LHC PERSONNEL PROTECTION SYSTEMS

IEC 61508 Experience
Future Perspective

P. Ninin
CERN, Geneva, Switzerland

What are the responsibility in the event of accident involving the loss of human life ?

Three Tier Responsibility Concept

1. Criminal responsibility
   - for the legal entity and the person in charge of the safety
   - consequence of accidents can be fines, prison and site closure
2. Civil
   - damages for the third party victims
3. Administrative
   - obligation to declare incident, suspension of activity, site closure
   - Regulatory Body for Industrial & Nuclear risks

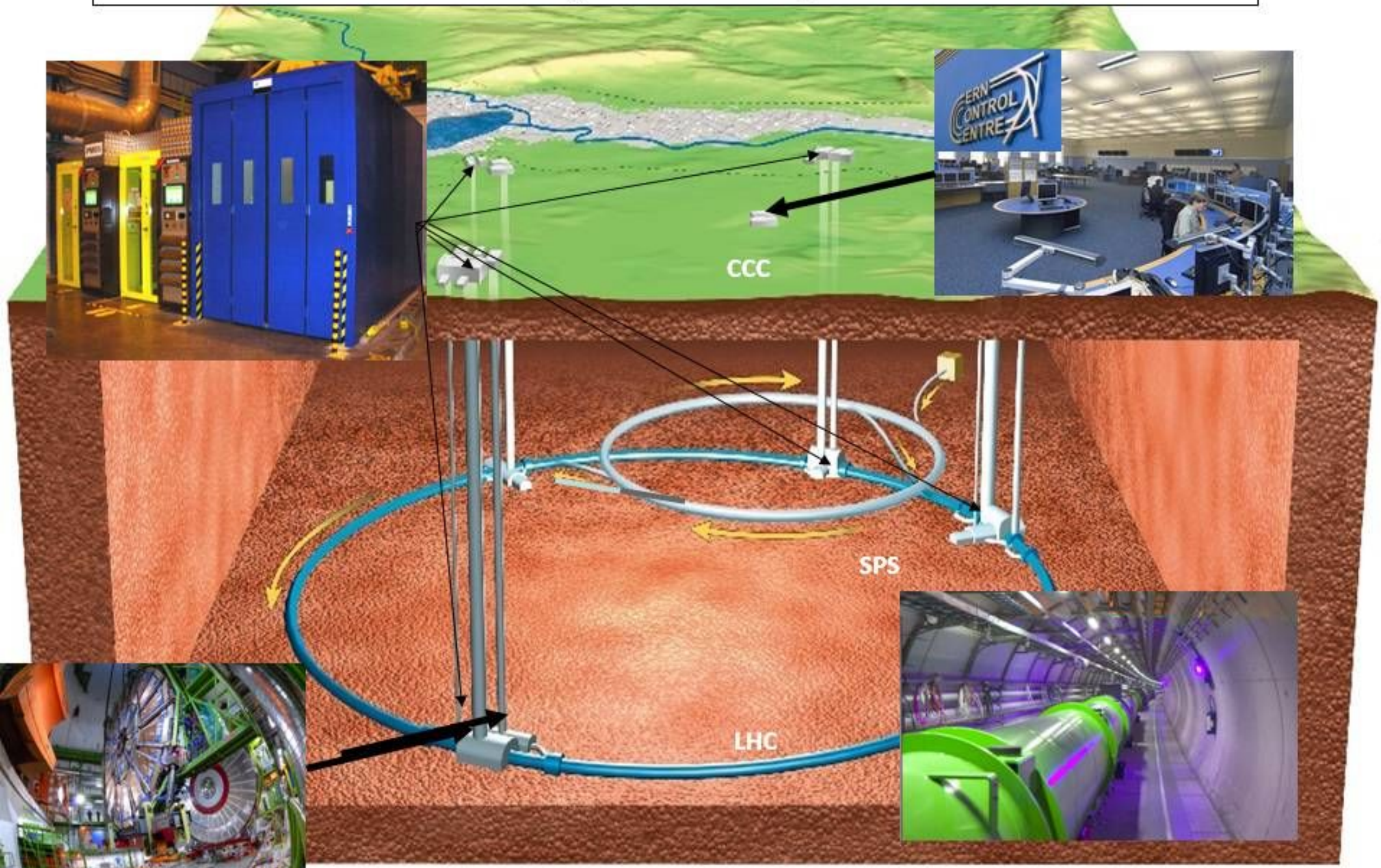
Autorisation to operate to be given by the Nuclear Authority

Does the IEC 61508 gives an answer ?

