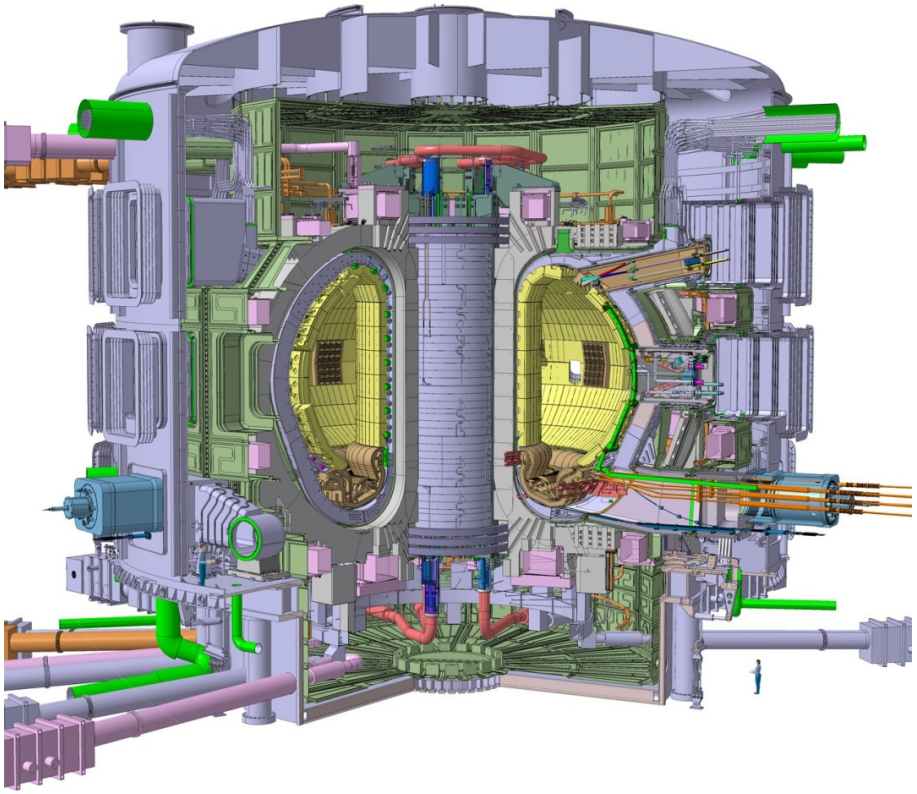
ITER magnet powering interlocks prototype



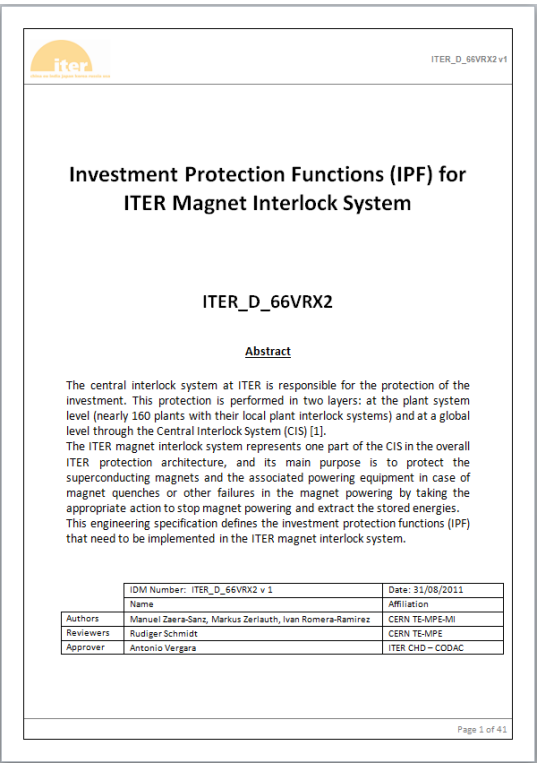
Manuel Zaera Sanz – GSI M.ZaeraSanz@gsi.de

Ivan Romera Ramirez - CERN Ivan.Romera.Ramirez@cern.ch

Agenda

1. Mission statement
2. Protection against
3. Initial approach
4. ITER Magnet Powering Interlock prototype
5. Conclusions and further work

