



# Architectures for PLC based interlocks

Manuel Zaera Sanz

GSI - Helmholtzzentrum für Schwerionenforschung

[M.ZaeraSanz@gsi.de](mailto:M.ZaeraSanz@gsi.de) (CSCO-IC)

# Agenda

1. Reliability issues
2. Safety and redundant PLC solutions
3. Use of current loops for interlocks implementation using PLCs
4. Fieldbus technologies for interlocks operation
5. Use of high speed boolean processors for interlocks
6. Example: HTS current leads interlock system
7. Conclusions

# 1. Reliability issues. Some definitions

- **Dependability:** means guarantee of working. It implies all or a set of the next specifications
  - **Reliability:** means that the system works without interruptions
  - **Safety:** means that the system prevents catastrophic failures
  - **Availability:** means that the system is ready the maximum possible time
  - **Maintainability:** means that the system is easily repairable
  - **Security:** means that the system is prepared faced to external intrusions

# Reliability issues. HW & SW faults manifestation



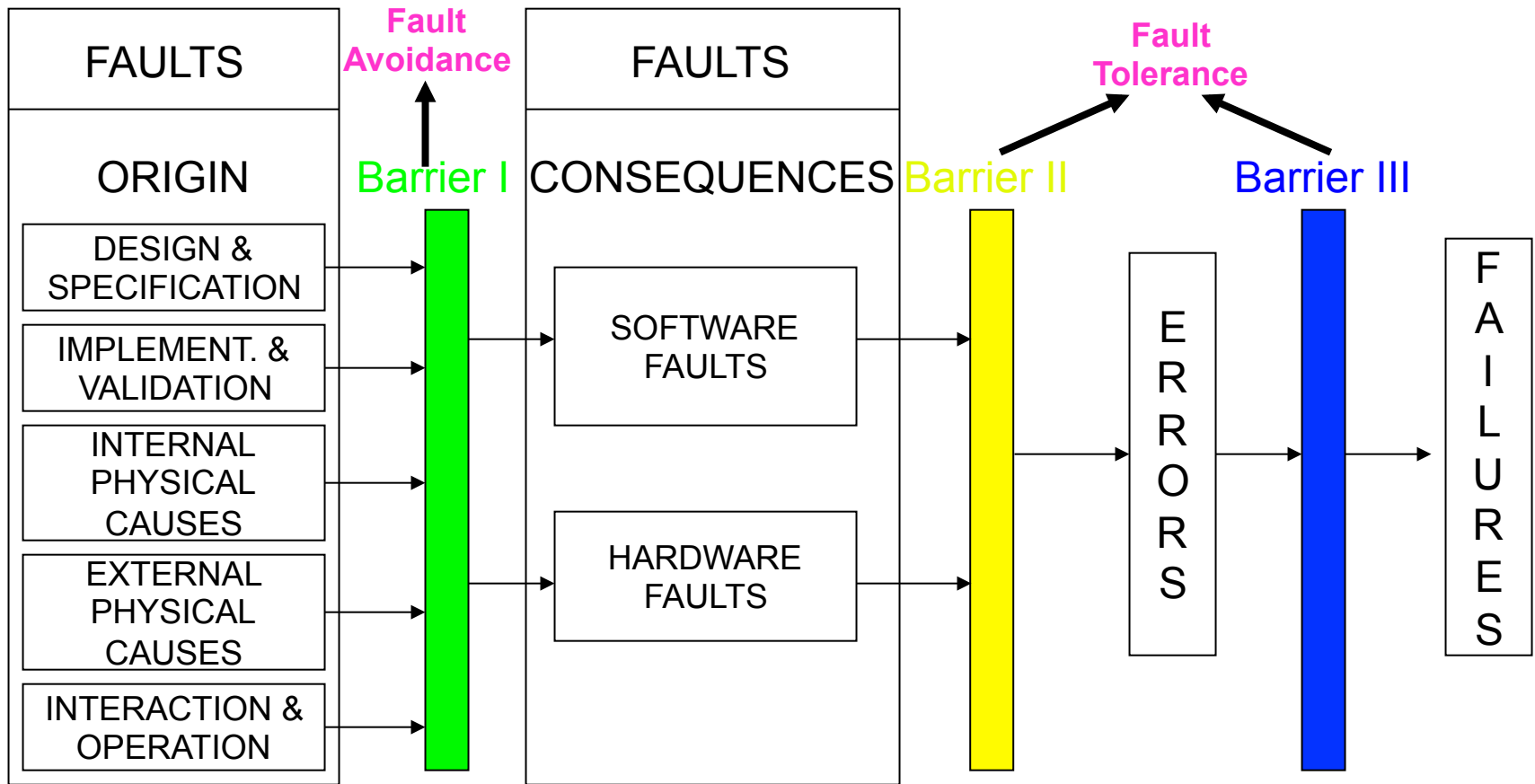
## - HW faults:

- Logic circuits: Stuck-at 0 or 1 (80%), open circuits,...
- ROM: Bad addressing, bad selection, bad cell content
- RAM: multiple writing, incorrect access time, transitory cell content change, pattern sensibility, no refresh, ...
- Microprocessors: invalid program flow (40%), incorrect opcode address, invalid read address, non existent memory, ...

## - SW faults:

- Computer crash (bug in the OS or program)
- Unlimited execution time of a program
- Unexpected results of computation
- Miss of deadlines in real-time applications

# Reliability issues. Barriers to prevent failures



## 2. Safety and redundant PLC solutions

- **Safety** means that the system prevents catastrophic failures performing fault detection and fault reaction functions at the CPU and I/O sides.
- **Availability** means that the system is ready the maximum possible time.
- **Safety families** (Siemens):
  - **Distributed safety** (F series): S7300F, S7400F, ET200S-F
  - **Process safety** (H or FH series): S7400H, S7400FH  
(Possibility of SW redundancy: S7300 and S7400 CPUs)
- **Implications?** MTBF, response times, delays, programming languages...

