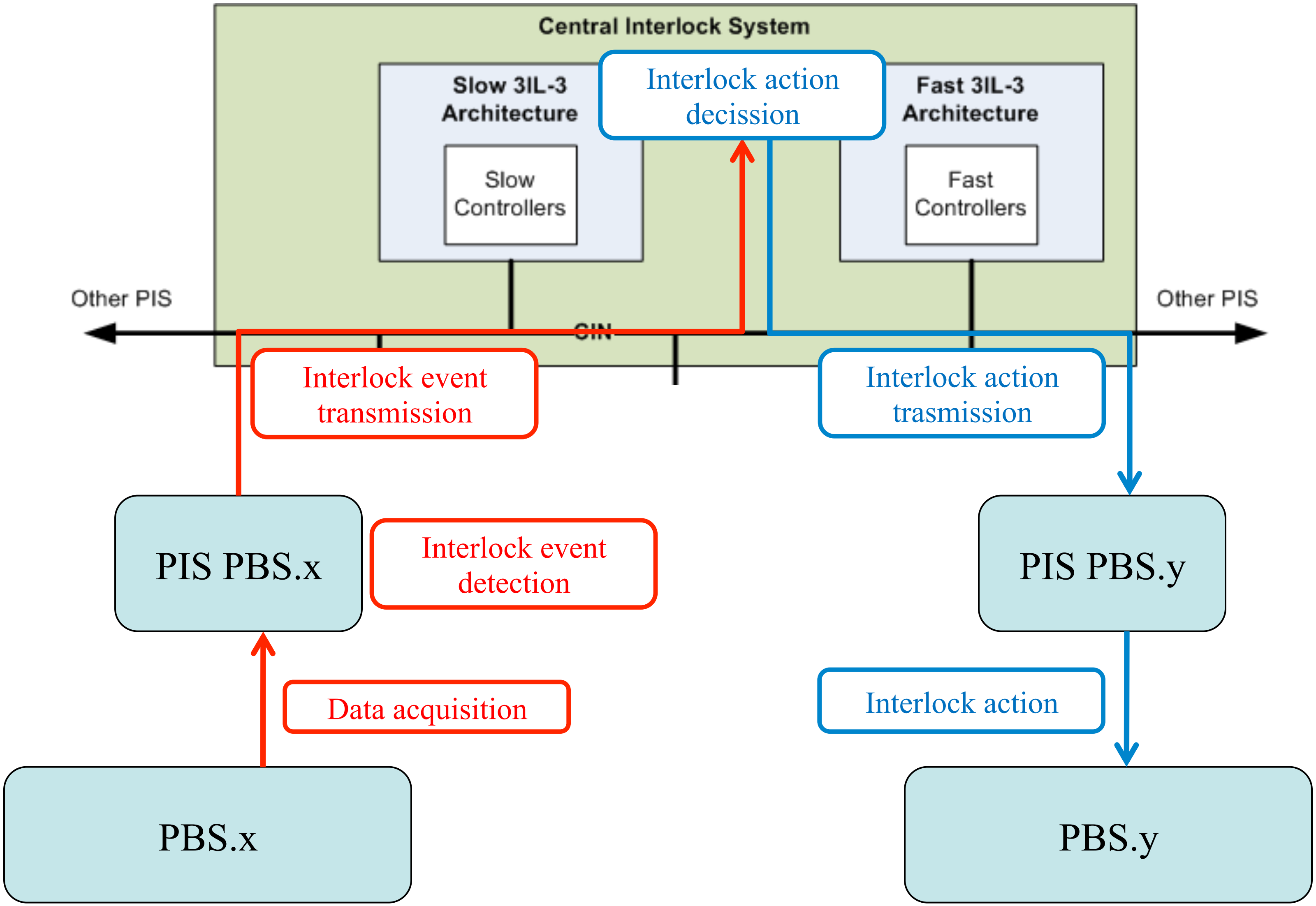
Fail safe reaction:

- ➢ Application of substitute values
- ➢ F-I/O passivation

Overview of interlocks architect.



Central interlock function



Central interlock function

Central interlock function requirements:

- ➢Integrity: SIL3 loop has to be guaranteed (safety-related protocol/hardwiring)
- ➢Dependability: tolerance to 'easy-triggering'
  - ➢ 99.9% inherent availability
  - ➢ 99.6% overall reliability, over two 8h-shifts
- ➢ Time-outs: imposed to up to 1sg

Problems appear when:

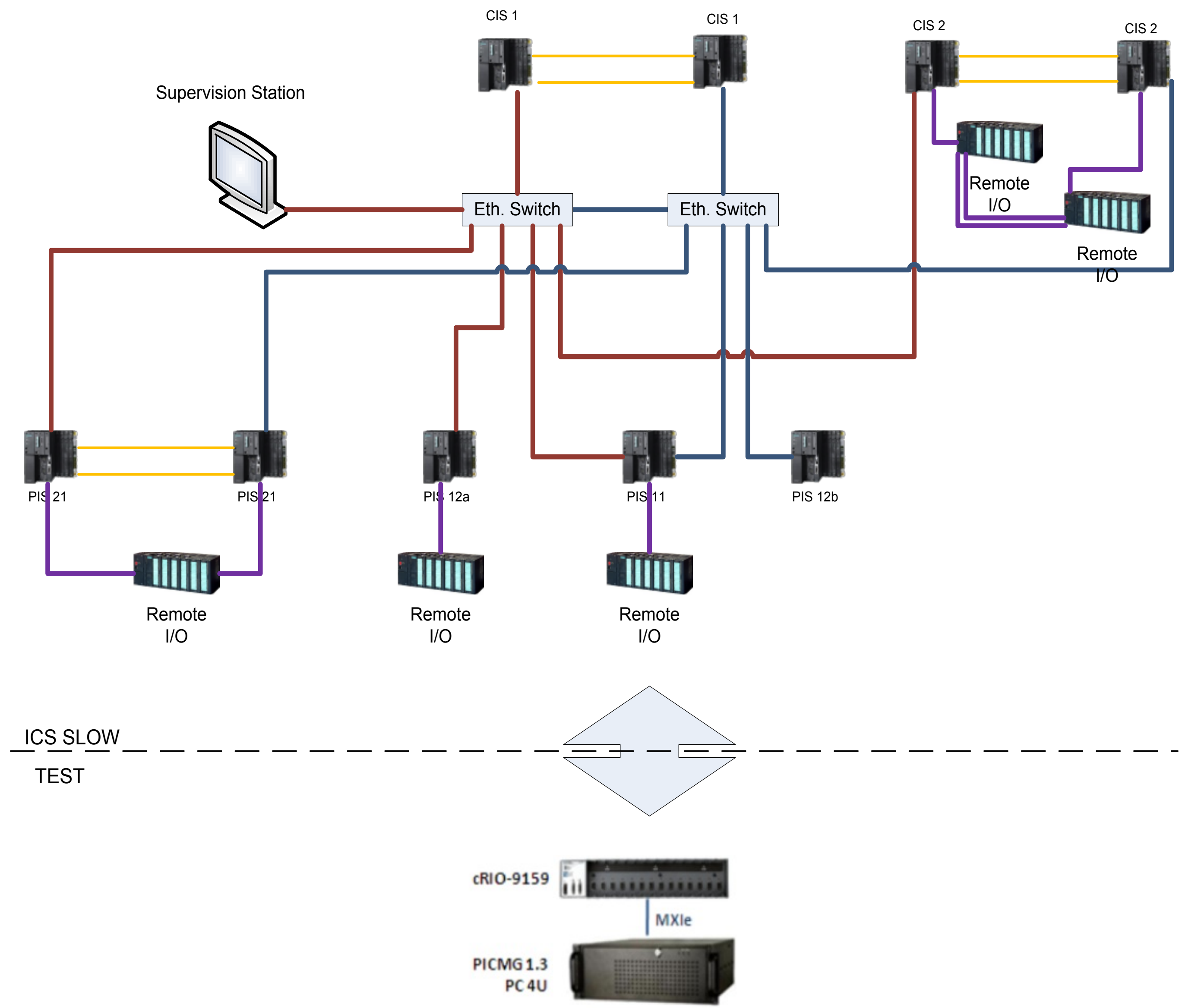
- ➢Integrity: SIL3 loop has to be guaranteed ('cheating' not allowed…)
- ➢Safety-related protocol behaves like a master-slave fieldbus protocol
- ➢Increasing number of communication partners (Plant Interlock Systems) with each central module

CIS test platform

Evolution of CIS test platform:

1) First proto: slow and fast prototype (2010-2011)
2) First discharge loop prototype: CERN (2011-2012)
3) Intensive prototype campaign: 2013 -
   - TCS (India)
   - CERN
   - ASIPP (China)
   - RF-DA
   - Delft Tech.University
   - KO-DA

CIS test platform



CIS test platform

CIS test platform: based on CPU siemens S7 414-4H

- Almost all possible configurations covered
- Local and Central interlock functions executed (including I/O)
    - Simple logic applied to I/O signals
- Works mostly focused on behavior of safety communications
- Several test campaigns have been performed

Main parameters measured:

- Execution time for all communications, from the first block to the last
- Execution time of the safety part of the code (safety processing + safety communications)
- Longest CPU cycle execution time
- Execution time for local/central function, including physical I/O