1. Mission statement



ITER_D_66VRX2 v1

Investment Protection Functions (IPF) for ITER Magnet Interlock System

ITER_D_66VRX2

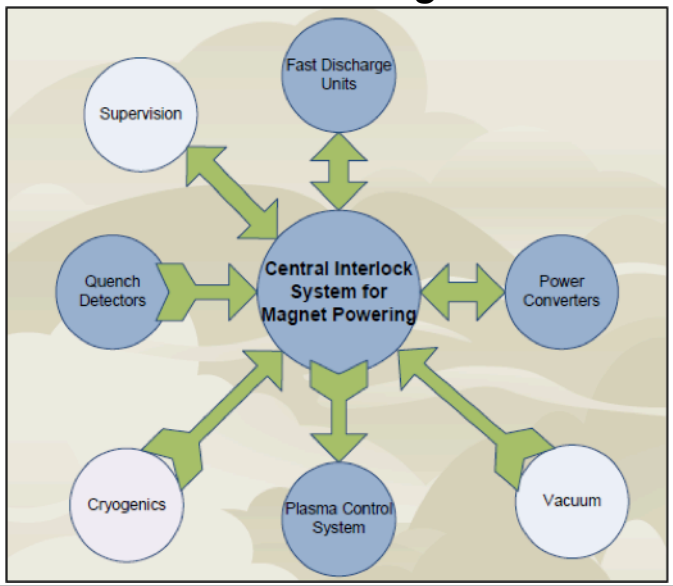
Abstract

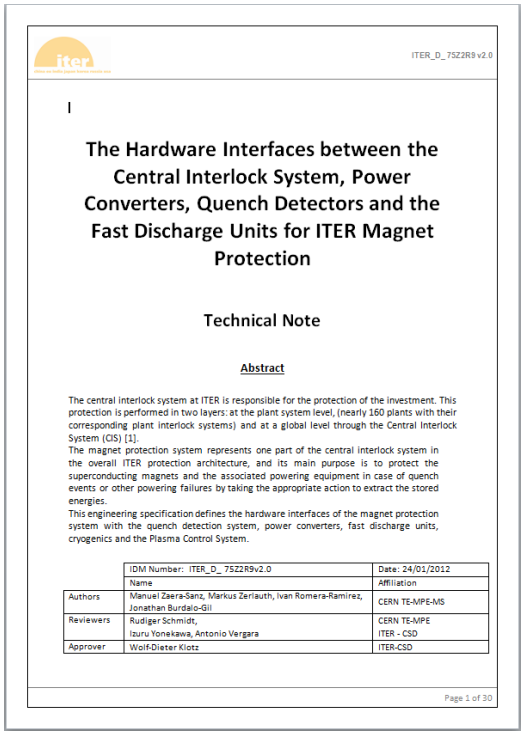
The central interlock system at ITER is responsible for the protection of the investment. This protection is performed in two layers: at the plant system level (nearly 160 plants with their local plant interlock systems) and at a global level through the Central Interlock System (CIS) [1].
The ITER magnet interlock system represents one part of the CIS in the overall ITER protection architecture, and its main purpose is to protect the superconducting magnets and the associated powering equipment in case of magnet quenches or other failures in the magnet powering by taking the appropriate action to stop magnet powering and extract the stored energies.
This engineering specification defines the investment protection functions (IPF) that need to be implemented in the ITER magnet interlock system.

	IDM Number: ITER_D_66VRX2 v 1	Date: 31/08/2011
	Name	Affiliation
Authors	Manuel Zaera-Sanz, Markus Zerlauth, Ivan Romera-Ramirez	CERN TE-MPE-MI
Reviewers	Rudiger Schmidt	CERN TE-MPE
Approver	Antonio Vergara	ITER CHD – CODAC

Page 1 of 41

Protect the superconducting magnets and the associated powering equipment in case of magnet quenches or other failures in the magnet powering by relaying signals between the different actors in the magnet/circuit protection to stop magnet powering and extract the stored energies





ITER_D_75Z2R9 v2.0

The Hardware Interfaces between the Central Interlock System, Power Converters, Quench Detectors and the Fast Discharge Units for ITER Magnet Protection

Technical Note

Abstract

The central interlock system at ITER is responsible for the protection of the investment. This protection is performed in two layers: at the plant system level, (nearly 160 plants with their corresponding plant interlock systems) and at a global level through the Central Interlock System (CIS) [1].
The magnet protection system represents one part of the central interlock system in the overall ITER protection architecture, and its main purpose is to protect the superconducting magnets and the associated powering equipment in case of quench events or other powering failures by taking the appropriate action to extract the stored energies.
This engineering specification defines the hardware interfaces of the magnet protection system with the quench detection system, power converters, fast discharge units, cryogenics and the Plasma Control System.

	IDM Number: ITER_D_ 75Z2R9v2.0	Date: 24/01/2012
	Name	Affiliation
Authors	Manuel Zaera-Sanz, Markus Zerlauth, Ivan Romera-Ramirez, Jonathan Burdalo-Gil	CERN TE-MPE-MS
Reviewers	Rudiger Schmidt, Izuru Yonekawa, Antonio Vergara	CERN TE-MPE ITER - CSD
Approver	Wolf-Dieter Klotz	ITER-CSD

Page 1 of 30

2. Protection against...

- **Magnet powering** system failures (not being exhaustive):
  - Magnet quenches
  - FDUs spurious openings
  - Power Converter failures
  - ...

- Failures of the **protection equipment**
  - Quench detector failures
  - FDUs internal failures

- **External system** failures: Cryogenics

Protection against...

How to **implement** such protection?