# Safety and Redundant PLC solutions.

## F series: Safety mechanisms

- **Fault detection and Fault reaction:**
  - Located in the safety program and F-I/O
  - Supported by the hardware and Operating system
- **Safety program (F-CPU):**
  - Fault detection:
    - Hardware: time monitoring (watch-dogs)
    - Software: Operating system (self-tests)
  - Fault reaction: lead the system to a safe state
  - Mechanisms: self tests, logical program execution & dataflow monitoring, failsafe user times, password protection (CPU & safety program)

# Safety and Redundant PLC solutions.

## F series: Safety mechanisms

### - F-I/O:

- Safety communications protocols between F-CPU & F-IOs following **PROFIsafe** specifications
- No possibility of direct **access to the periphery** (use of channel drivers)
- **“Health”** monitoring mechanisms
- SM-F modules: self detection of **wiring faults** (wire break)

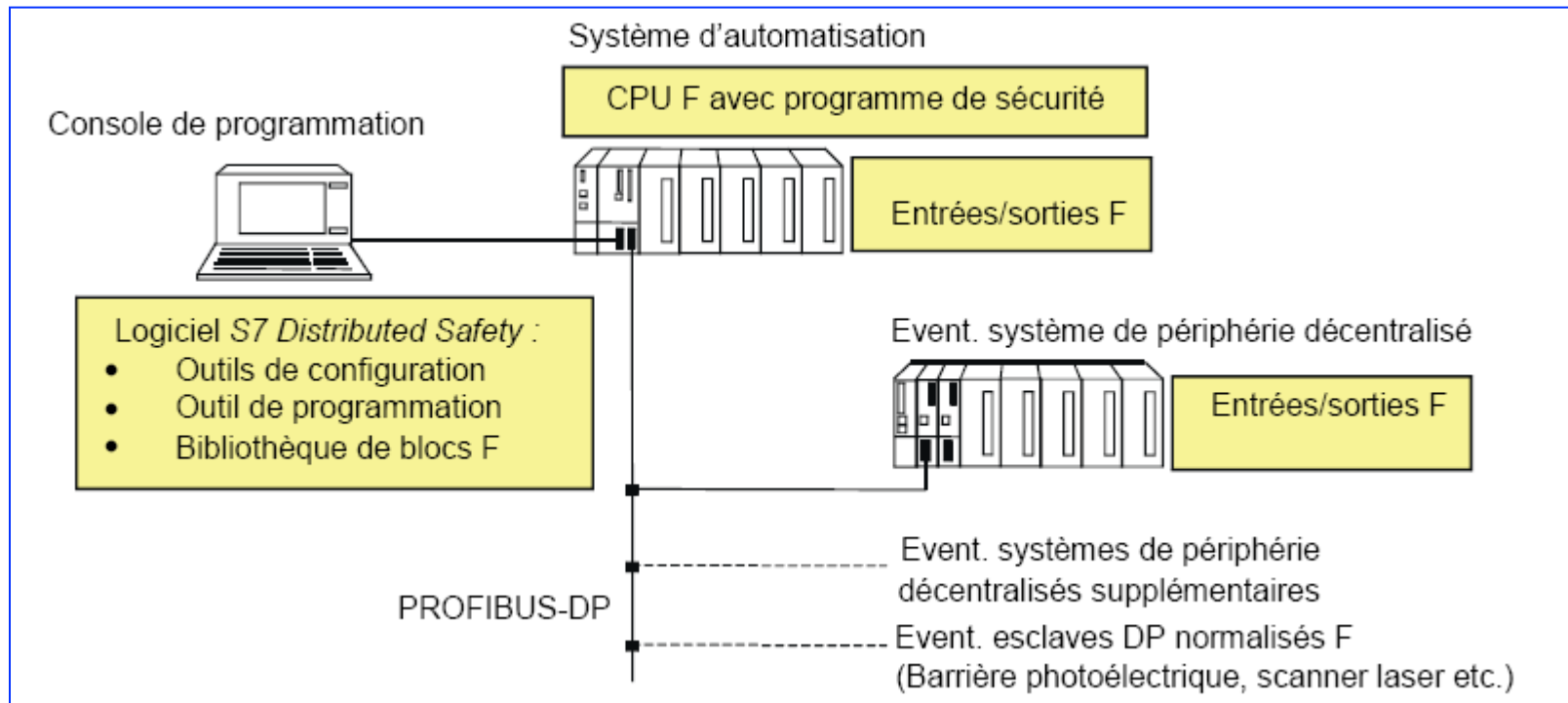
### - Safety fulfillments (standards):

- Requirement classes AK1 to AK6 in accordance with DIN V19250/  
DIM V VDE 0801
- SIL1 to **SIL3** in accordance with IEC 61508
- **Categories 1 to 4** in accordance with EN 954-1



