An overview of the ITER interlock and safety systems

Luigi Scibile, Jean-Yves Journeaux, Wolf-Dieter Klotz, Anders Wallander, Izuru Yonekawa

ITER Organization, 13067 St. Paul lez Durance, France

Outline

- Context of the interlock and safety systems in ITER
- Main functional requirements
- Main design requirements
- Main system requirements
- Some current activities

Context of the interlock and safety systems in ITER

- **Origin of the requirements:**
  - ITER involves a number of potential identified hazards to personnel, the environment, and to the machine itself: the main hazards being linked to radiations, the stored energies, the operation of the large industrial systems and the operation of the plasma
  - ITER Generic Site Safety Report (GSSR)
  - Preliminary Safety Report (Rapport Préliminaire de Sûreté, RPrS)

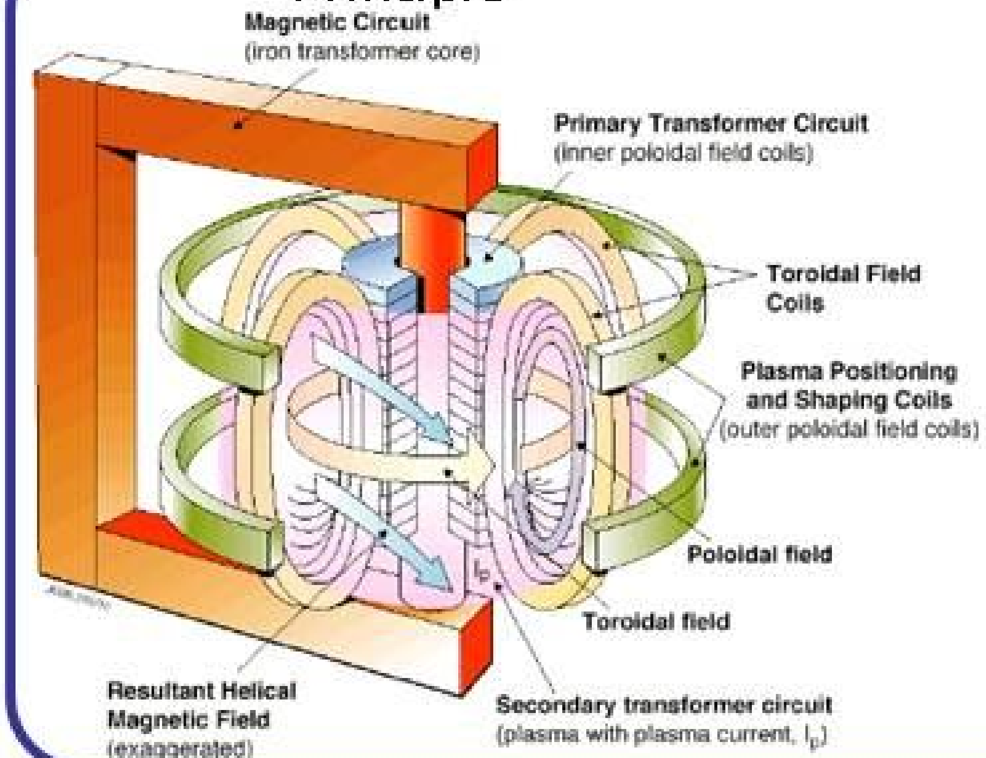
- **The regulatory context**
  - ITER is classified as Basic Nuclear Installation (Installation Nucléaire de Base, INB) based on the French Laws

- **The procurement structure and the technical organization**

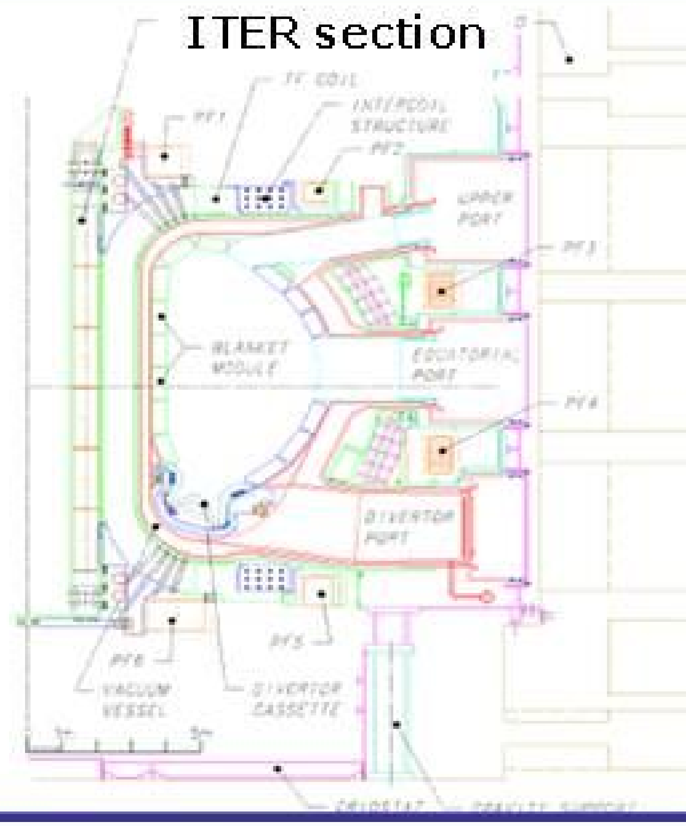
Why protections: examples (1/2)

- Tokamaks work on the principle of magnetic confinement:
  - Creating a magnetic “bottle” giving a shape to the plasma and keeping it isolated from the physical container (Vessel) .
  - magnetic bottle depends on the current flowing in the supercounducting coils and the plasma current in a very delicate equilibrium.
- Superconducting magnets:
  - High stored energy ~ 100Gj -> Quench, plasma termination
  - Interaction of strong magnetic fields (~5T, up to ~17MA) -> power interlock, coil protection, disruption mitigation.