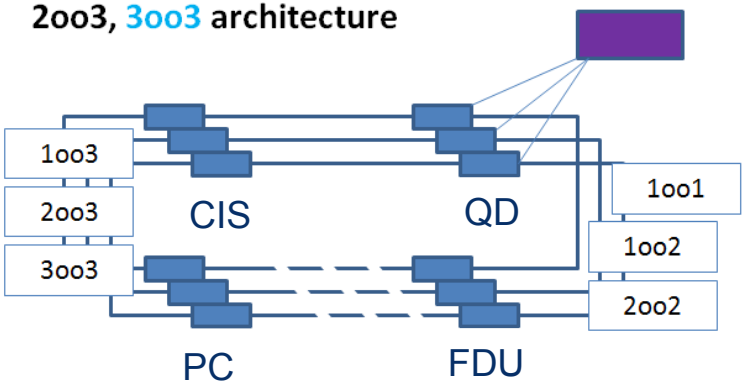
- **PLC based** technology: S7400 series according to ITER interlocks architecture
- Use of **current loops** to meet dependability requirements (ITER specification: one false trigger of the system in 20 years)
- **Several prototypes** developed according to achievements and knowledge obtained after testing
  - Redundant + Safety configuration: **FH solution + 2oo3**
  - Redundant configuration: **H solution + 2oo3**

3. Initial approach: 2oo3 justification

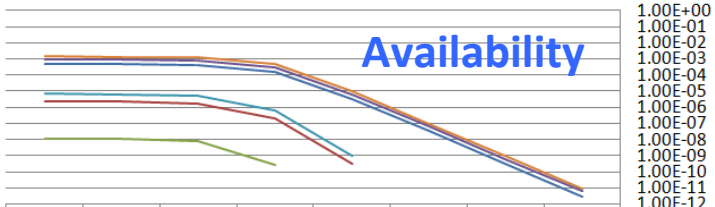
Dependability requirements of ITER for **high safety AND availability** are huge challenge for machine protection systems

Dependability studies done, confirming 2oo3 architecture as the most suited candidate to meet dependability requirements

Comparison between 1oo1, 1oo2, 1oo3 , 2oo2 2oo3, 3oo3 architecture

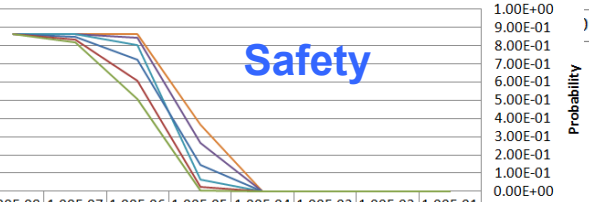


n:250, Demand missed B6A



	1.00E-08	1.00E-07	1.00E-06	1.00E-05	1.00E-04	1.00E-03	1.00E-02	1.00E-01
3003	1.40E-03	1.39E-03	1.25E-03	4.77E-04	9.49E-06	9.62E-08	9.63E-10	9.00E-12
2002	9.37E-04	9.27E-04	8.35E-04	3.18E-04	6.33E-06	6.42E-08	6.42E-10	6.00E-12
2003	6.63E-06	6.47E-06	5.10E-06	6.19E-07	9.54E-10	0.00E+00	0.00E+00	0.00E+00
						3.21E-08	3.21E-10	3.00E-12
						0.00E+00	0.00E+00	0.00E+00
						0.00E+00	0.00E+00	0.00E+00