# Safety and Redundant PLC solutions.

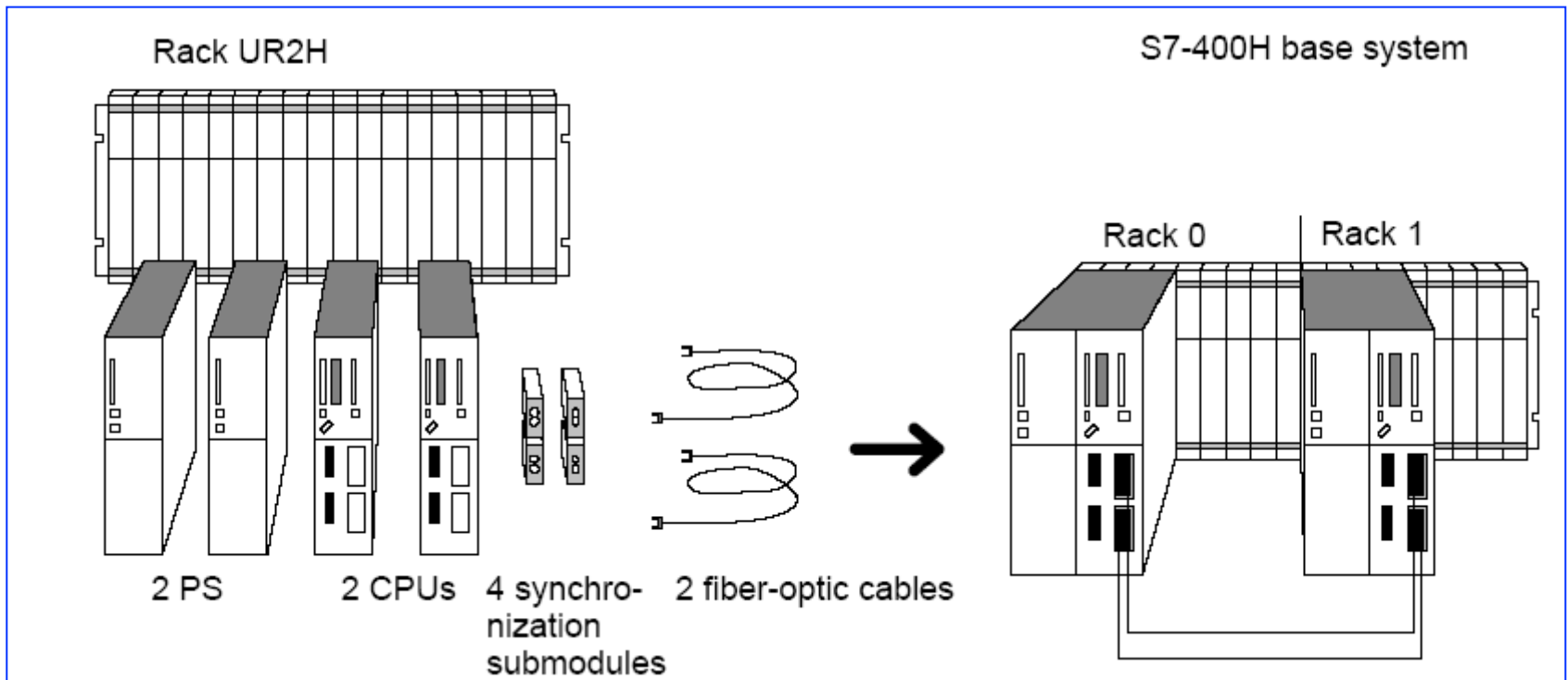
## F series: HW and SW architecture



# Safety and Redundant PLC solutions.

## H series: Redundant mechanisms

- **Basic components of an H CPU system**

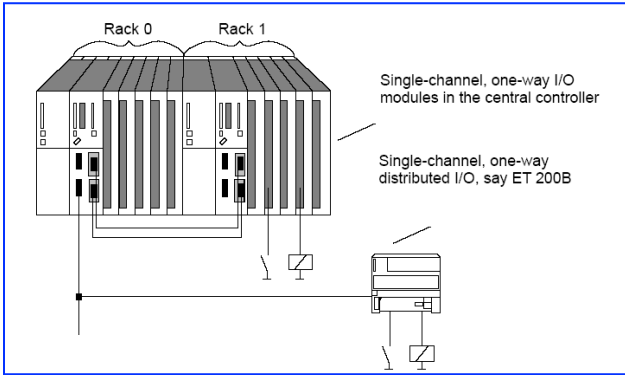


# Safety and Redundant PLC solutions.

## H series: Redundant mechanisms

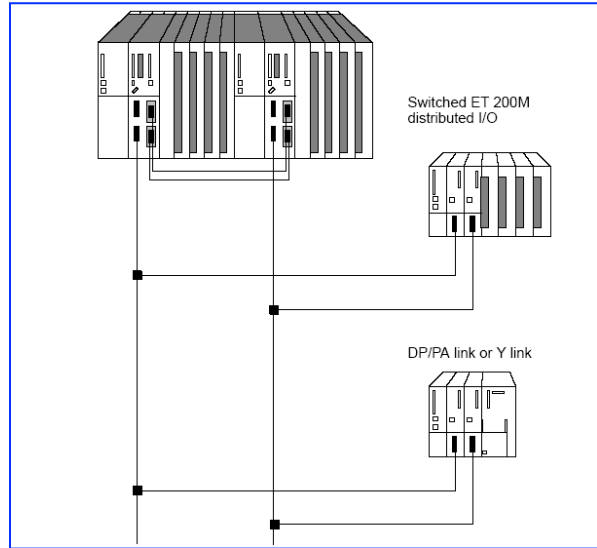
### - I/O configurations

Single channel, one way  
(Normal Availability I/O)



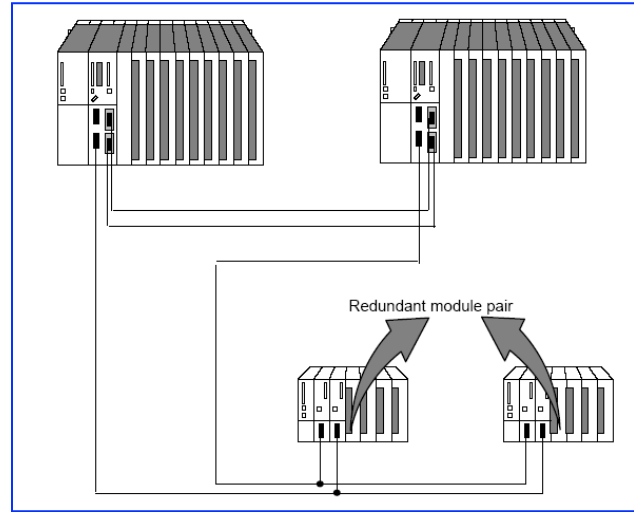
- No tolerance of the failure of single I/O modules
- Centrally or distributed
- I/O failure may generate a system failure

Single channel, switched I/O  
(Enhanced Availability)



Tolerate the failure of individual IM modules within the ET200  
(redundancy inside the ET200)

Dual channel, redundant I/O  
(+ Fault tolerance)



Tolerate the failure of individual modules between different ET200  
(redundancy of ET200)

### - Active bus modules for hot swap improving maintenance

# Safety and Redundant PLC solutions.

## F and H series: Gains

- **F series:** support of all the **safety** mechanisms detailed before
- **H series:** high **availability** providing
  - Additional redundancy error OBs
  - Additional SFC for fault-tolerant systems
  - Fault tolerant communication connections
  - Self-testing
  - Switched I/O
  - Additional monitoring and system status information
- **F + H: Safety + Availability**