Test campaigns

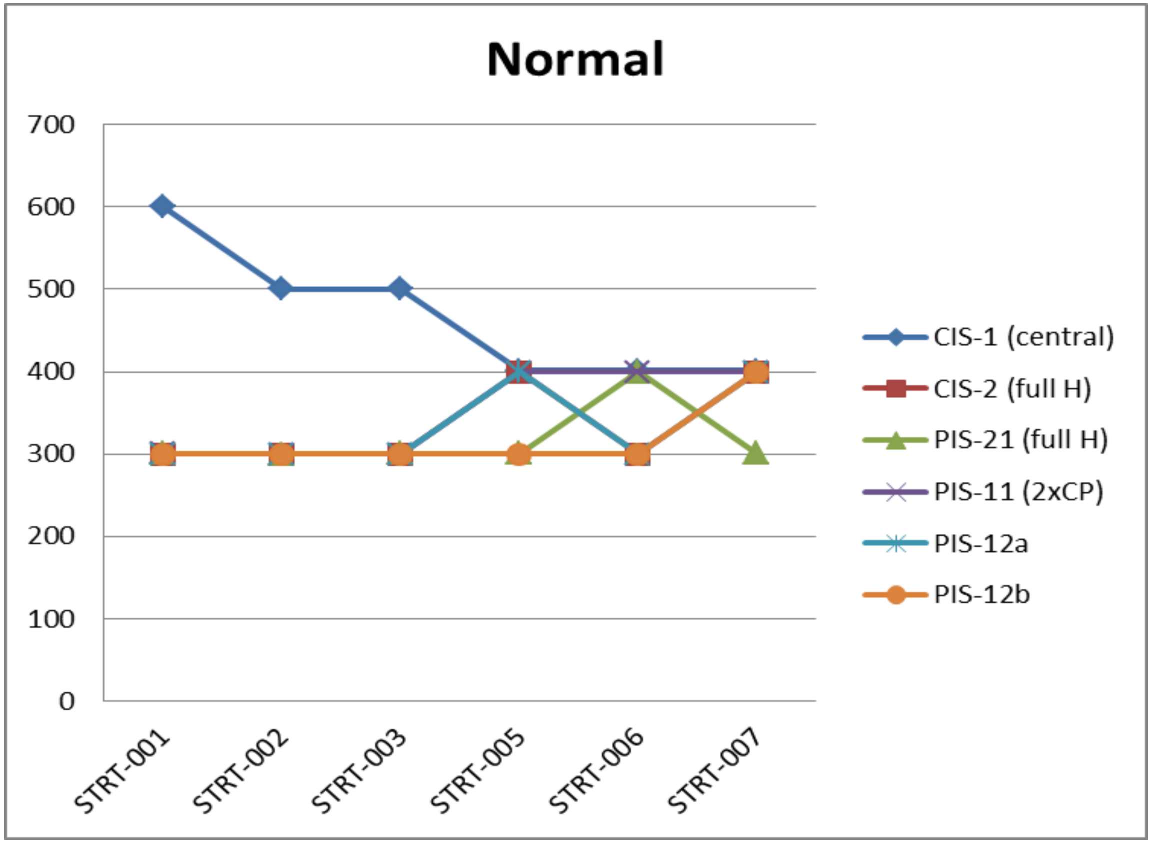
1st test campaign:

- Communications simulated: several-1 block (20 bits) to various partners (contracts)
- Several parameter configurations where tested, in order to learn how to optimize communications:
    - Priorities of different function blocks
    - Interval of execution times for function blocks
- Tested different operating configurations (failure, loss of redundancy, etc)
    - Exec.time in normal mode
    - Exec.time after loss of CPU
    - Exec.time without redundancy
    - Exec.time during resynchronization

Test results

1st test campaign:

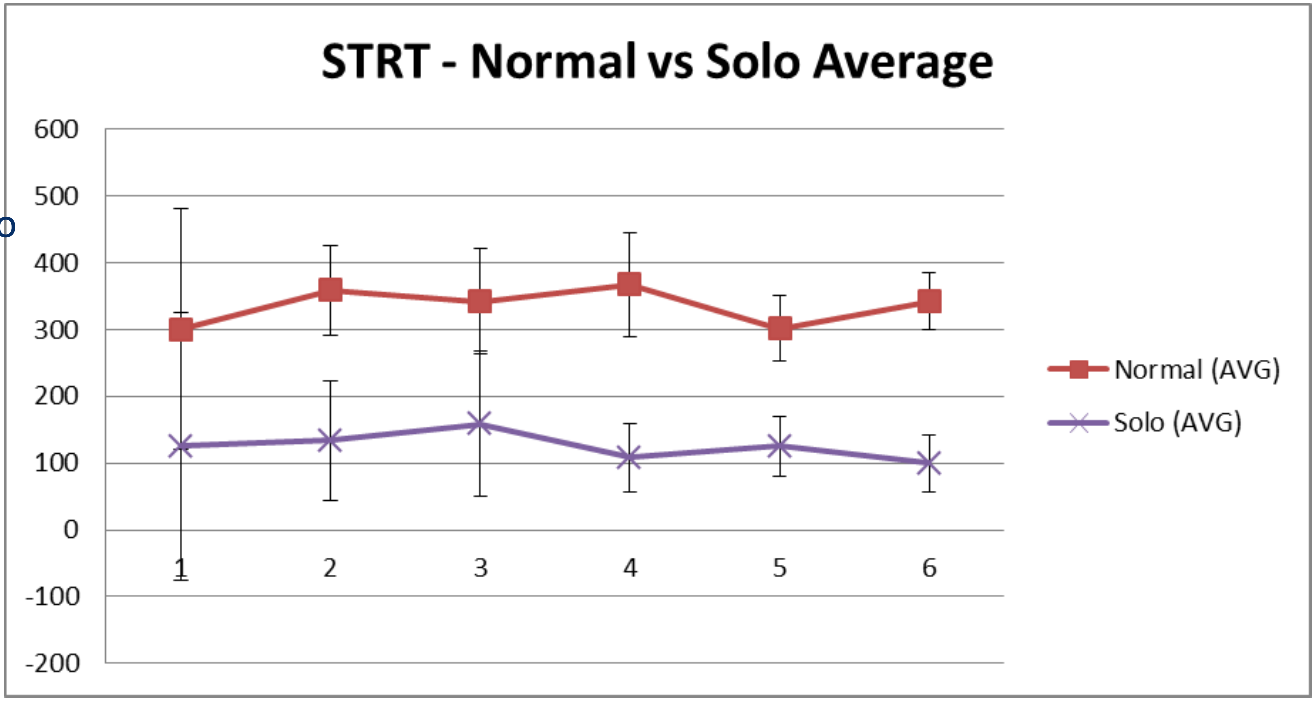
- Communication times
  - For 10 partners
  - Decreasing cycle time
  - Increasing priority



Test results

1st test campaign:

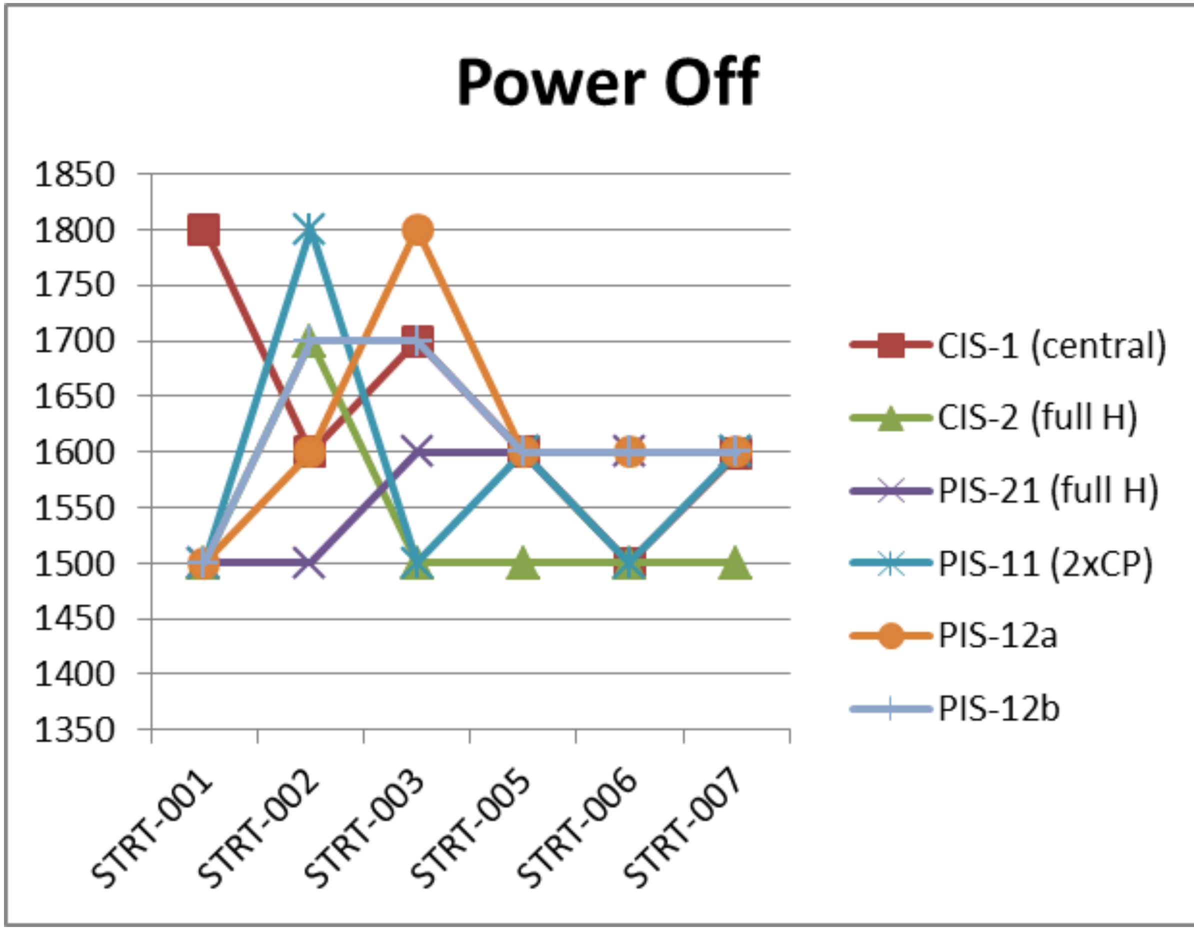
➢ 'H' configuration seems to introduce important delays