-

The case of the LHC Access system

Authorization, training, dosimeter check,
Biometry identification,
Access authorized according to the LHC operation mode



Strategy

- Strict application of the IEC61508 Safety lifecycle
- Specific requirements of the Nuclear Safety
- « GO-NO GO » -> French Regulatory body (ASN-IRSN)
- Activity definition in a set of document

1	Functional Safety Plan
2	Preliminary Risk Analysis
3	Specification of the Safety Functions
4	Preliminary Safety Study
5	Final Safety Study
6	DB of Safety data
7	Verification & Validation Plan
8	Operation and Maintenance Plan

Preliminary Risk Analysis

- Definition of the Equipment Under Control (EUC), its limits, its environment
- Analysis for all the operation modes of the hazards and risks
- Calculation of the Safety Integrity Level required to prevent each identified risk

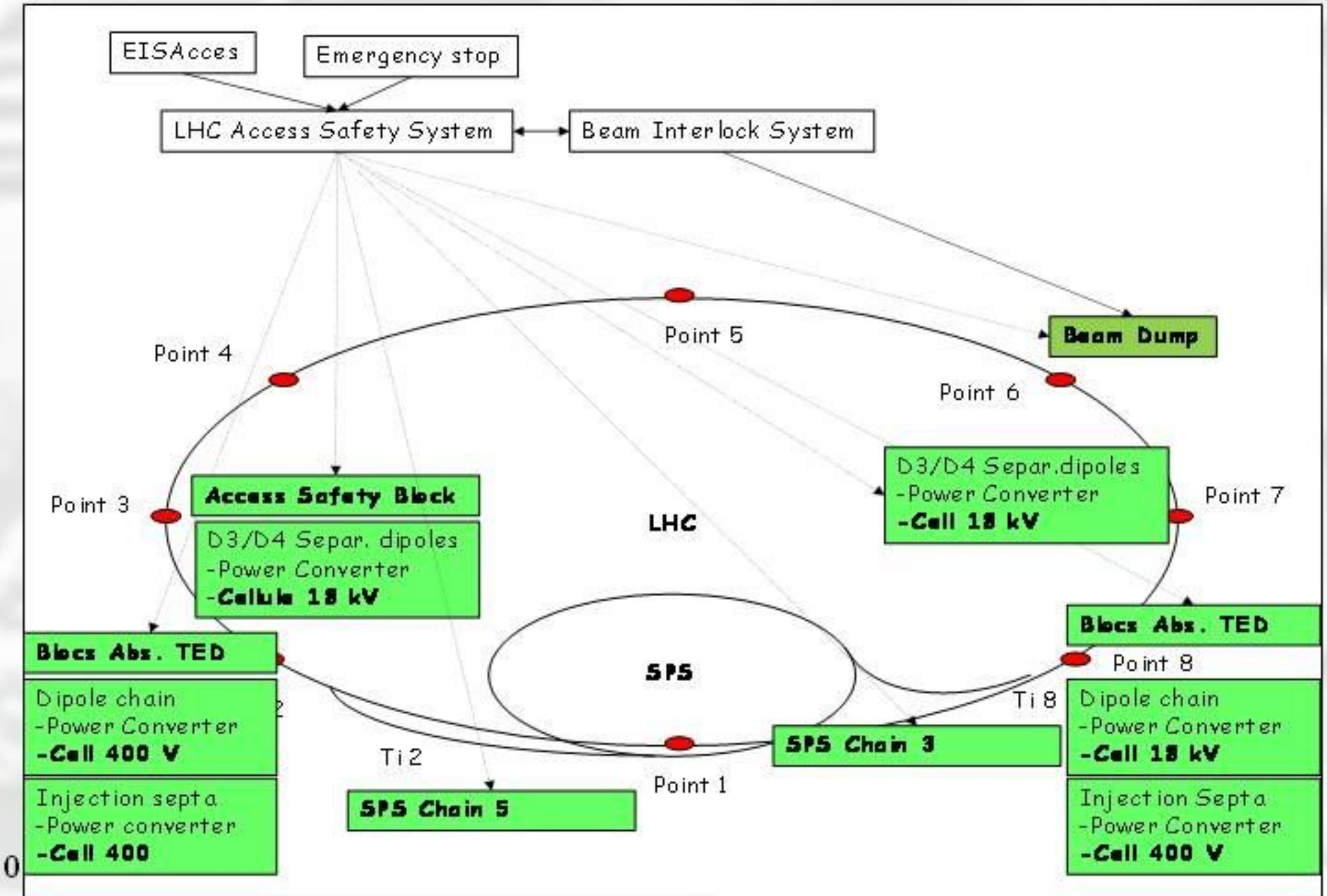
Potential risk identification
Ionizing Radiation*
Magnetic Field
Microwaves
Electrical Hazards
Lasers
Vacuum and Pressure
Cryogenic fluids
Flammable gasses
Chemicals