# Safety and Redundant PLC solutions.

## F and H series: Impact

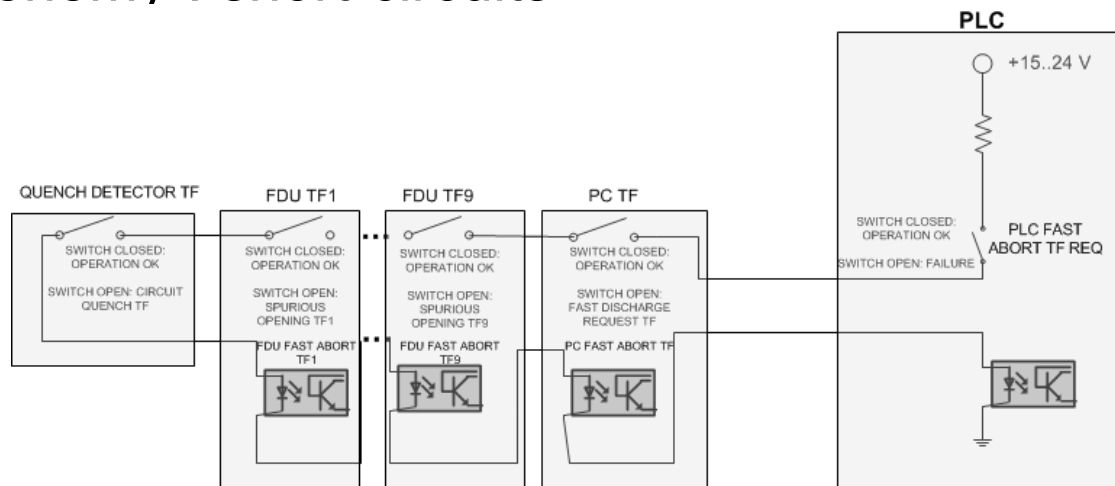
- **F series: “Big impact”**
  - The OS and compiler introduces many **SW modules** to improve safety
  - **MTBF** 3 to 5 times lower for F PLC modules
  - Increment on the **response time**
  - Higher **price** compared to standard series
  - **Closed programming** environment: Distributed Safety (F-LAD, F-FBD), Process Safety (CFC + F libraries for FH series, open for H series)
- **H series: “Little effect”...but exists**
  - **MTBF** of the synchronization modules (H config) is only 2 years
  - Depending on the SW, some **delays** due to CPUs synchronization or switch over may occur
  - **Transparent** for the programmer
  - H+F, the drawbacks of the F series have to be added + PROFIBUS/PROFISAFE delays + Restrictions on the programming languages

# 3. Use of current loops for interlocks implementation. Main features

## How to achieve high safety and/or availability interlocks system with PLC technology?

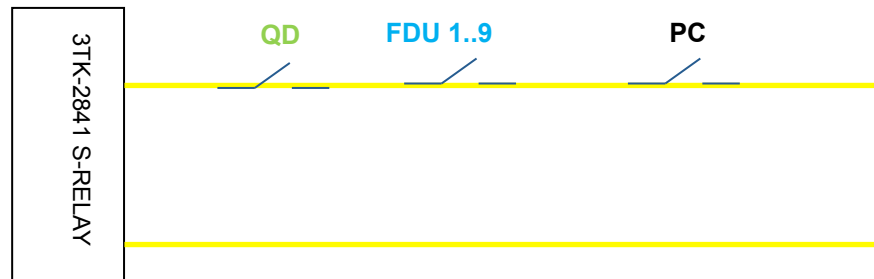
Interlock technique used: Current Loops

- **Fast** way (light speed) for interlock propagation and detection
- **Simple** interface requirements for detection and propagation of interlock signals
- Main „enemy“: short-circuits