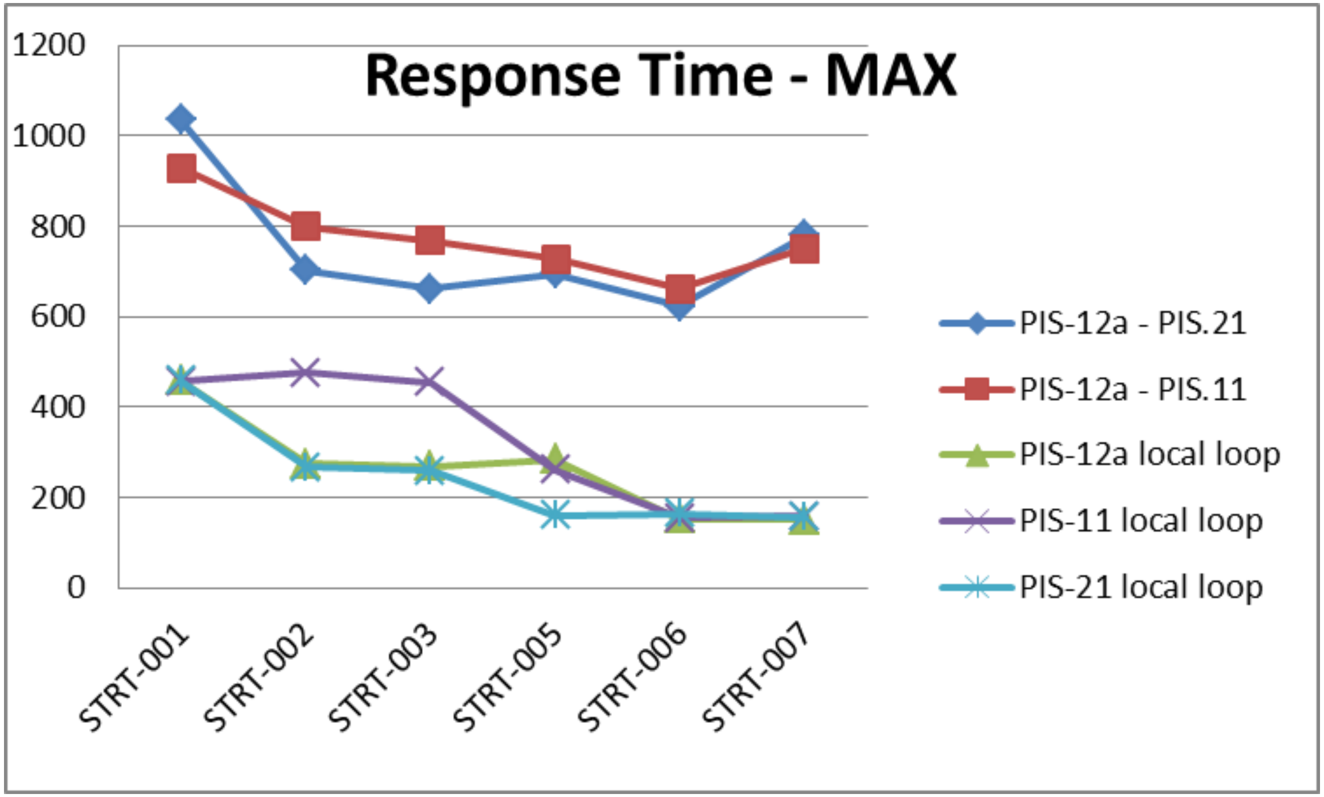
Test results

1st test campaign:

- ➢Delay after 'Power Off'
  - ➢Recovery time becomes unacceptable



Test results



1st test campaign:

➢Execution time for local and central function; close to the limits

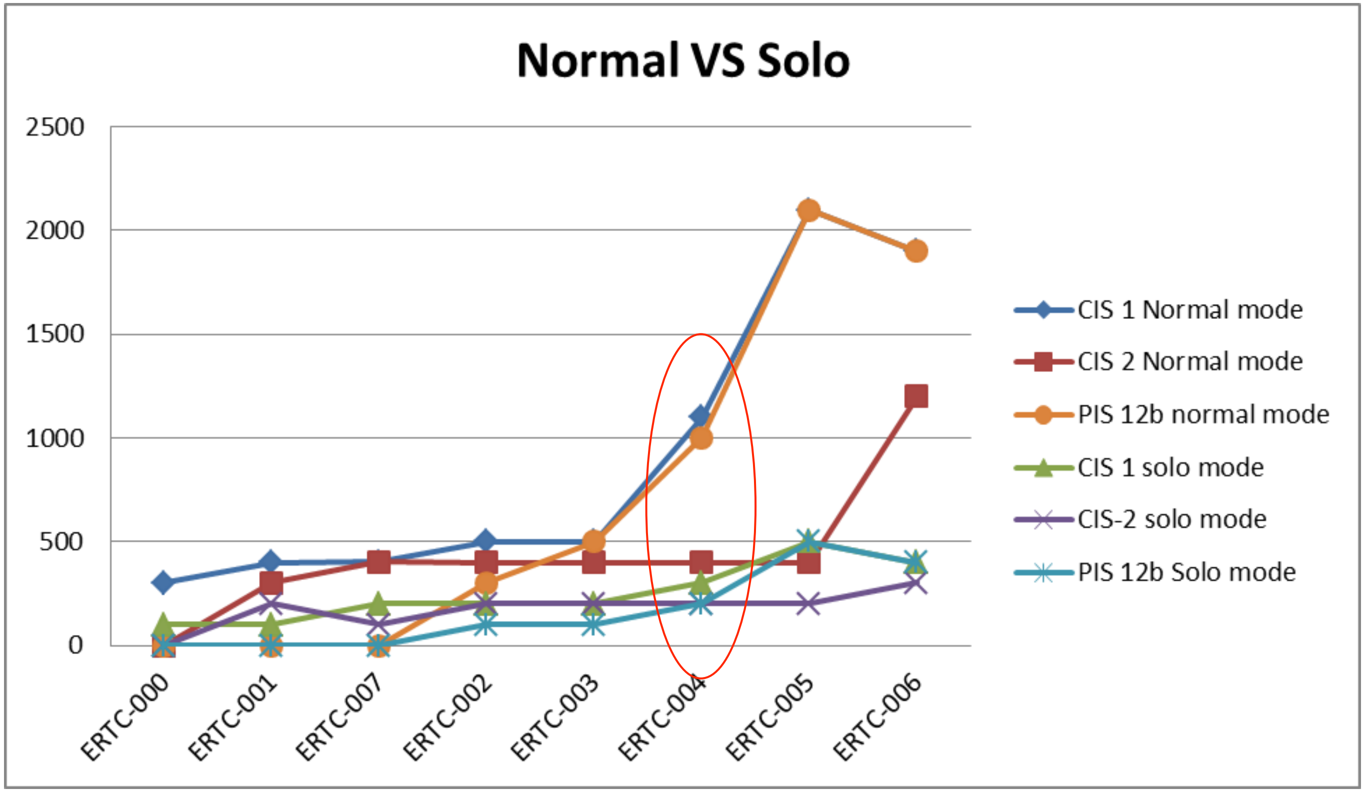
Test results

2nd test campaign:

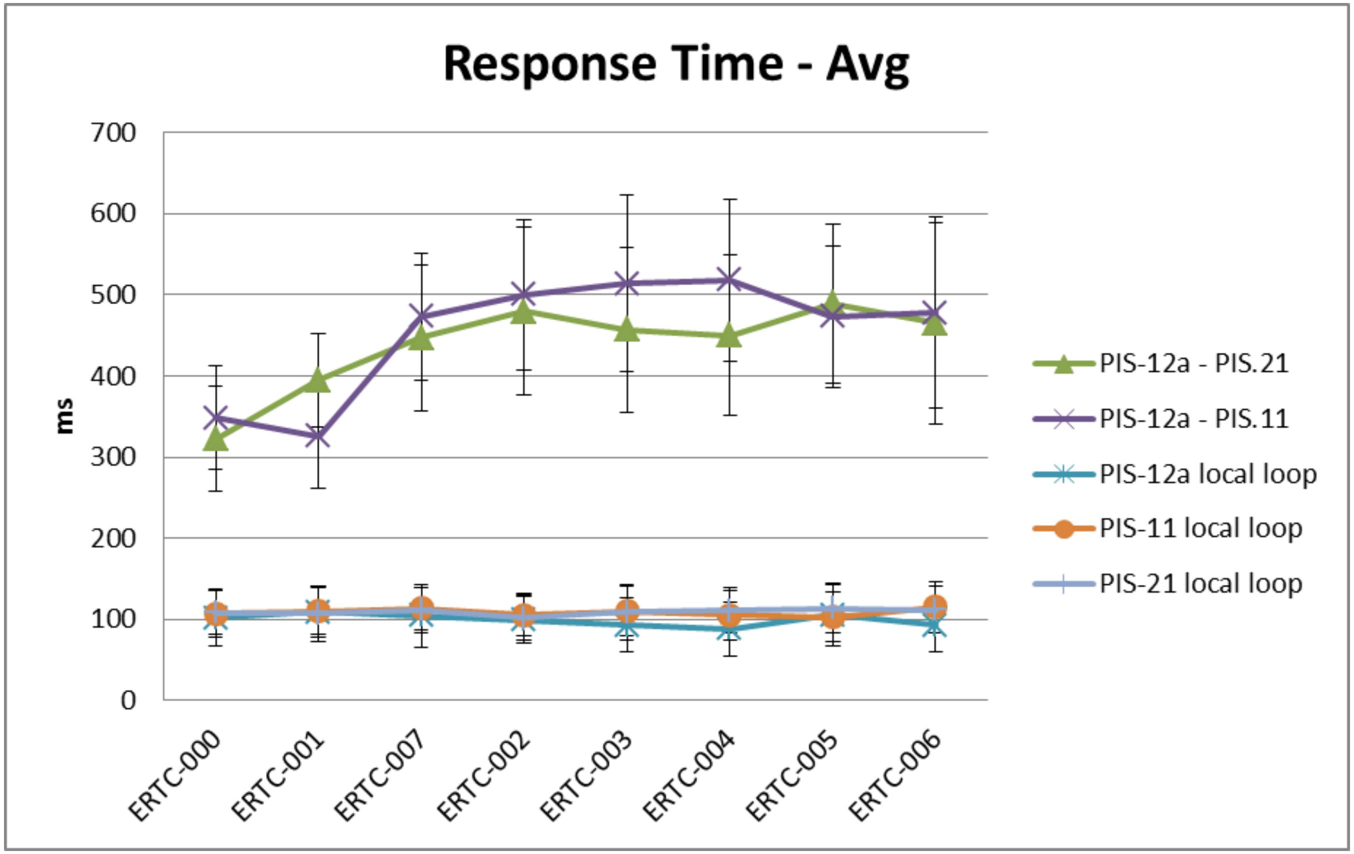
- ➢Keeping same configuration, increasing number of partners
- ➢From 8 comm.blocks (3 contracts)
- ➢Up to 30 comm.block (5 contracts)

➢Up to 15 partners,

Reasonable performance



Test results



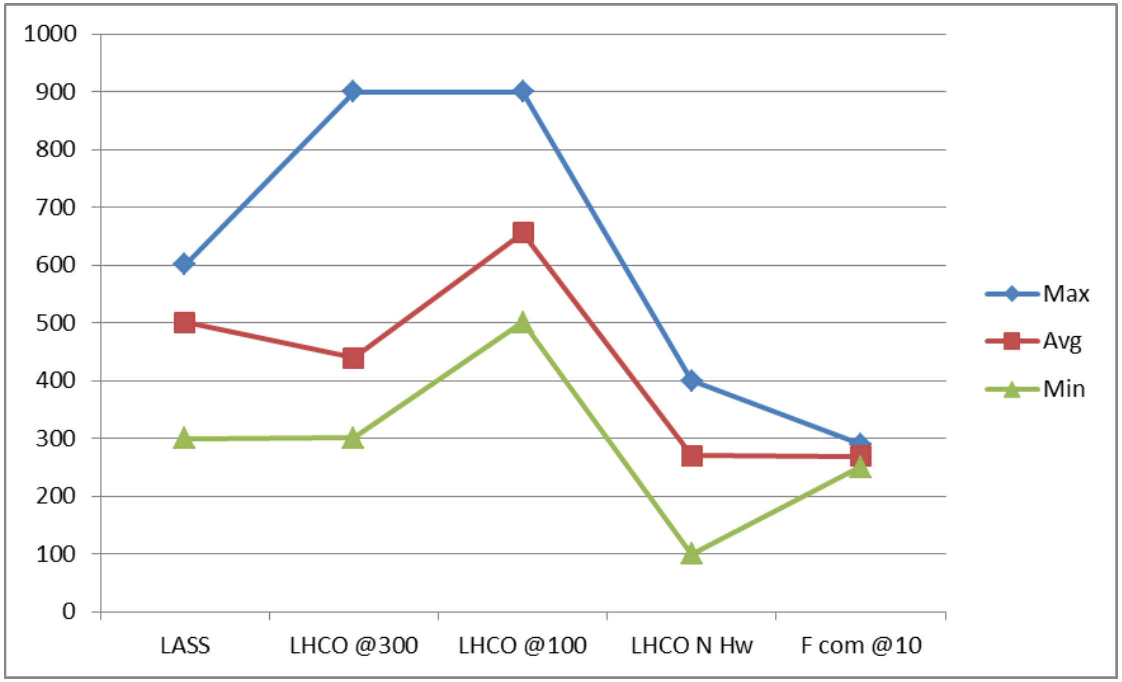
- ➢Execution time for local and central function; close to the limits