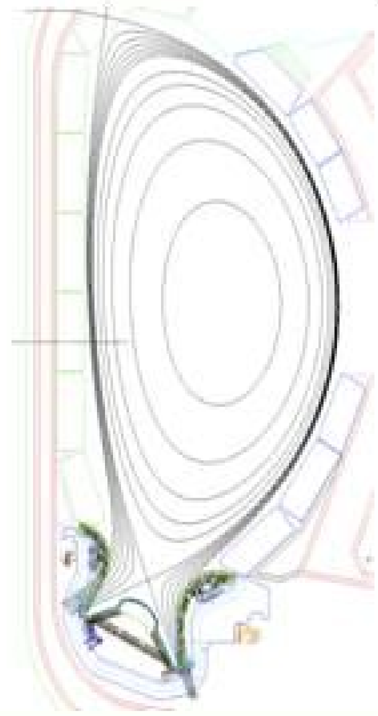
Principle



ITER section

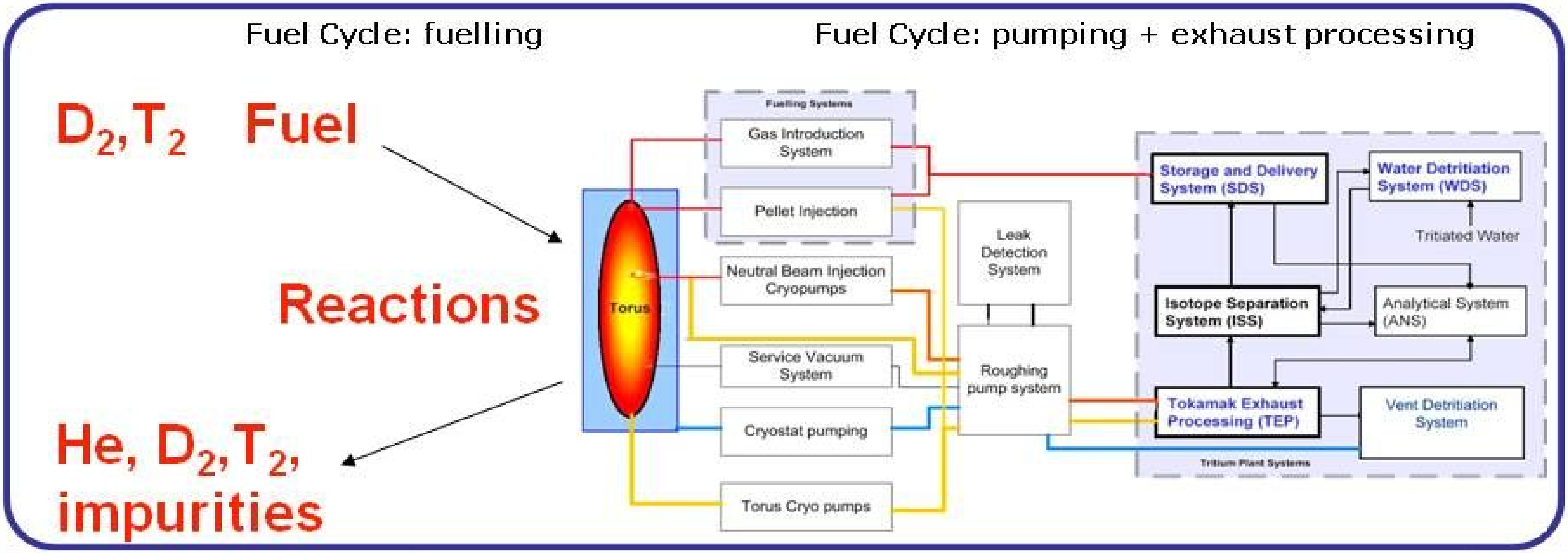


Typical plasma shape

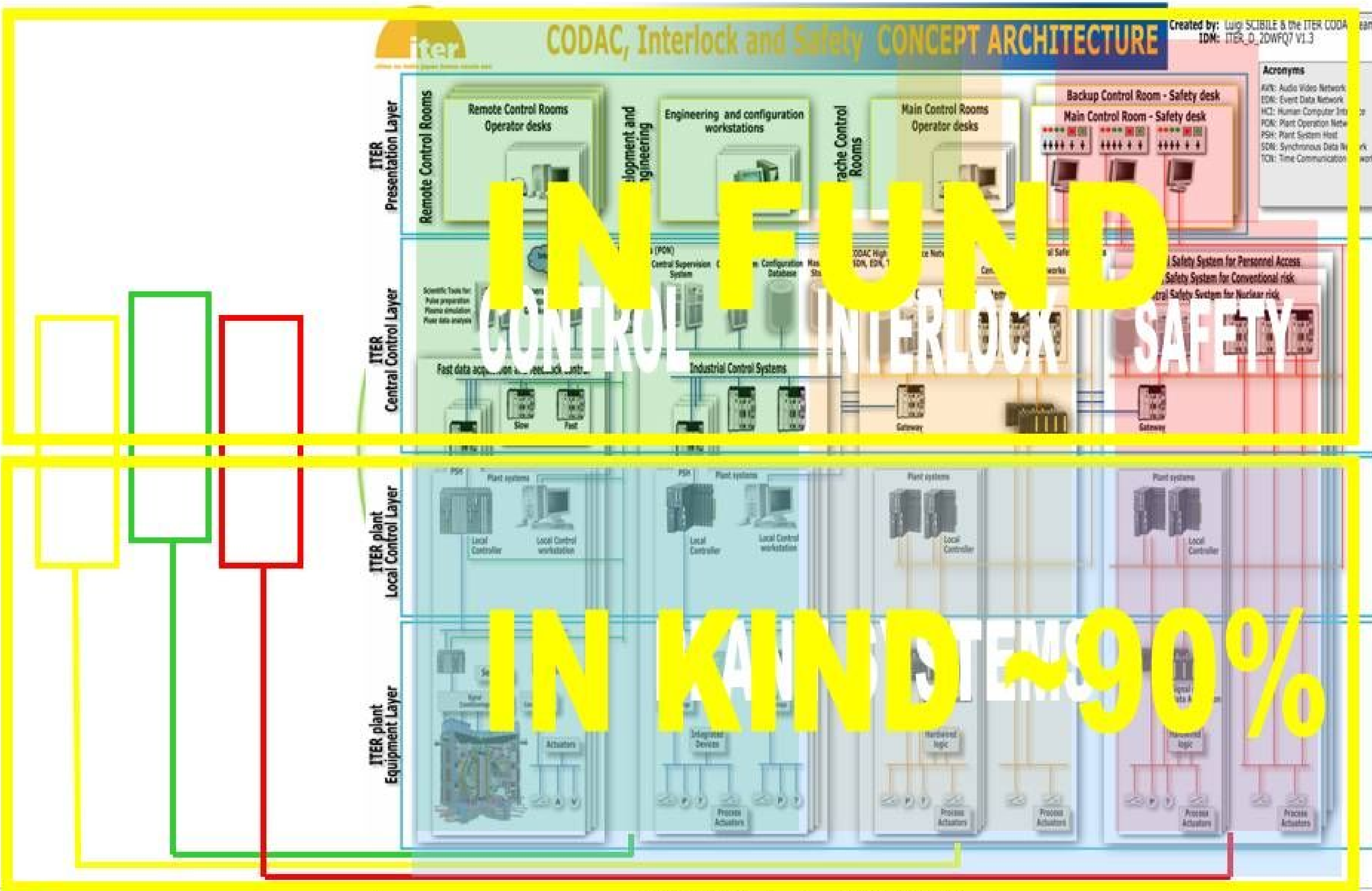


Why protections: examples (2/2)

- In Tokamaks, the fusion elements and products can be radioactive:
  - One of the fusion reaction is based on Deuterium-Tritium elements (to generate 500 MW of total fusion power, about 0.4 g of tritium will be burnt)
  - However, the operational conditions require that more than 100 g of tritium will be injected into, pumped from the vessel and processed on line
- Confinement:
  - Leakages -> Confinement components protection, Isolation valves and buffer circuits
  - Human actions -> interlock risky operations.