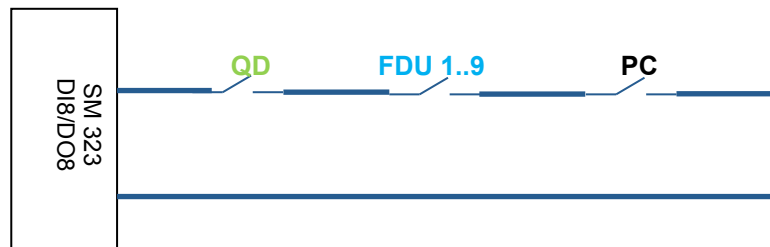


# Use of current loops for interlocks implementation. Implementation using PLC

- Use of Failsafe **discrete relays** (3TK2841). Limitation: 5mA current

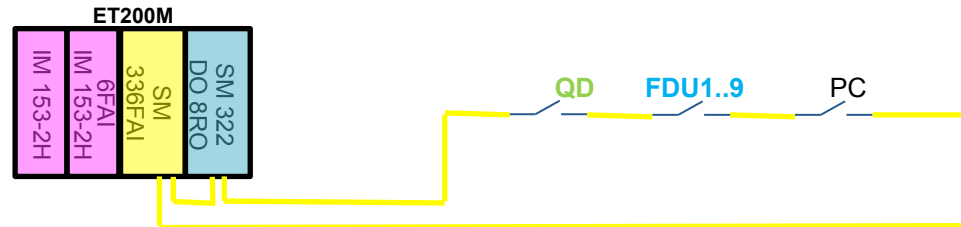


- Use of a **DI and DO** modules or DIDO modules

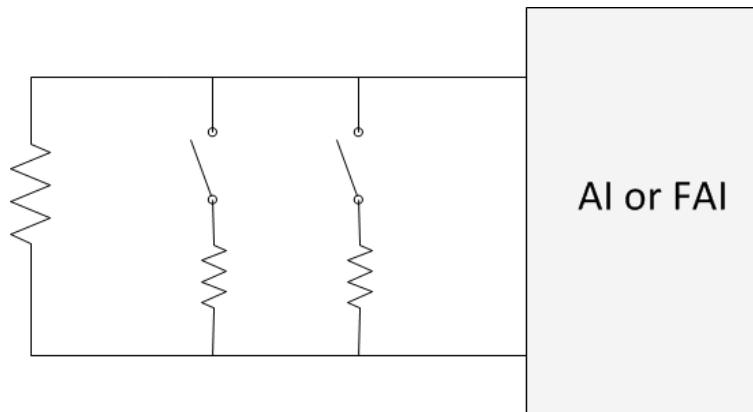


# Use of current loops for interlocks implementation. Implementation using PLC

- Use of **AI** or **FAI** modules



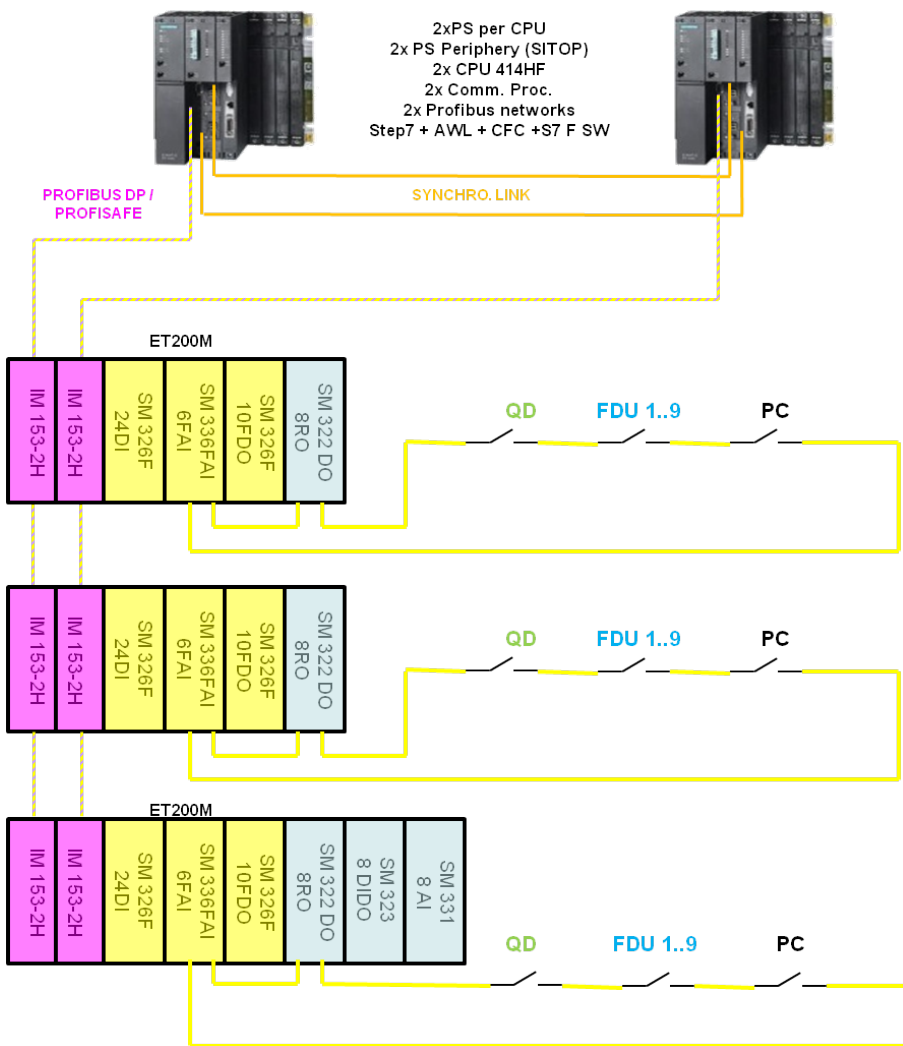
- Current loops for **another applications**





# Use of current loops for interlocks implementation. Integration in a FH system

## - FH system

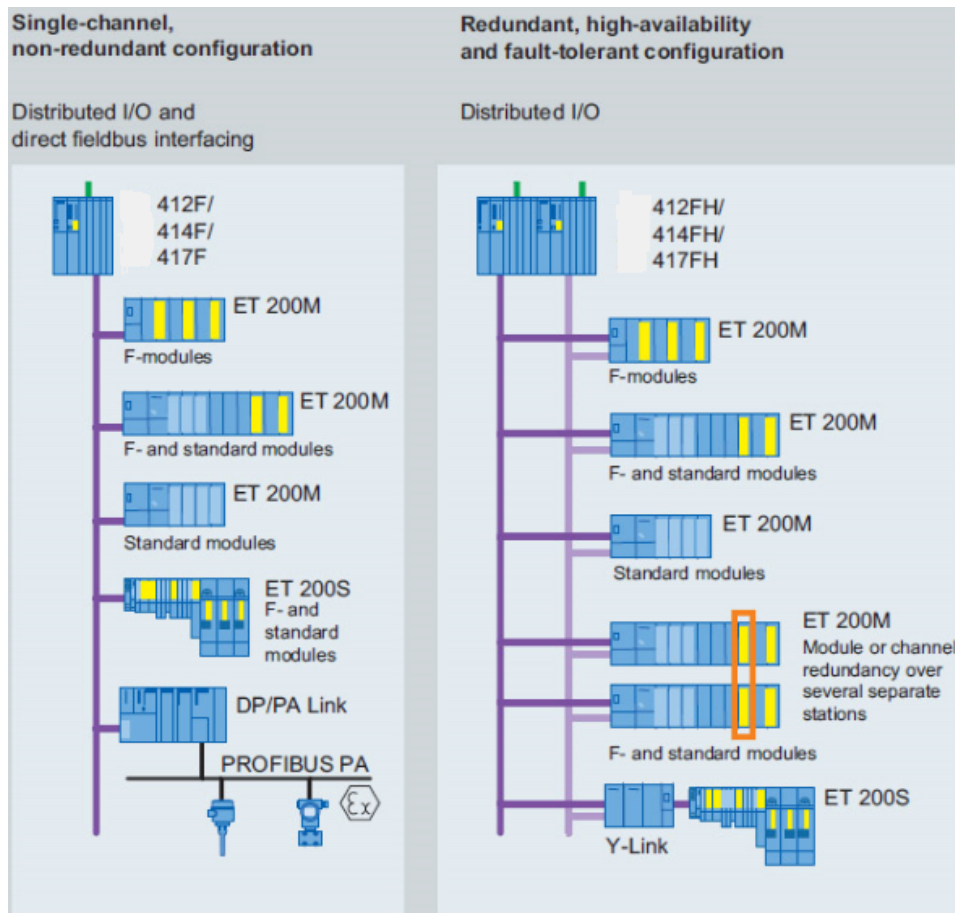


# 4. Fieldbus technologies for interlocks operation

- Need to perform **networking** of components conforming a distributed system
- Several solutions exist: Industrial Ethernet, **PROFIBUS** and **PROFINET** are good candidates
- Solution to choose **depends on requirements** (speed, determinism, length of network, topology, physical connection....):
  - **High speed**: Gigabit Ethernet (1000Mbps)
  - **Real-time** (determinism):
    - PROFIBUS DP: up to 12MBps
    - PROFINET: up to 100MBps with two profiles:
      - Real-time: data transmission via prioritized Ethernet message frames
      - **Isochronous real-time**: synchronized data transmission for cyclic exchange