Safety Functions

Main Safety Functions to protect people against radiation hazards – SIL 3

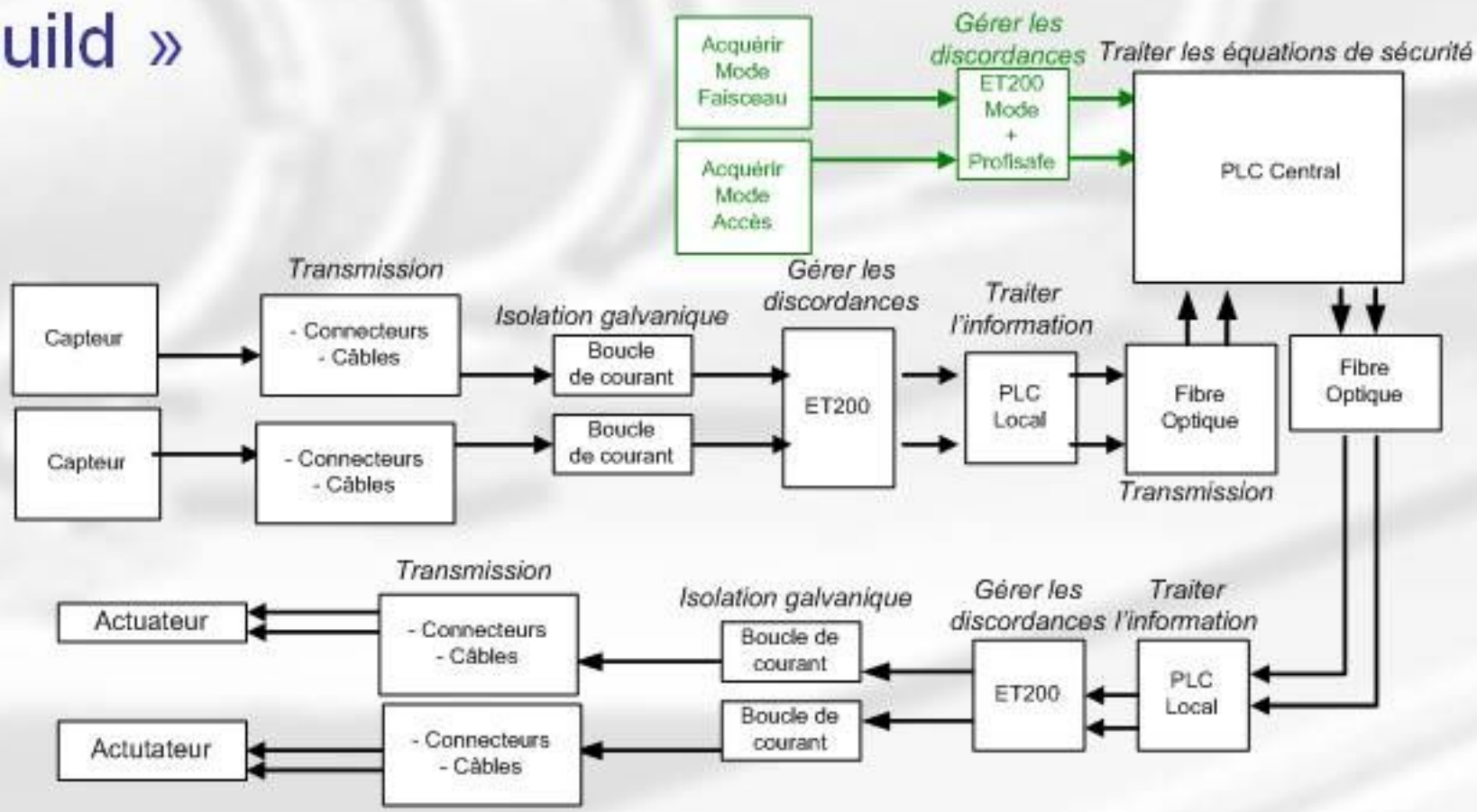
BEAM => Forbid access and stop the beams in case of intrusion