Two layers - Three tiers



Main functional requirements

- The main functions are linked to:
  - the confinement of the radioactive material
  - the limitation of internal and external exposure to ionizing radiations
  - the stored energies
  - the operation of the large industrial systems
  - the operation of the plasma
- Grouped in two main categories:
  - Protection functions
  - Monitoring functions.
- Functional analysis:
  - To map the functional requirements to actual plant systems
  - To identify and formalize the interfaces between the various plant systems and the central systems.

Main design requirements

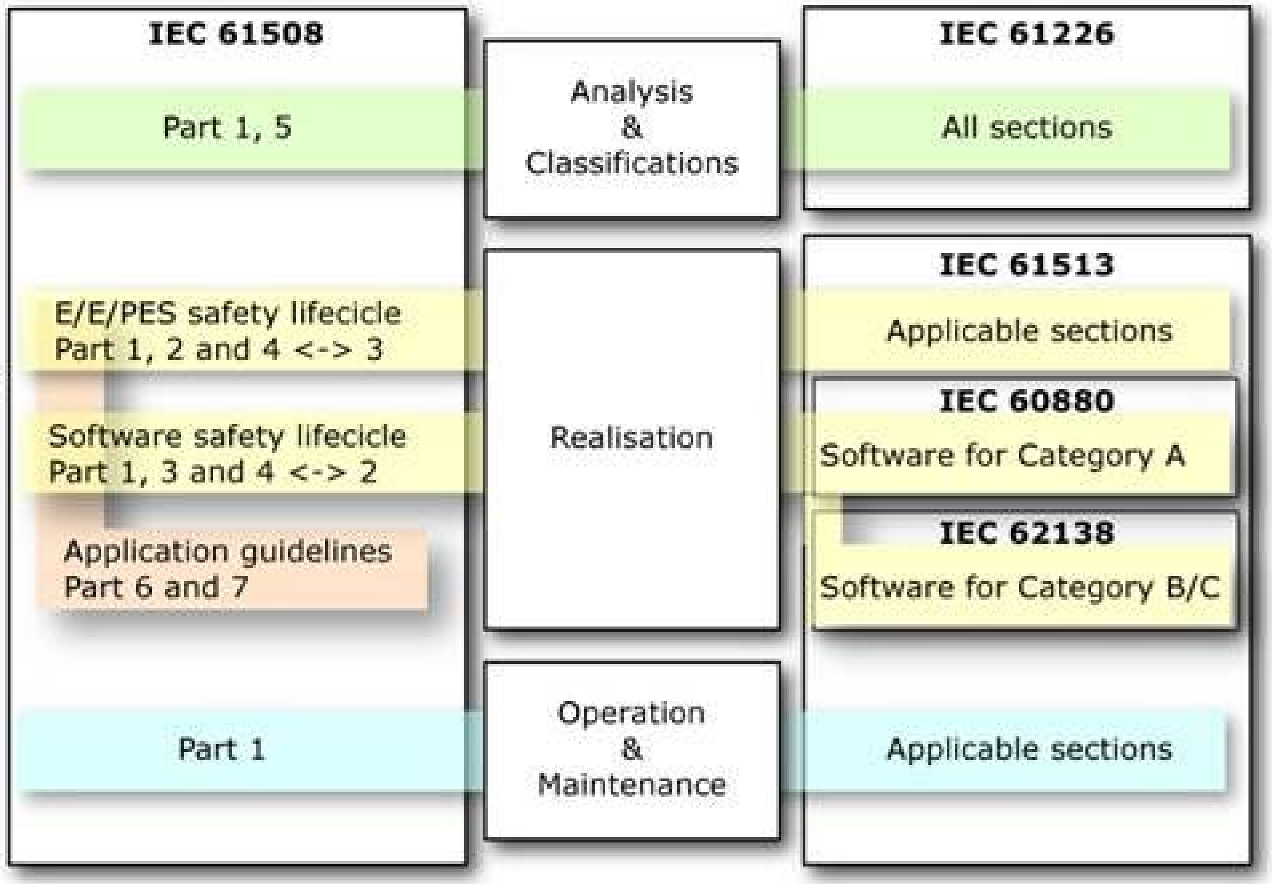
- Top level design principles:
  - Graded approach
  - Defense-in-Depth principles and separation
  - Redundancy and Single Failure Criteria
  - Avoidance of Hazards
  - Priority among the 3 tiers
- Based on:
  - The current ITER design and organized in the ITER Plant Control Design Handbook
  - Recommendations and requirements from selected standards

Application of international standards

- IEC 61508 Family: to minimize diversity in the development approach
- To unify the communication in terms of common objectives
- For the compliance to the national regulations that are in vigour in France where ITER is located

For conventional instrumented safety systems:

[IEC 61508], Functional safety of E/E/PES safety related systems



For the nuclear sector:

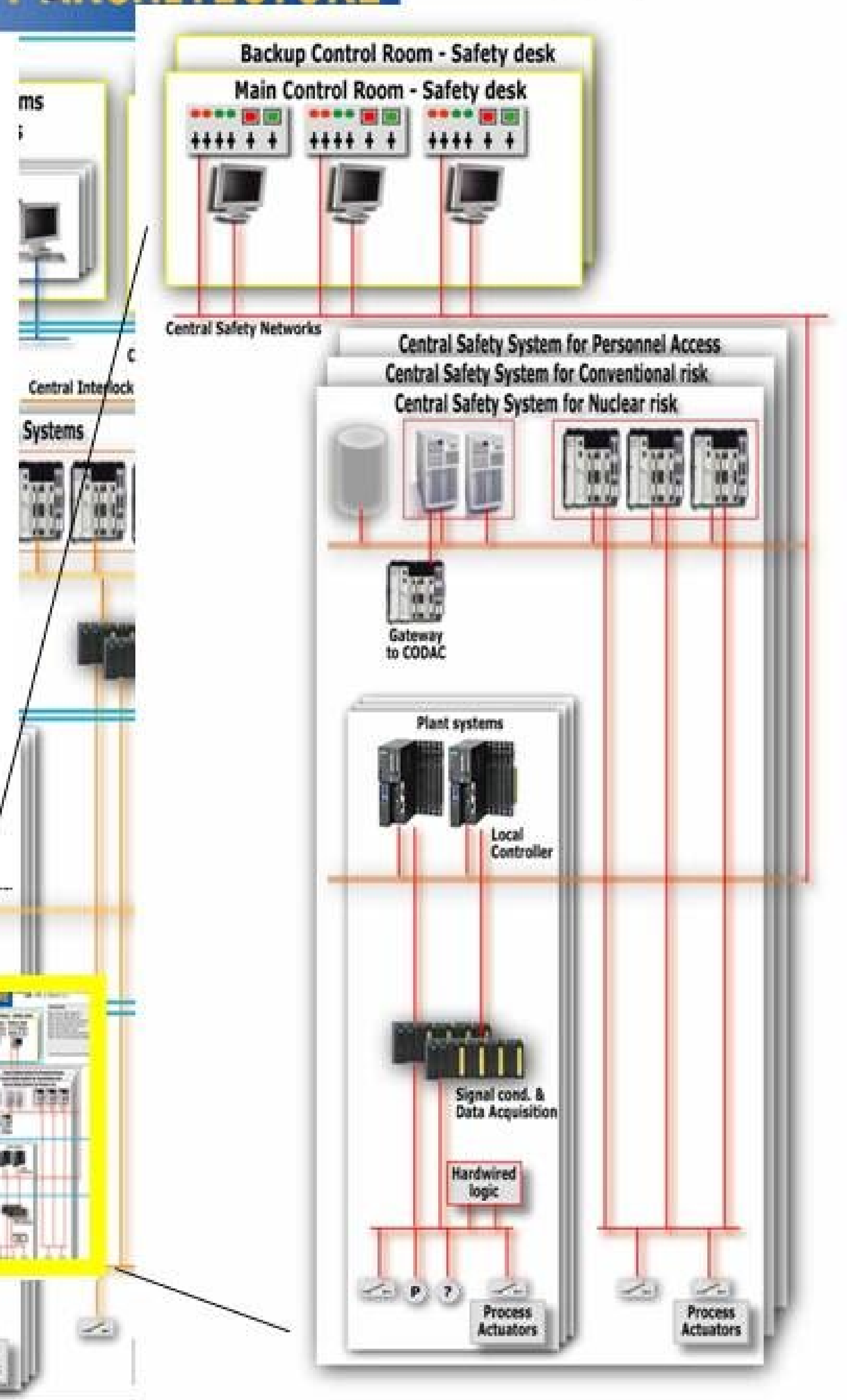
[IEC 61226], Nuclear Power Plants Instrumentation and Control Systems Important for Safety Classification

[IEC 61513], Nuclear power plants Instrumentation and control for systems important to safety General requirements for systems

Safety Control Systems

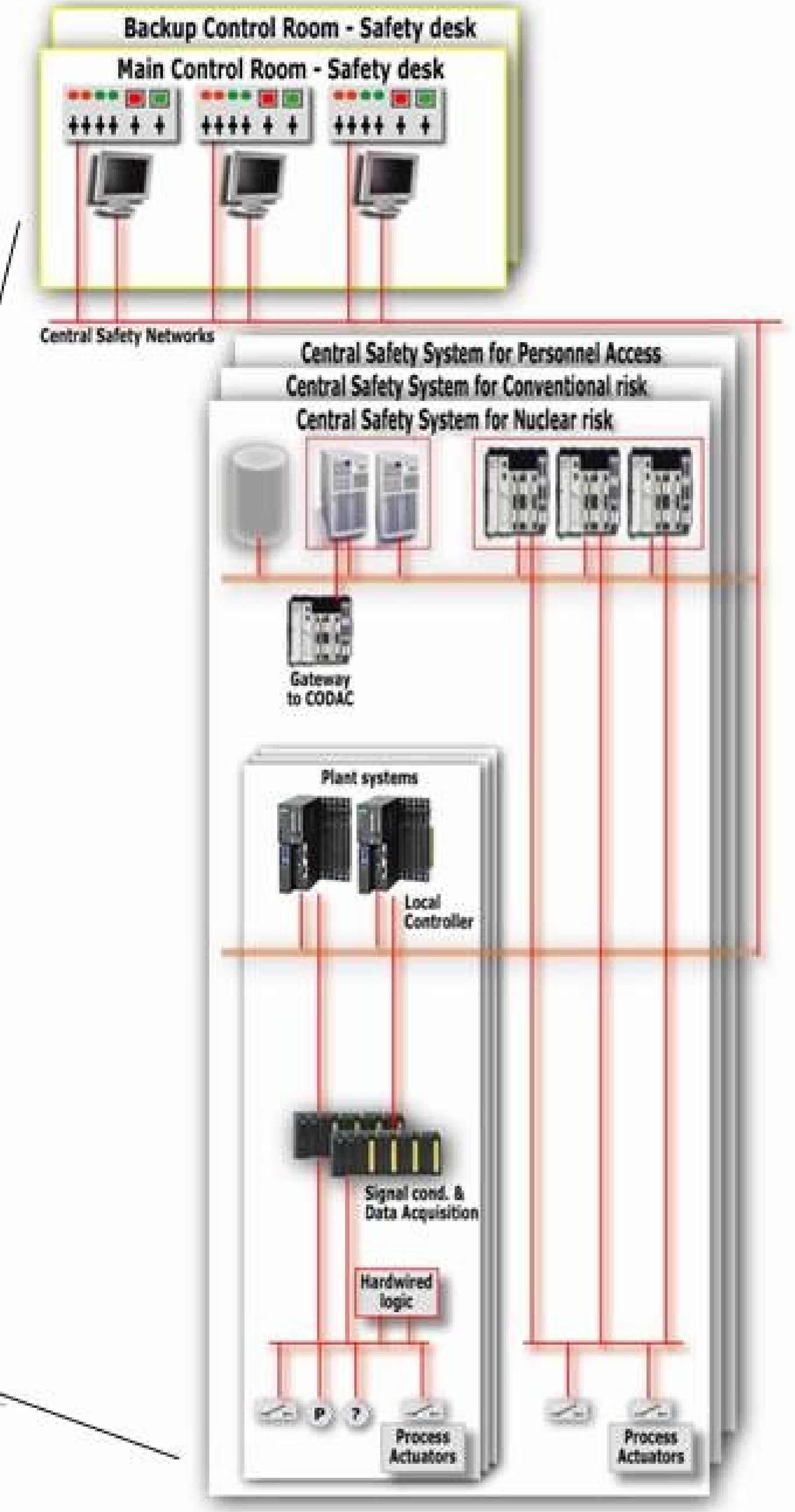
Created by: Luigi SCIBILE & the ITER CODAC team
IDM: ITER_D_2DWFQ7 V1.3

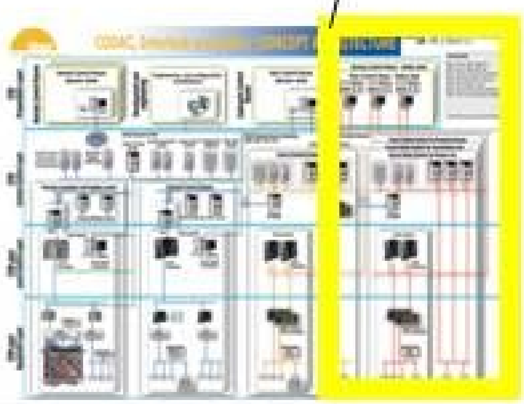
- **Main system requirements**
  - The CSS for Nuclear risk and Personnel access are classified as a SIC system classed as implementing safety functions of category B (IEC 61226) with systems of class 2 (IEC 61513)
  - Safety functions of category A will be implemented via hardwired logic with systems of class 1.
  - No Common Cause of Failure
  - Multiple line of defense