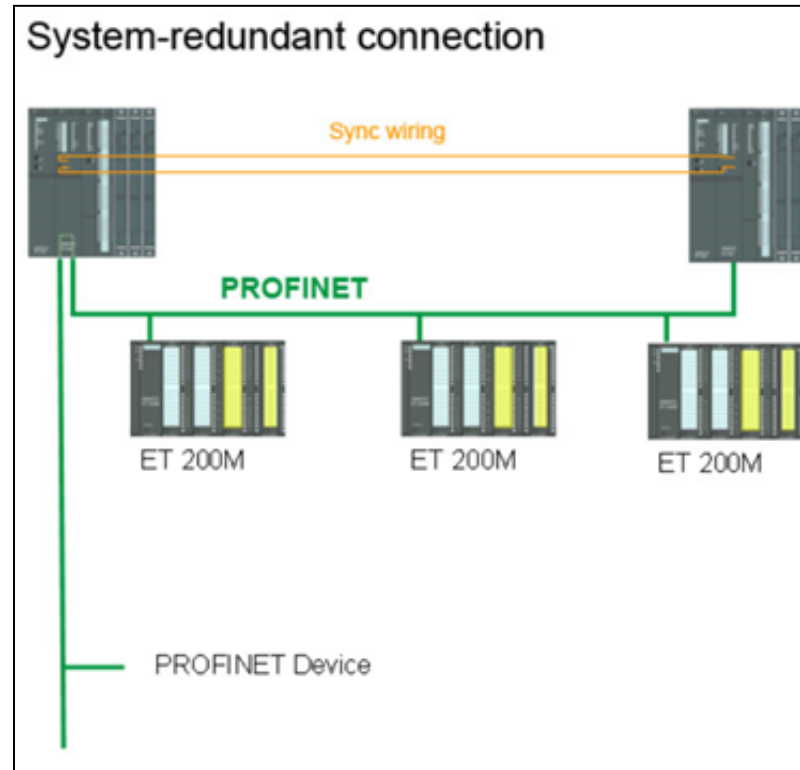
# Fieldbus technologies for interlocks operation

- Our **current experience** for interlocks is mainly based on industrial Ethernet (SCADA) and **PROFIBUS**



# Fieldbus technologies for interlocks operation

- Although PROFINET is foreseen for fast and hard real-time control signals exchange even with high availability

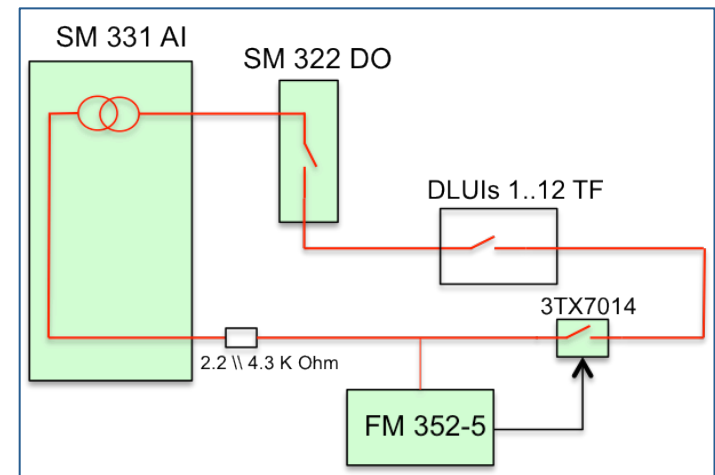
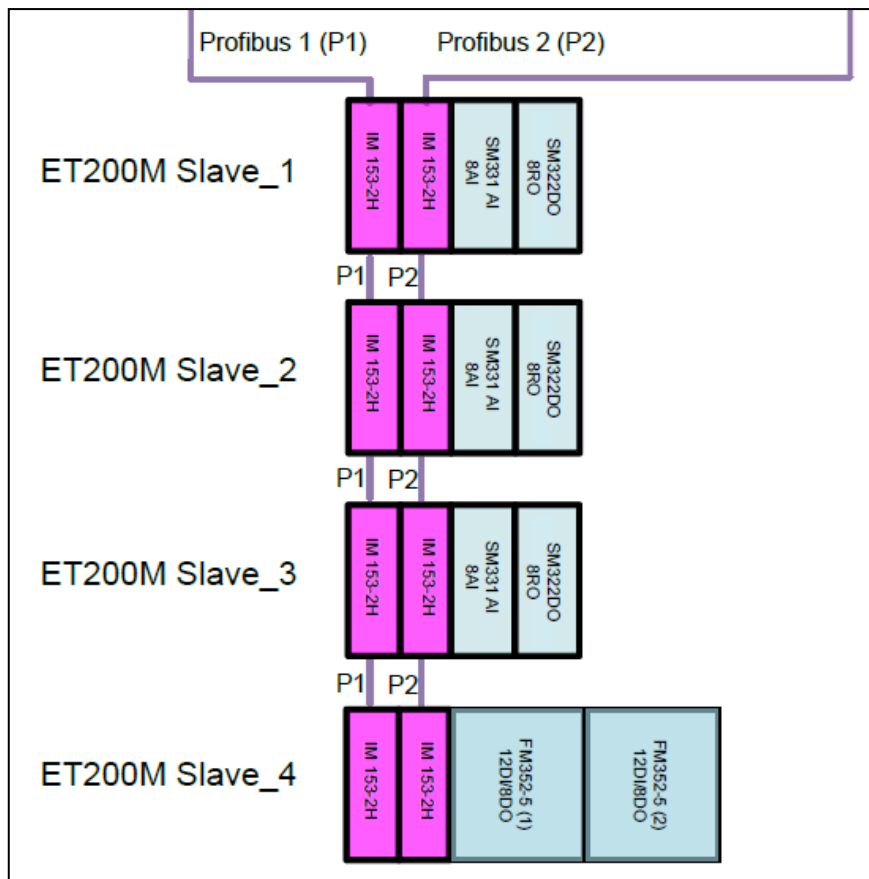


# 5. Use of high speed boolean processors for interlocks

- The FM352-5 Boolean processor provides **independent and fast control** (microseconds order) using an on-board FPGA
- It is programmable using a subset of the Step 7 KOP language
- Each module support **up to 15 inputs and 8 outputs**, easily chained
- It can work as a **standalone** controller or in a **PROFIBUS slave**
- Interesting alternative for **redundant interlocks architectures** increasing the dependability
- Main drawback: time stamping of events dependency on the PLC CPU
- Initial approach for the LHC Beam Interlock System, currently used in the warm magnets interlocks system and for ITER prototype


# Use of high speed boolean processors for interlocks

Prototype for ITER magnet powering: fast response time and increment of dependability (redundant approach)



# 6. Example: HTS current leads interlock system

**Mission statement:** “Protect the HTS current leads and the associated powering equipment in case of magnet quenches or other failures in the magnet powering by taking the appropriate actions to stop magnet powering with high dependability constraints.”