Hardware analysis

Average CPU execution times:

	414-4H	414-5H	416-5H	417-5H
Fixed.p.	45 ns	18,7 ns	12,5 ns	7,5 ns
Float.p.	135 ns	37,5 ns	25 ns	15 ns

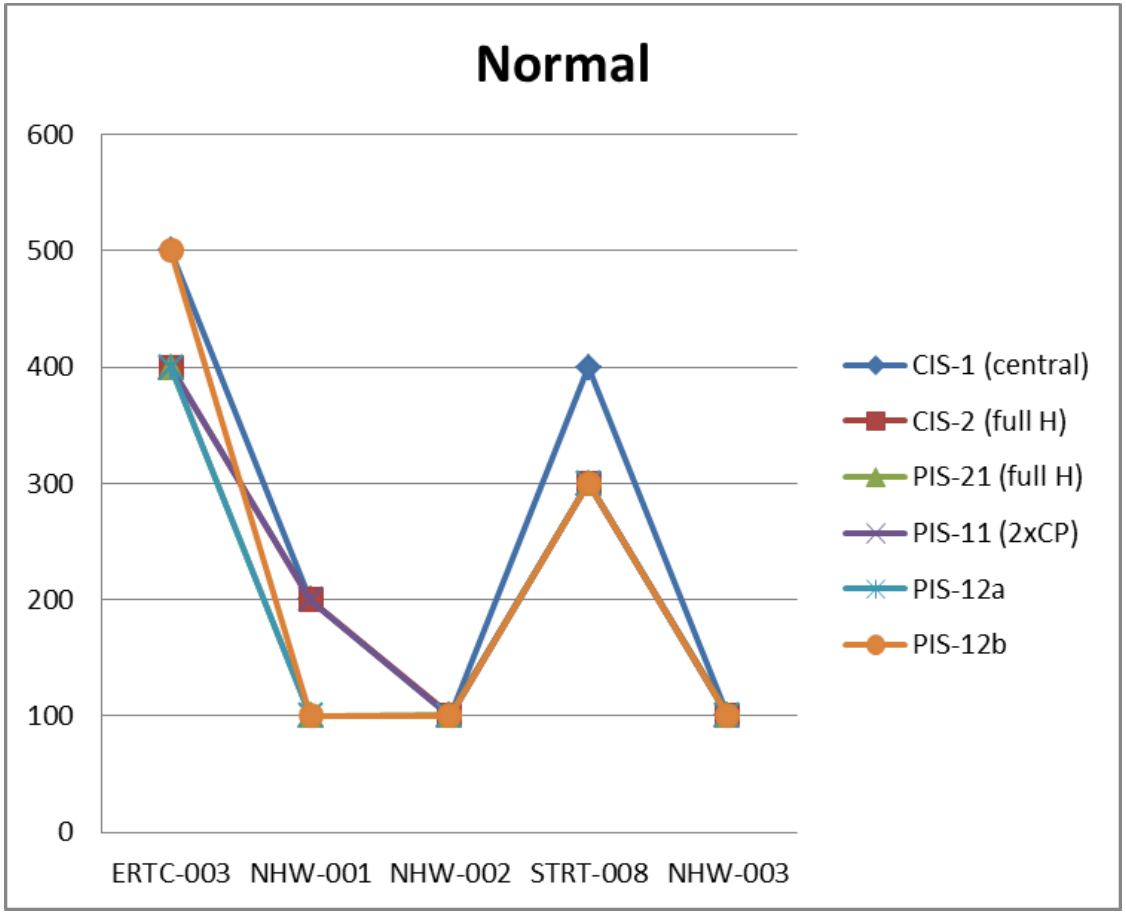
- **Following analysis by Nacho…**

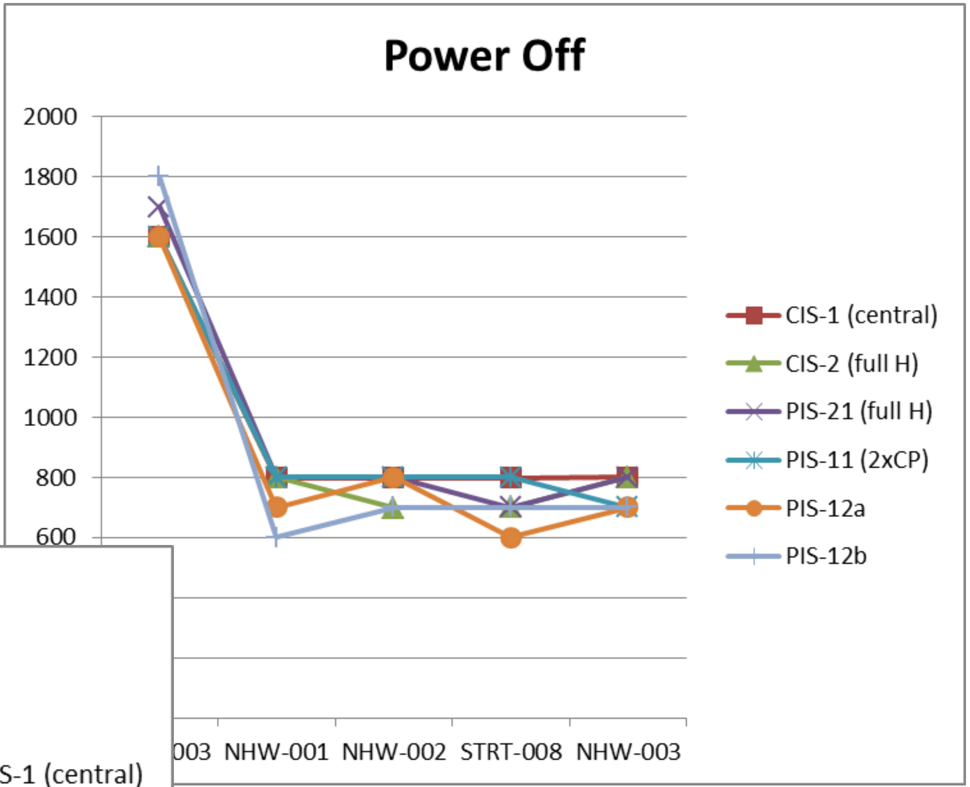


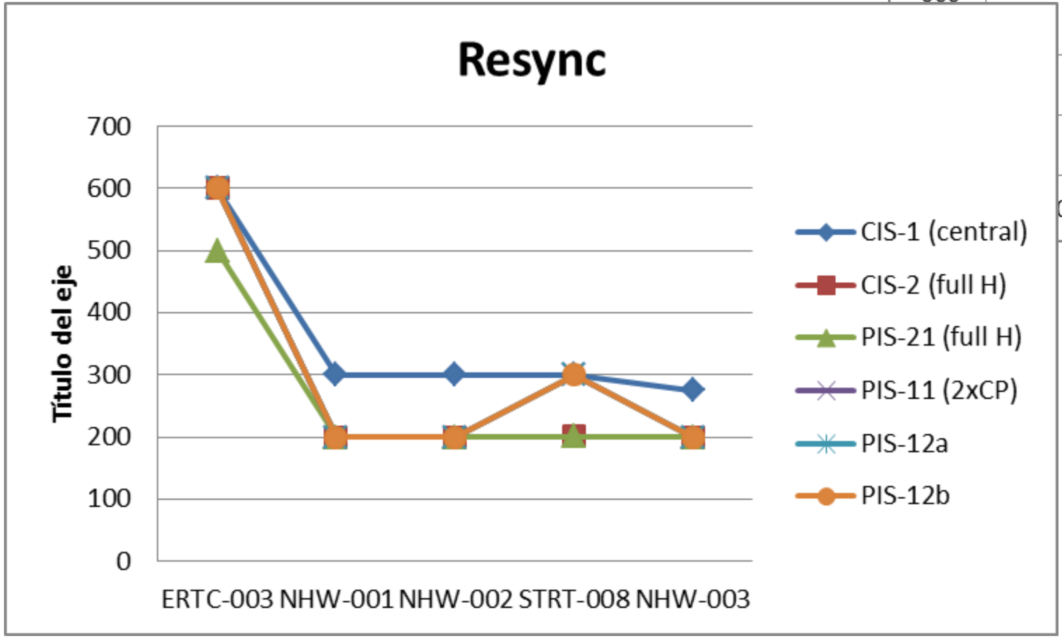
Test results

New hardware campaign:

- CPU: 417-5H
- 14 comm. blocks
- Important reduction in time




Power Off
2000
1800
1600
1400
1200
1000
800
600
003 NHW-001 NHW-002 STRT-008 NHW-003
CIS-1 (central)
CIS-2 (full H)
PIS-21 (full H)
PIS-11 (2xCP)
PIS-12a
PIS-12b


Resync
Titulo del eje
700
600
500
400
300
200
100
0
ERTC-003 NHW-001 NHW-002 STRT-008 NHW-003
CIS-1 (central)
CIS-2 (full H)
PIS-21 (full H)
PIS-11 (2xCP)
PIS-12a
PIS-12b

Test results

Initial conclusions:

- Critical management of time-outs
- Resynchronization: very dependent on the volume of data managed
- Failure in one CPU does not affect the performance of the others or the network
- Correct tuning of the CPU parameters is essential to optimize CPU and communications throughput
- But, only CPU was changed, other pieces of hw could be improved as well

Communications using S7 safety profile:

- Seems more disadvantages than advantages
- gets worse with traffic in the network
- possibility to switch to distributed I/O for critical signals
-

Test results