Safety Control Systems

- **Main system requirements**
  - The CSS for Nuclear risk and Personnel access are classified as a SIC system classed as implementing safety functions of category B (IEC 61226) with systems of class 2 (IEC 61513)
  - Safety functions of category A will be implemented via hardwired logic with systems of class 1.
  - No Common Cause of Failure
  - Multiple line of defense

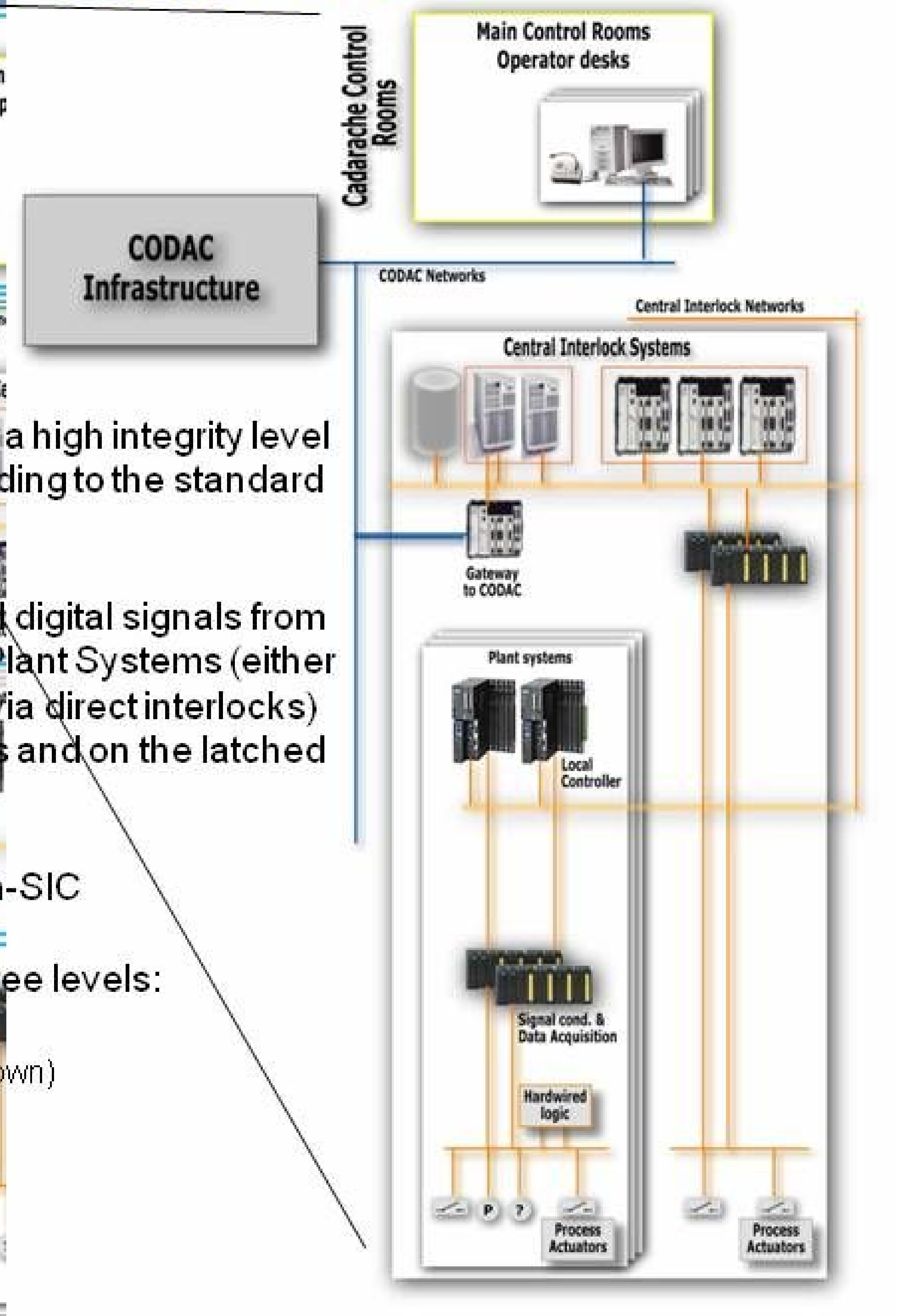




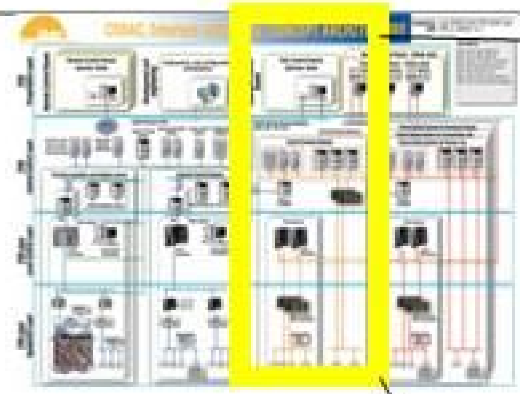
Interlock Control Systems

Created by: Luigi SCIBILE & the ITER CODAC team
IDM: ITER_D_2DWFQ7 V1.3

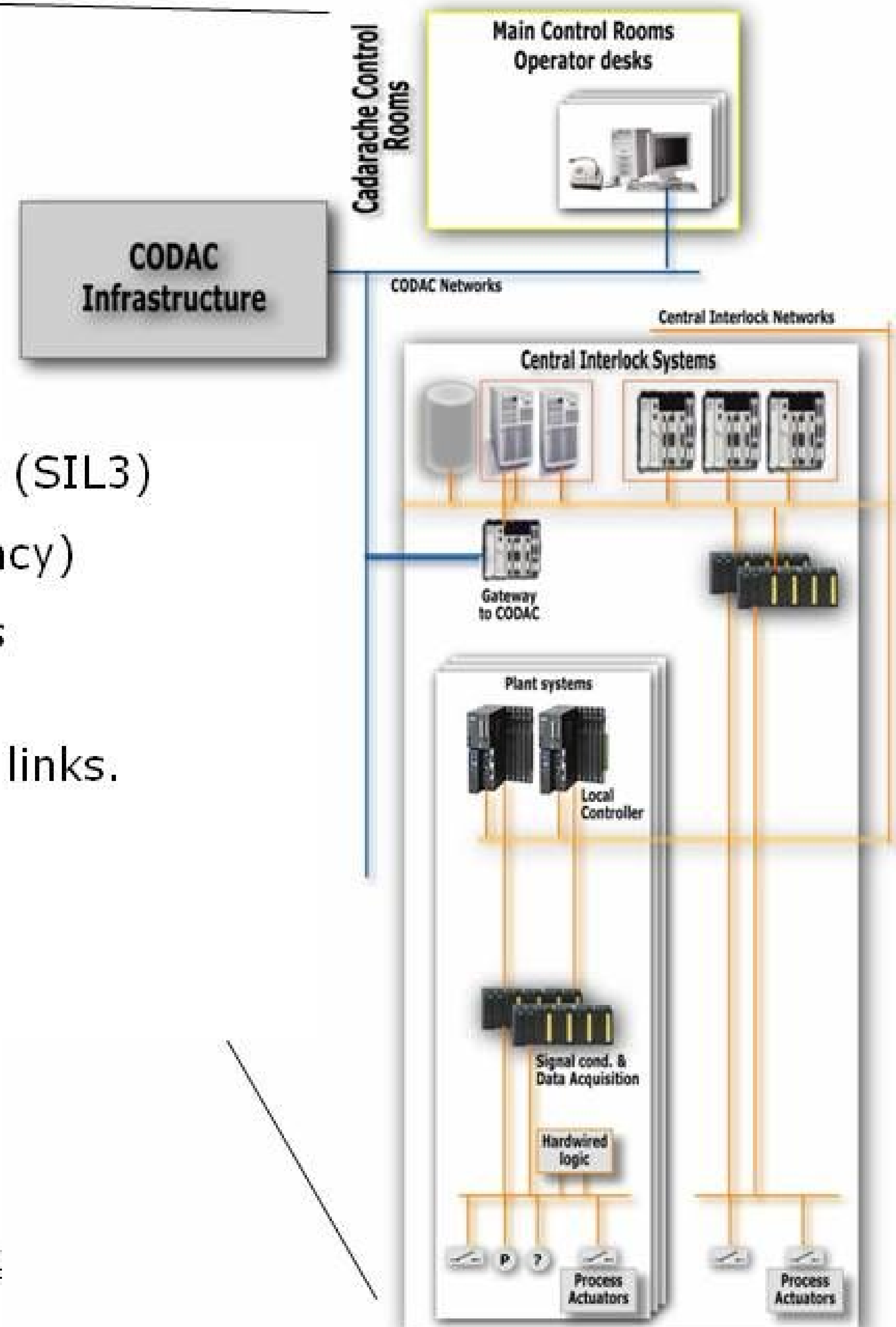
- **Main system requirements**
  - Highest level interlock functions will be designed to a high integrity level conforming to a Safety Integrity Level (SIL) 3 according to the standard IEC 61508
  - The Central Interlock System will acquire the critical digital signals from the Plant Interlock Systems and deliver outputs to Plant Systems (either via