ITER\_D\_7LGM5B v1.0

## Implementation of the interlock system for the HTS current lead test

ITER\_D\_7LGM5B

Abstract

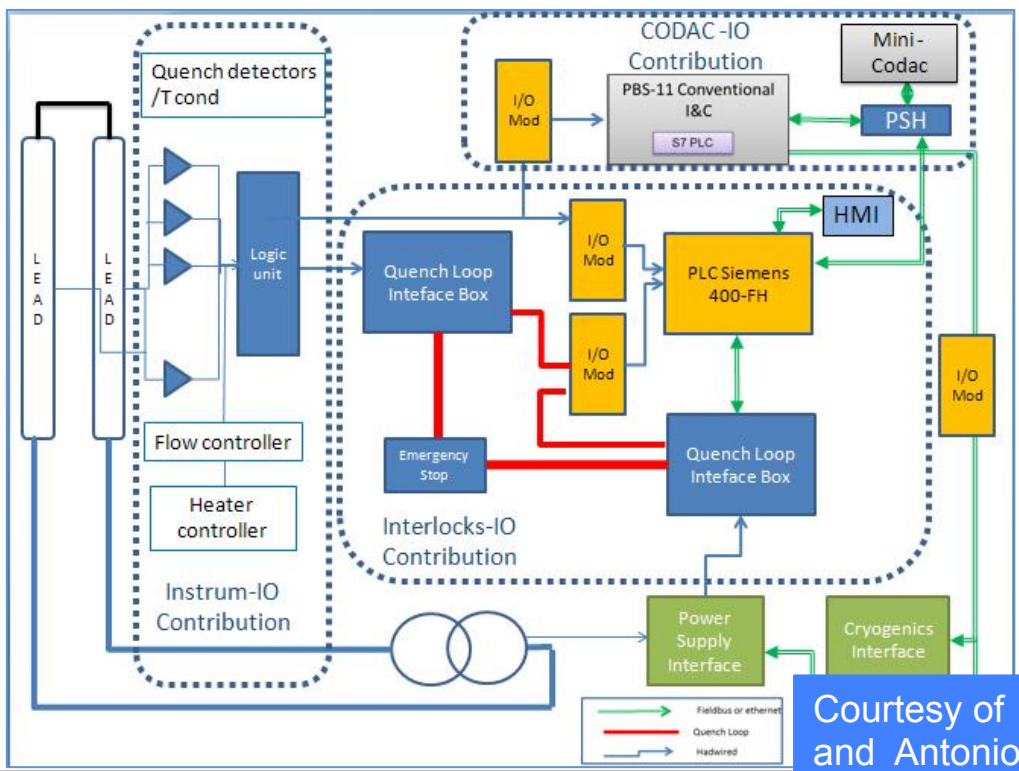
The ITER tokamak construction involves the development of cutting edge technologies, especially those ones involving HTS (High Temperature Superconducting) current leads. In order to test their correct operation, a set of tests have been foreseen. These tests need an interlock system able to protect the equipments under test in case of malfunction in conjunction with the quench detection. The system, which is in charge of providing the related interlocks, is called in the following HTS current leads interlocks.

Its main purpose is to provide dependable interlocking for the HTS current leads and the associated powering equipment in case of quenches or other failures in the powering and/or cryogenics systems, by taking the appropriate actions to stop current leads powering with high dependability constraints. Besides, it must provide a supervision tool or HMI (Human Machine Interface) for on-line monitoring, logging and alarm systems.

This engineering specification describes the implementation of the interlocks system for the HTS current leads test using PLC (Programmable Logic Controllers) technology.

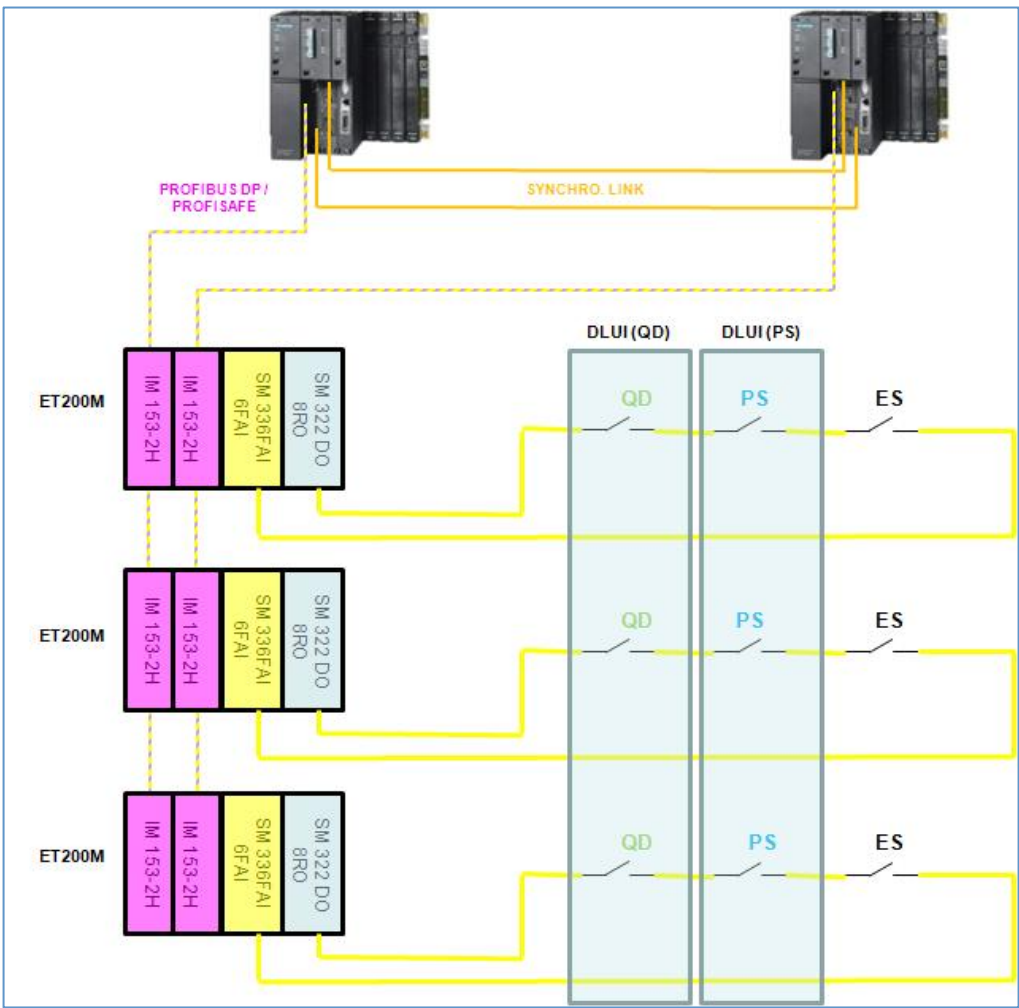
IDM Number: ITER_D_7LGM5B	Date: 19/10/2012
Name	Affiliation
Authors: Manuel Zaera-Sanz	CERN TE-MPE
Reviewers: Rudiger Schmidt, Markus Zerlauth, Jonathan Burdalo	CERN TE-MPE
Approver: Antonio Vergara, Felix Rodriguez-Mateos	ITER CHD – CODAC