n:250, Mission completed B7

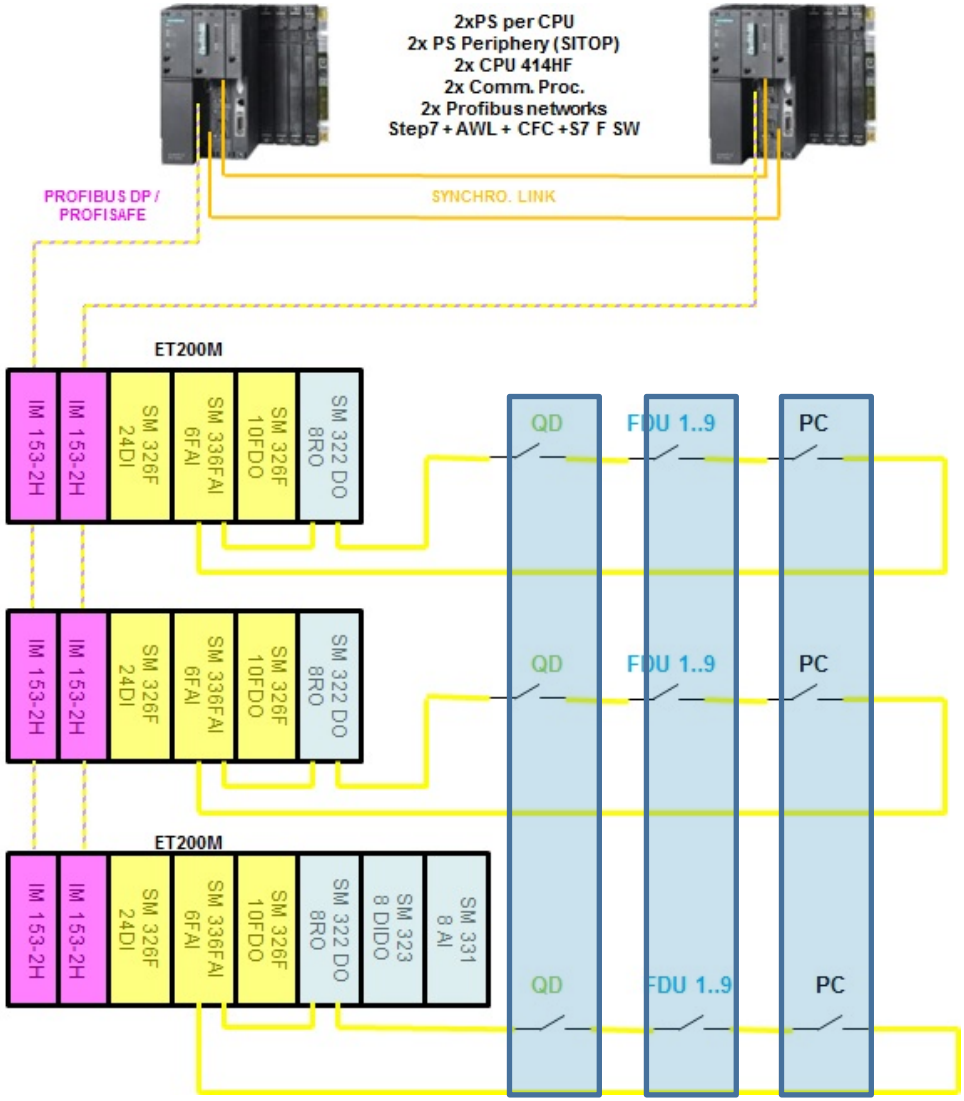


	1.00E-08	1.00E-07	1.00E-06	1.00E-05	1.00E-04	1.00E-03	1.00E-02	1.00E-01
3003	8.66E-01	8.66E-01	8.62E-01	3.64E-01	4.23E-08	0.00E+00	0.00E+00	0.00E+00
2002	8.66E-01	8.66E-01	8.43E-01	2.64E-01	2.82E-08	0.00E+00	0.00E+00	0.00E+00
2003	8.66E-01	8.65E-01	8.04E-01	6.39E-02	0.00E+00	0.00E+00	0.00E+00	0.00E+00
1001	8.64E-01	8.50E-01	7.24E-01	1.44E-01	1.41E-08	0.00E+00	0.00E+00	0.00E+00
1002	8.63E-01	8.35E-01	6.05E-01	2.40E-02	0.00E+00	0.00E+00	0.00E+00	0.00E+00
1003	8.61E-01	8.21E-01	5.06E-01	3.99E-03	0.00E+00	0.00E+00	0.00E+00	0.00E+00

λf

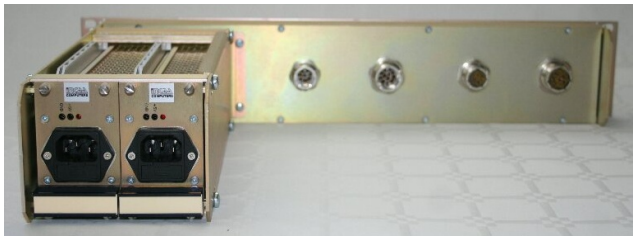
Courtesy of S.Wagner

Initial approach: CIS for MPI. Ex: DL TF

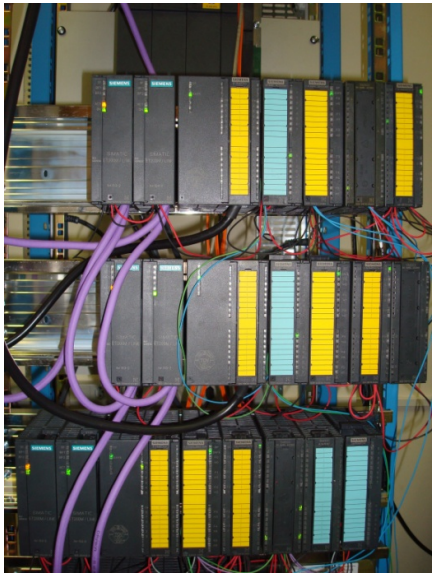


Standard interface between user and the discharge loop

- CERN CIBU inspired
- Configurable 1oo2/2oo3
- Actel FPGA (radiation tolerant, candidate for future use in CERN CIBU)
- Profibus/Profinet ASIC for remote test and monitoring through PLC