the corresponding "Plant Interlock Systems" or via direct interlocks) on the basis of boolean logic on the full set of inputs and on the latched outputs
  - The Central Interlock Systems are classified as non-SIC
  - The interlock protective actions will be graded at three levels:
    - Level 1 interlock events (Fast shutdown)
    - Level 2 interlock events (Fast Controlled Pulse Shutdown)
    - Level 3 interlock events (Inhibit)



Interlock Control Systems

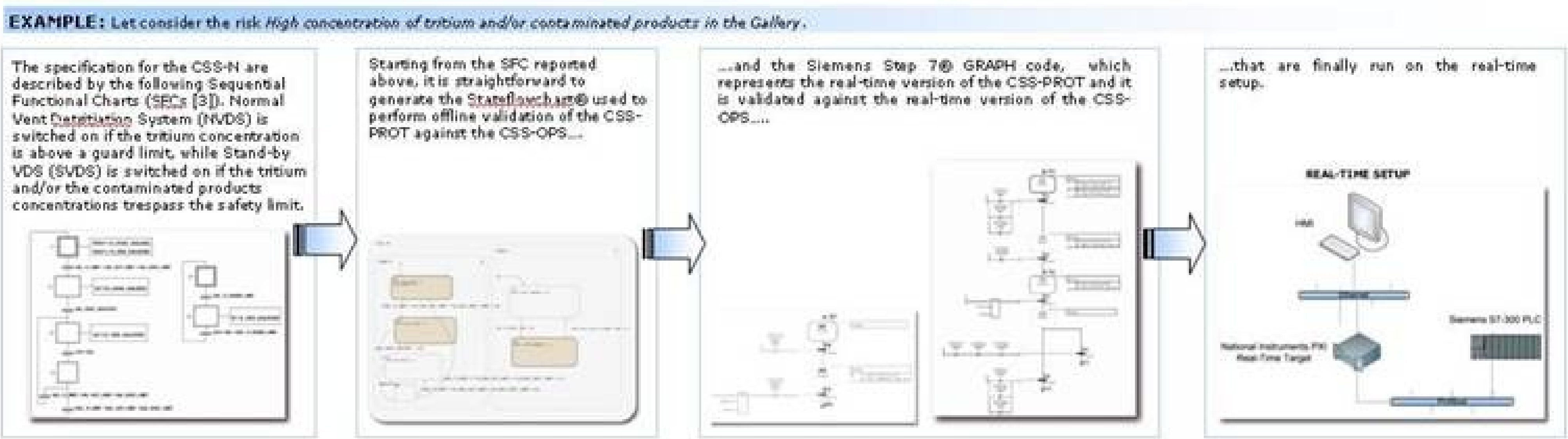


- **Equipment required:**
  - Highly reliable and available PLC systems (SIL3)
  - Some hardwired systems (2oo3 redundancy)
  - Various type of transducers and actuators
  - Various type of networks:
    TCP/IP, field buses, monitored hardwired links.
  - Supervisory systems
  - Short term data storage
  - Operator synoptic via CODAC + Gateway

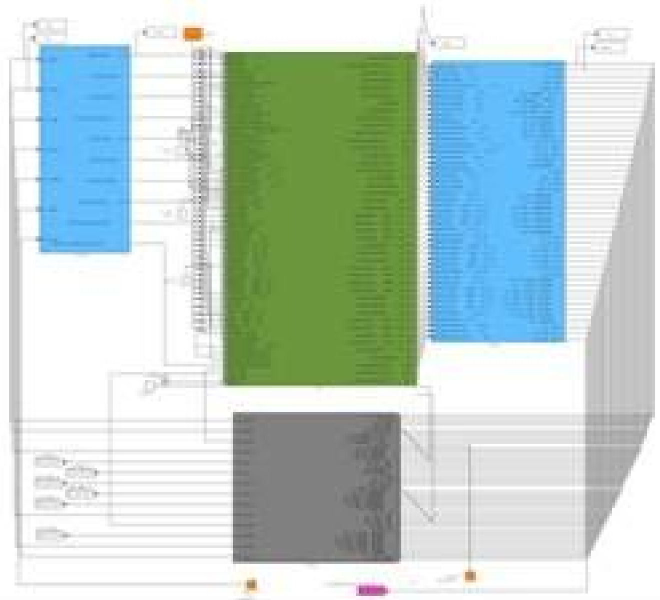


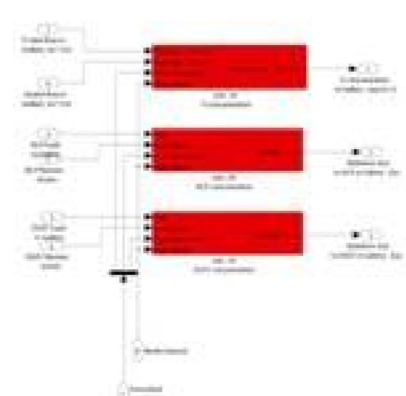
Some of the running activities (1/4)