Page 1 of 25



Courtesy of Felix R.M. and Antonio V.F

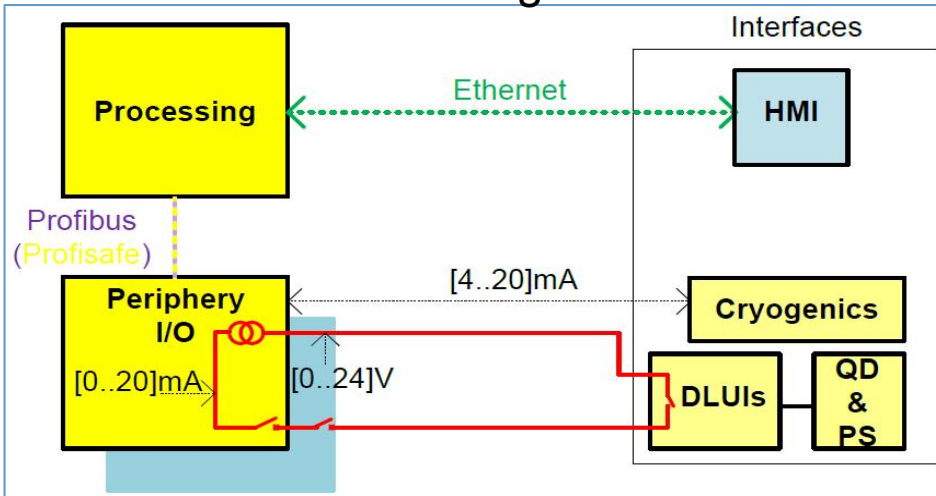
# Example: HTS current leads interlock system (Only discharge loops represented)



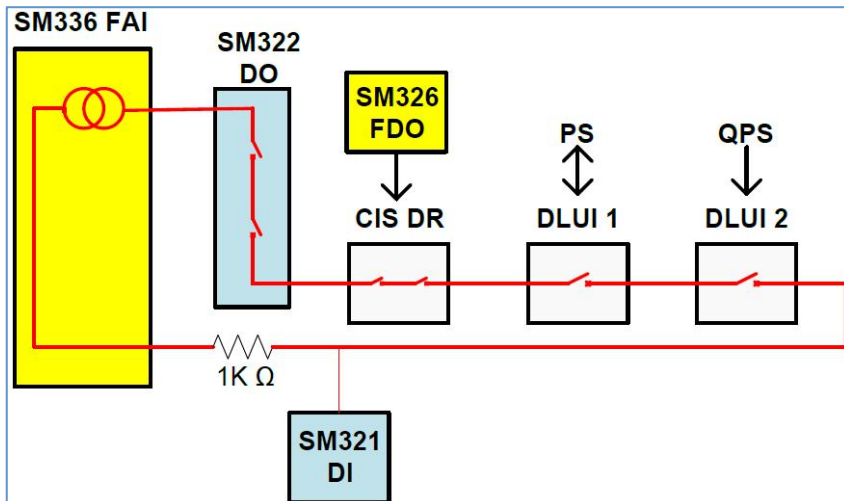


# Example: HTS current leads interlock system

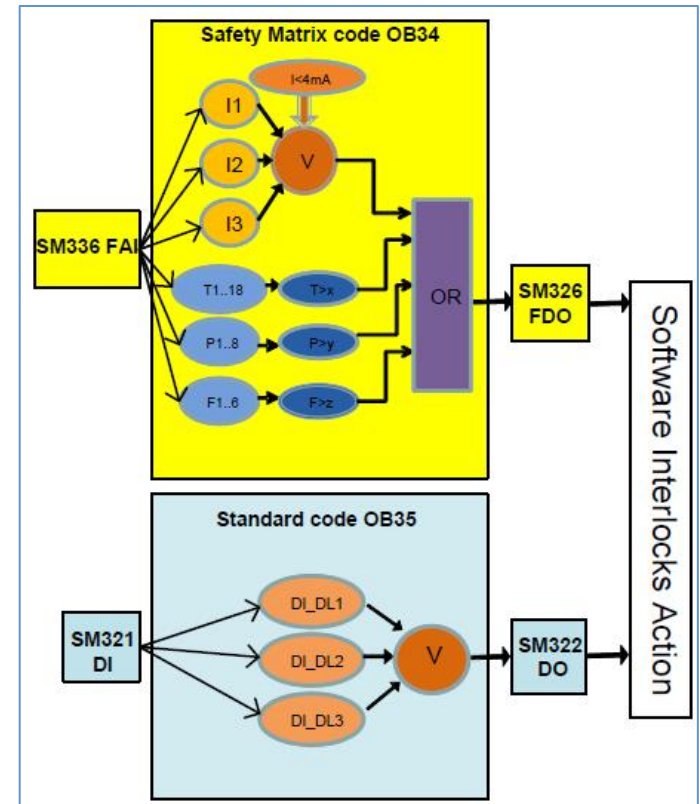
Block diagram



Interlocks current loop



Interlocks N-version SW



# 7. Conclusions

- **PLCs** provide a **robust** and **reliable** platform controlled by a real-time operating system supporting industry standard programming languages providing **high dependability** (safety, availability, security, maintainability)
- A **risk analysis** must drive the required architecture
- They are **computer based systems**, so they will follow a similar exponentially growing curve: smaller, more performance, cheaper
- **Extended use**: NASA (Wind tunnels control, Life sciences and Astrobiology research, Sustainability base), Europe's space port in French Guiana (ground segment and test facilities for Ariane V, Soyuz and Vega), Particle accelerators (CERN, ITER, DESY, GSI), Industry (Chemical, Nuclear, Plastic, Ceramic, Composites, Automobile),.....



**THANK YOU!!!**