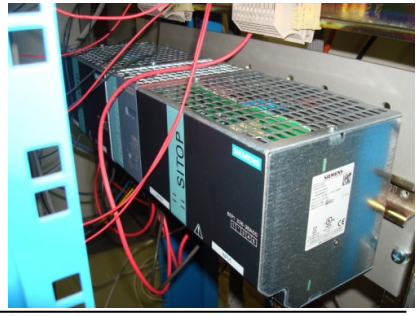


Initial approach: Implementation

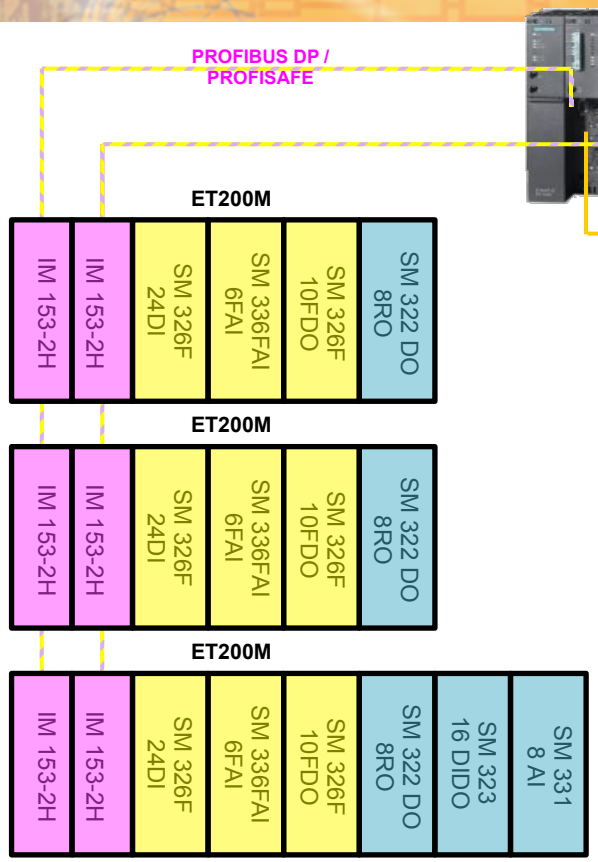


2x Power Supplies PS 407 10A R per CPU
2x CPUs 414-4H (FH configuration)
2x FO links per CPU
2x Communication processors CP 443-1 Adv
Profibus/Profinet/Ethernet/MPI networking
Step7 + AWL + CFC + S7 F Software certified

2x Profibus/ProfiSafe networks (1 per CPU)
2x IM153-2 per ET200M slave
3 ET200M in total
One Profibus connection per IM
FDI, FAI, FDO, DIDO and RO modules
Redundant Powering (SITOP 20A)



Initial approach: Measurements



MEASUREMENTS OF KEY RESPONSE TIMES (Failsafe and Redundant or only Redundant configurations)

- FROM INPUT TO OUTPUT
  (Ex: From Cryogenics fault to command Plasma Control System)
- FROM INPUT TO OPEN CURRENT LOOP
  (Ex: From Cryogenics fault to open powering permission loop)
- FROM OPEN CURRENT LOOP TO OUTPUT
  (Ex: From Quench to command Plasma Control System)
- FROM OPEN CURRENT LOOP TO OPEN ANOTHER CURRENT LOOP
  (Ex: From Quench to remove powering permission)

TEST EQUIPMENT

Profibus speed	12Mbps
Scan Cycle Time (shortest, longest)	7ms (1ms,10ms)
Safety program located in OB35	15ms period, priority 12

Initial approach: Response times

		EXAMPLE	FAILSAFE & REDUNDANT CONFIGURATION	REDUNDANT CONFIGURATION
FROM INPUT TO OUTPUT		From Cryogenics fault to PCS	42ms 	7ms 
FROM INPUT TO OPEN LOOP		From Cryogenics fault to remove powering permission	61ms 	18ms 
FROM OPEN LOOP TO OUTPUT	Wire Break	From Quench to command PCS	144ms 	-
	I<Imax		387ms 	169ms (1 Channel) 402ms (4 Channels) 664ms (8 Channels) 
	DI		42ms 	7ms 
FROM OPEN LOOP TO OPEN ANOTHER OPEN LOOP	Wire Break	From Quench to remove powering permission	120ms 	-
	I<Imax		134ms 	199ms (1 Channel) 379ms (4 Channels) 700ms (8 Channels) 
	DI		61ms 	18ms 