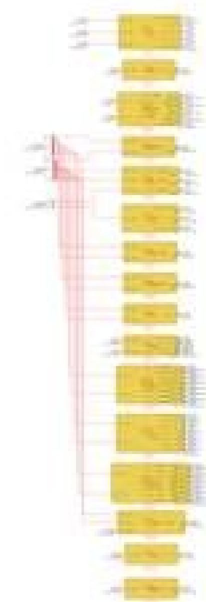
- Documentation – writing and reviewing
- Central Safety System rapid prototype

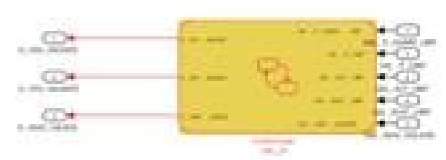


- Matlab/simulink modelling



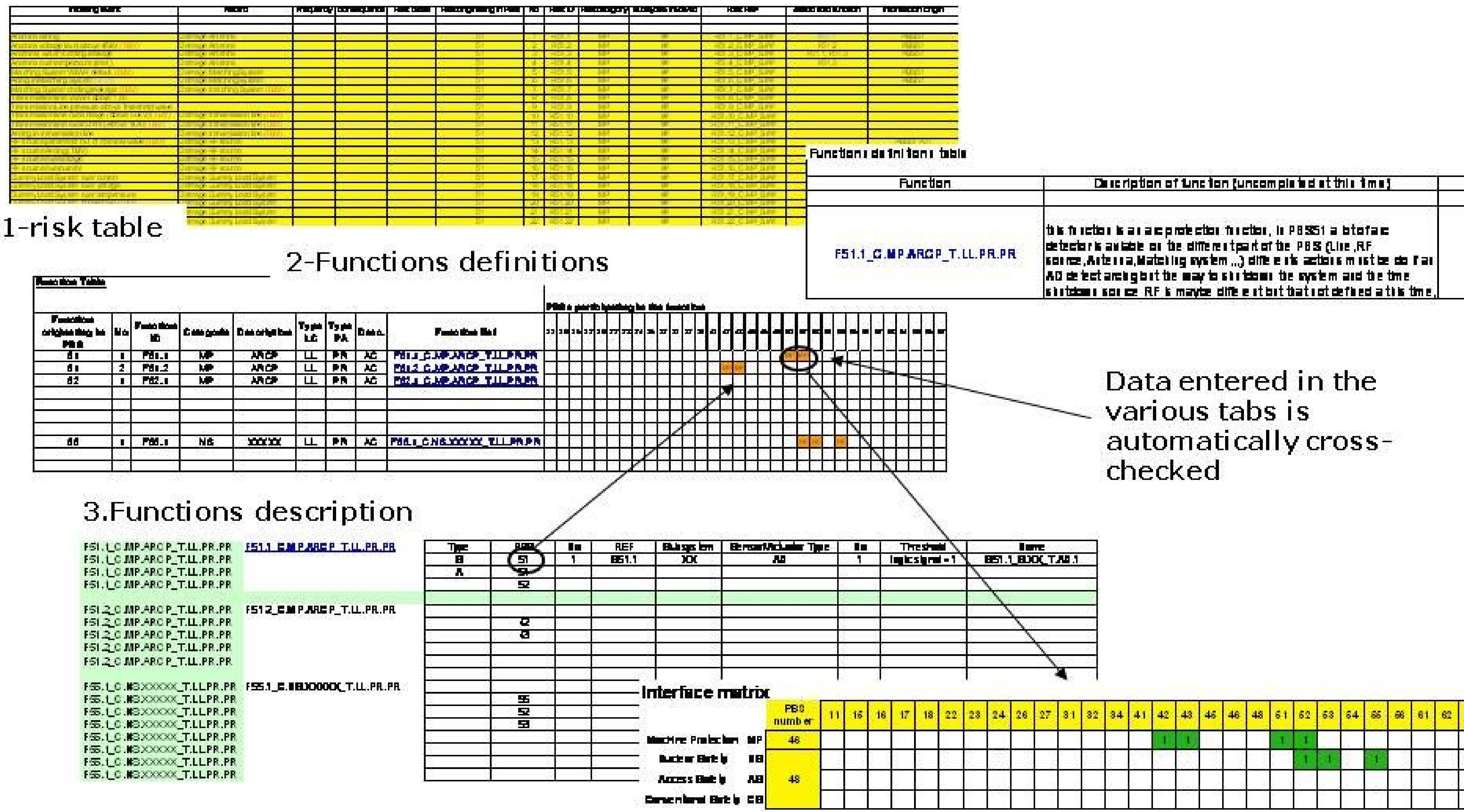






Some of the running activities (2/4)