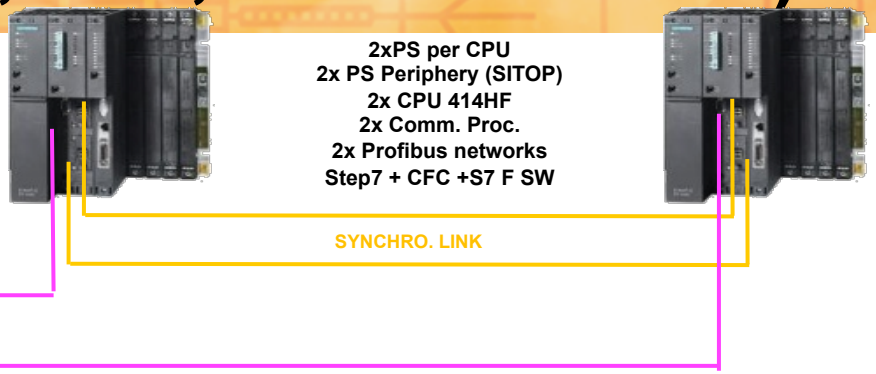
Initial approach: Conclusions

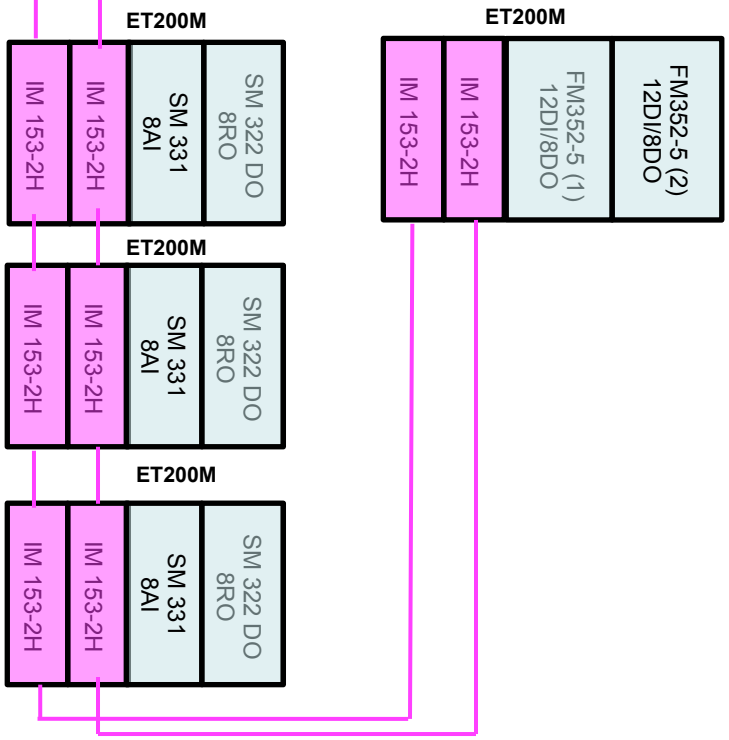
- Based on the measured **response times**
- Based on **MTBF** figures from SIEMENS catalog, standard modules have a factor 3 to 5 less likelihood to fail than safety ones
- Based on the **minimization** of the amount of **current loops** thanks to the use of PROFINET/PROFISAFE to provide SIL3 signals exchange between the plant interlock systems. Ex: Cryo, PCS, PP, PF, FDUQD-F

Our proposal consists on:

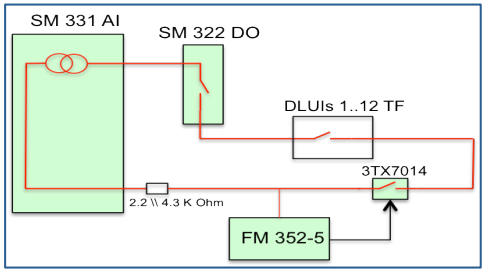
- Failsafe redundant solution **S7400FH**: CPU to CPU communications
- **Discharge loops** implementation:
  - Only **standard modules** in the ET200M slaves
  - **2oo3** configuration of I/O modules
  - **FM352-5** high speed boolean proc. to increase dependability and decrease the reaction time of critical investment protection functions
  - Use of **user interface boxes** for clients connectivity and diagnostics

4. ITER MPI prototype: Architecture for 6 loops (1TF, 2PF, 2CS and 1CC)

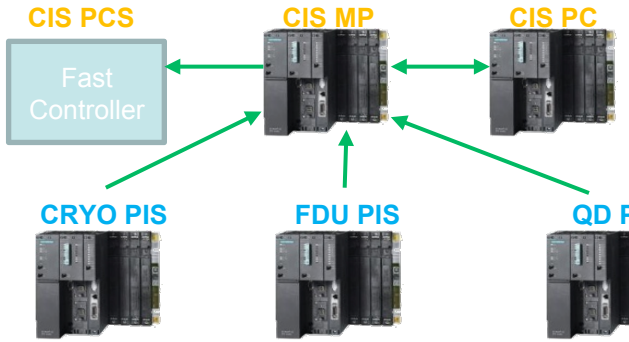




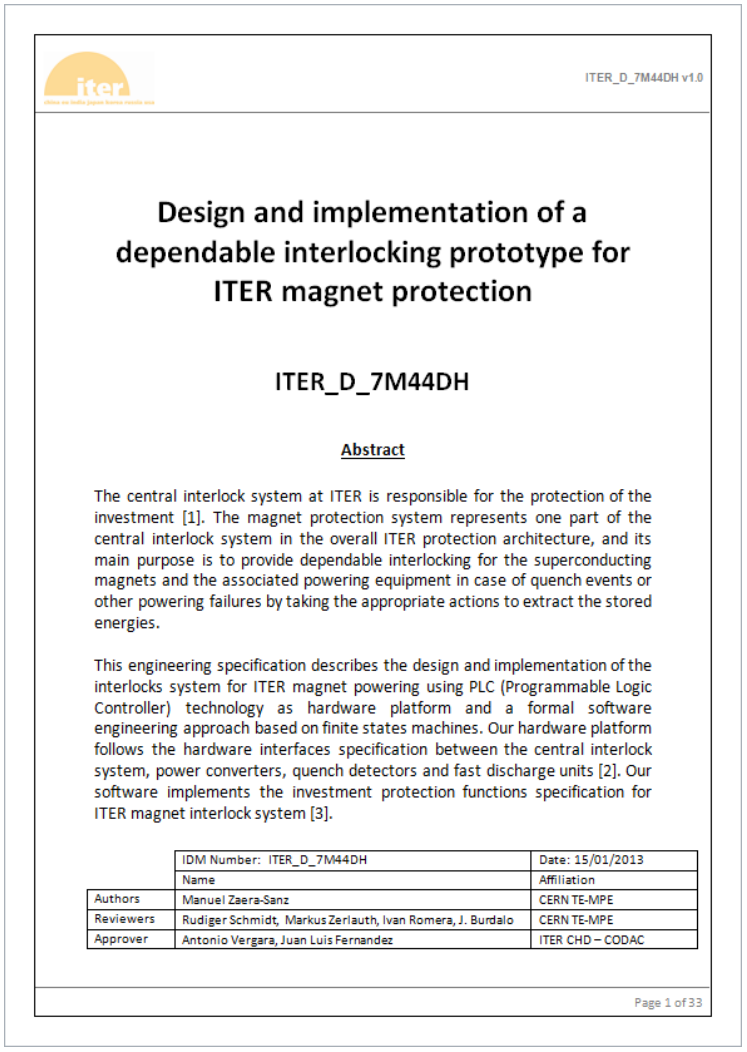
Discharge Loops (2oo3). Example: TF



CRYO, PCS, PP,PF, FDUQD-F : Profinet/Profisafe (CIN)



ITER MPI prototype: Documentation and HW implementation



ITER_D_7M44DH v1.0

Design and implementation of a dependable interlocking prototype for ITER magnet protection

ITER_D_7M44DH

Abstract

The central interlock system at ITER is responsible for the protection of the investment [1]. The magnet protection system represents one part of the central interlock system in the overall ITER protection architecture, and its main purpose is to provide dependable interlocking for the superconducting magnets and the associated powering equipment in case of quench events or other powering failures by taking the appropriate actions to extract the stored energies.

This engineering specification describes the design and implementation of the interlocks system for ITER magnet powering using PLC (Programmable Logic Controller) technology as hardware platform and a formal software engineering approach based on finite states machines. Our hardware platform follows the hardware interfaces specification between the central interlock system, power converters, quench detectors and fast discharge units [2]. Our software implements the investment protection functions specification for ITER magnet interlock system [3].

	IDM Number: ITER_D_7M44DH	Date: 15/01/2013
	Name	Affiliation
Authors	Manuel Zaera-Sanz	CERN TE-MPE
Reviewers	Rudiger Schmidt, Markus Zerlauth, Ivan Romera, J. Burdalo	CERN TE-MPE
Approver	Antonio Vergara, Juan Luis Fernandez	ITER CHD – CODAC