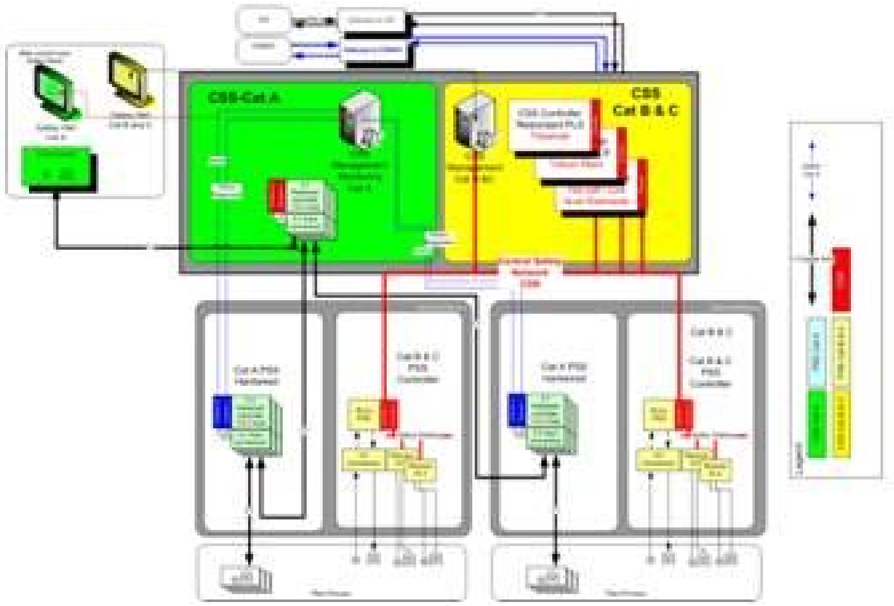
- Functional analysis



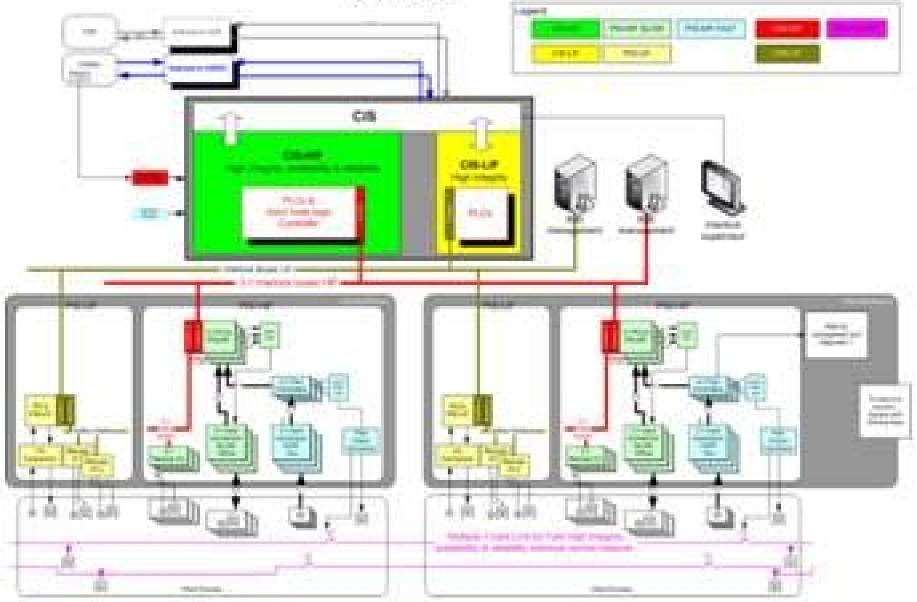
Some of the running activities (3/4)

- Preliminary architectures that map the required functions

Overall CSS



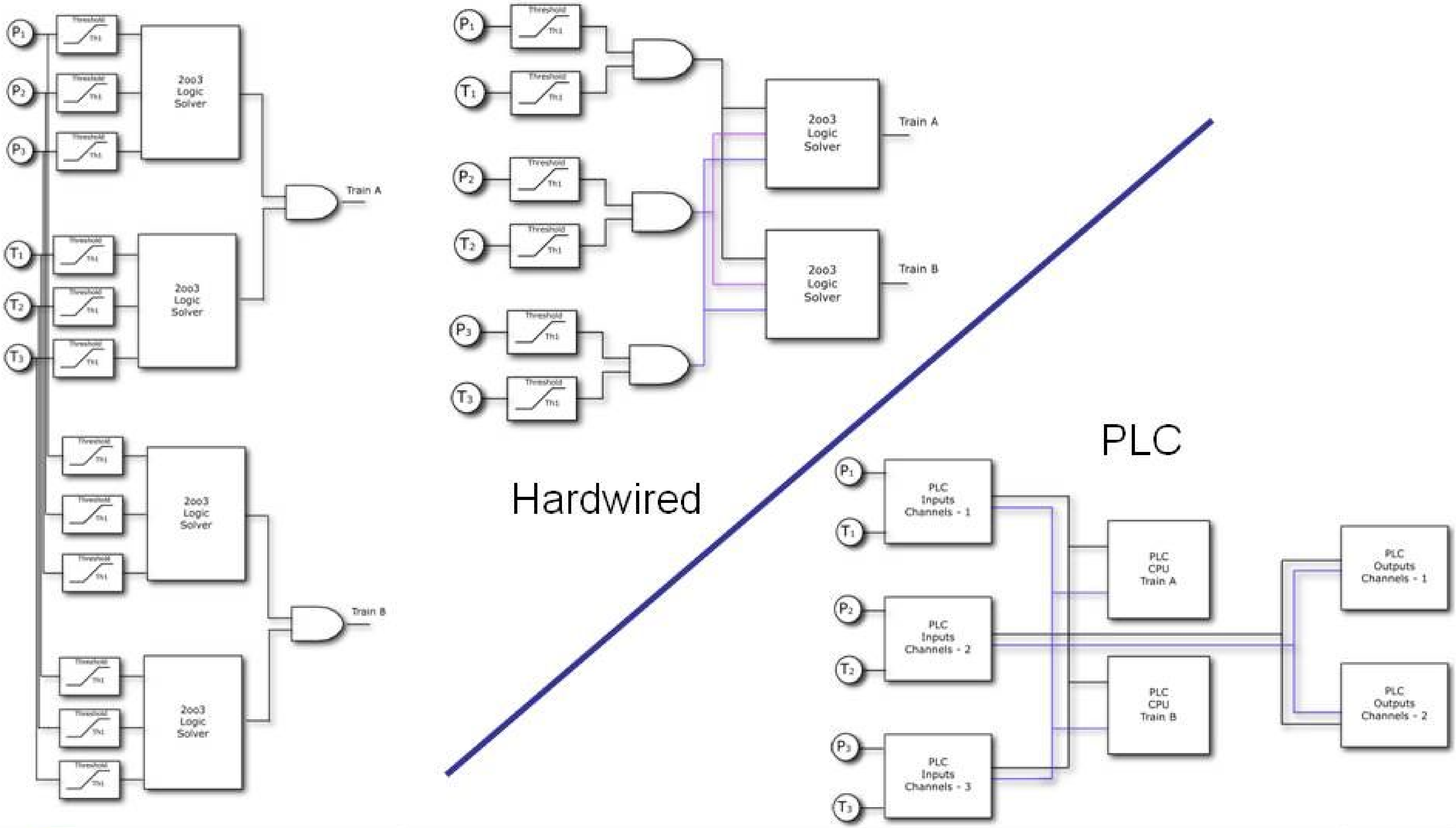
Overall CIS



- Application of the main design requirements
- Completeness verification
- Performance Analysis of:
  - Cycle time
  - Availability – Reliability
  - Volume vs Solutions
  - Networks
- Prototype realization for
  - Performance validation
  - Preliminary safety assessment
  - Validation of architectures

Some of the running activities (4/4)

- Preliminary architectures that address the redundancies



Conclusions

- Interlock and safety control systems in ITER participate to the implementation of the general safety objective and to the overall protection of the machine.
- The Safety control systems are subject to the approval of the Nuclear French regulator
- The current main priority is on the Conceptual Design
- Some information published through our public web site:
  http://www.iter.org/org/team/chd/cid/codac/Pages/default.aspx
- Lots of work in front of us……..

….and the target is worth the trip!