Page 1 of 33

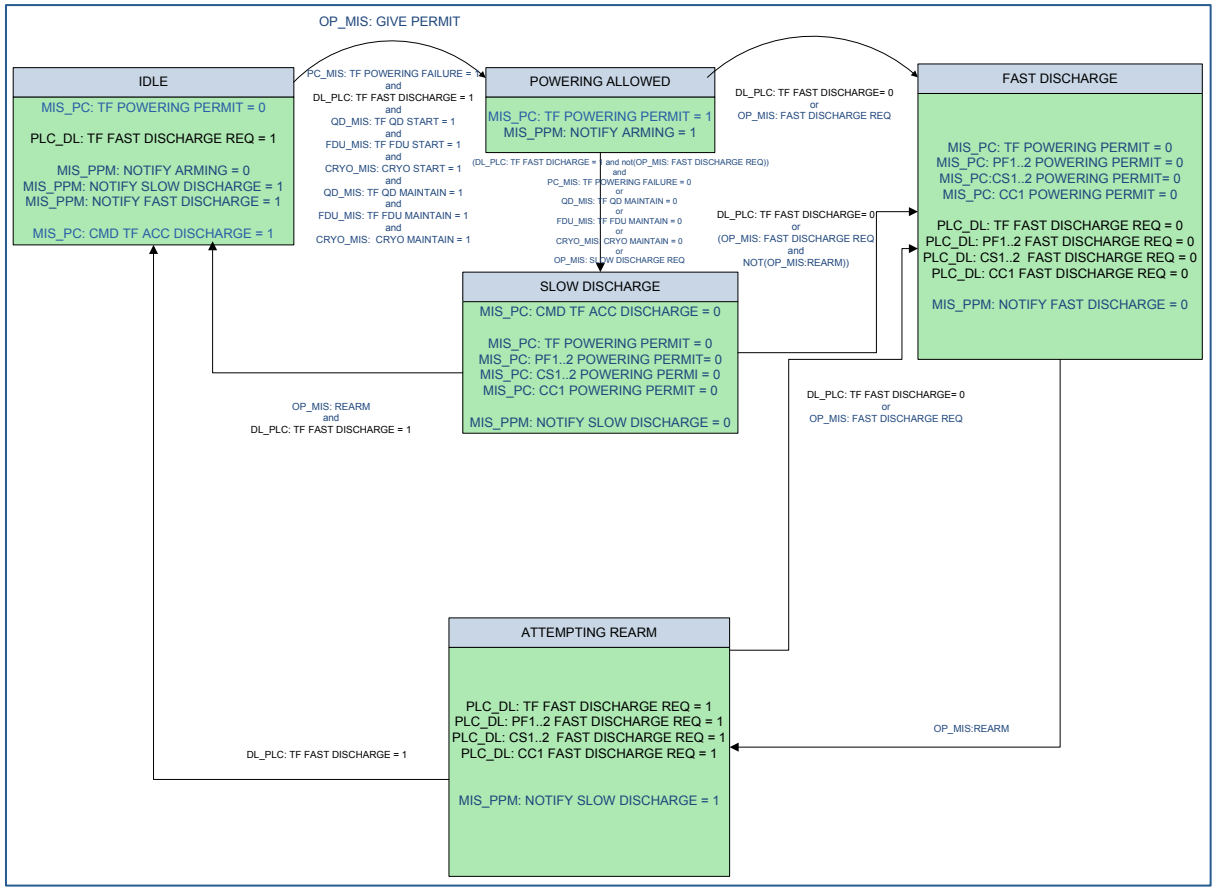
ITER MPI prototype: high dependability

- **Discharge loops**:
  - **High dependability** achieved thanks to redundant and independent processing units: S7400FH CPUs and FM352-5 FPGAs
  - **Independent software** development and **compilation** for CPUs and FPGAs
  - **Independent** and redundant **sensing** and **actuating** equipment:
    - Sensing: CPUs use AI modules, FPGAs hardwires
    - Actuating: CPUs use RO modules, FPGAs use discrete relays
    - PLC I/O modules physically arranged into different ET200M slaves

- Remaining signals exchanged by **PROFINET/PROFISAFE** with **CPU to CPU** communications (Not yet evaluated)

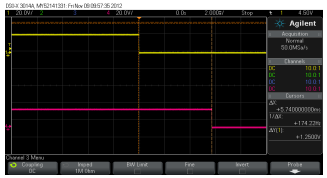
ITER MPI prototype: SW implementation

- Control **software** implemented following a **formal approach** from states diagrams until obtaining the state and output equations. Ex: Toroidal field family of circuits

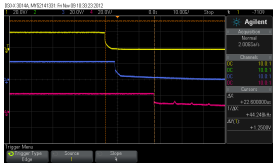


ITER MPI prototype: Response time

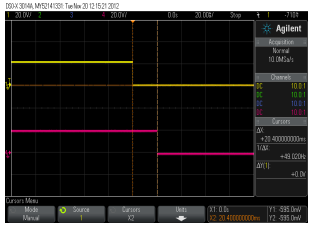
- Measured using **two software pieces** running in **parallel**:
  - **OB34**@10ms for the slow controls (H CPU) and acting on the RO PLC modules
  - **FB3 and FB5** for the fast controls (FM352-5 FPGAs) and acting on the discrete mechanical relays
- Results:
  - From a **quench to opening relay**: 5.74 ms
    (FM program + mechanical relay to open)



  - **Propagation of a quench** in one circuit to another: 22.6µs
    (FM program of 1st FPGA plus FM program of 2nd FPGA)



  - **From a quench to opening relay**: 20.4 ms
    (H program + RO module relay opens)



5. Conclusions and Further work

- **Promising results** of this prototype easily **scalable** to the 21 circuits
- **High dependability** achieved thanks to the redundancy of equipment in hardware and software
- Adjusted **response times to deadlines** required for the process control
- A lot of effort in **formalizing technical specifications** in collaboration with external company (CSL)
- Still a **lot of pending work**:
  - Programming of the remaining signals exchange **CPU to CPU**
  - Evaluation of the **response time** considering the above software
  - Design and implementation of **automatic tests** generating all the possible paths in the states diagrams and evaluating the correctness of the system

THANK YOU!!!