ACCESS => Forbid the injection and circulation of beams

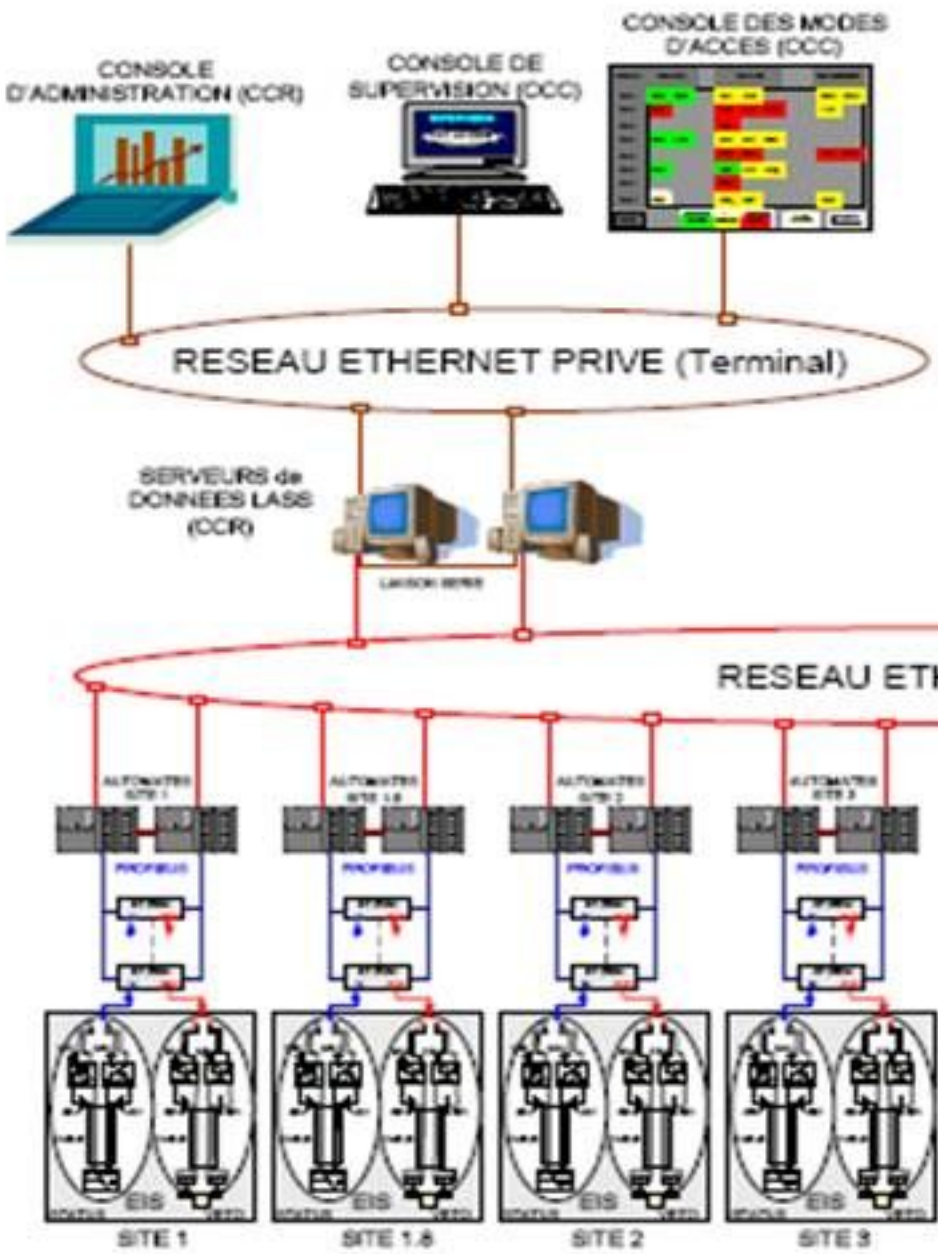


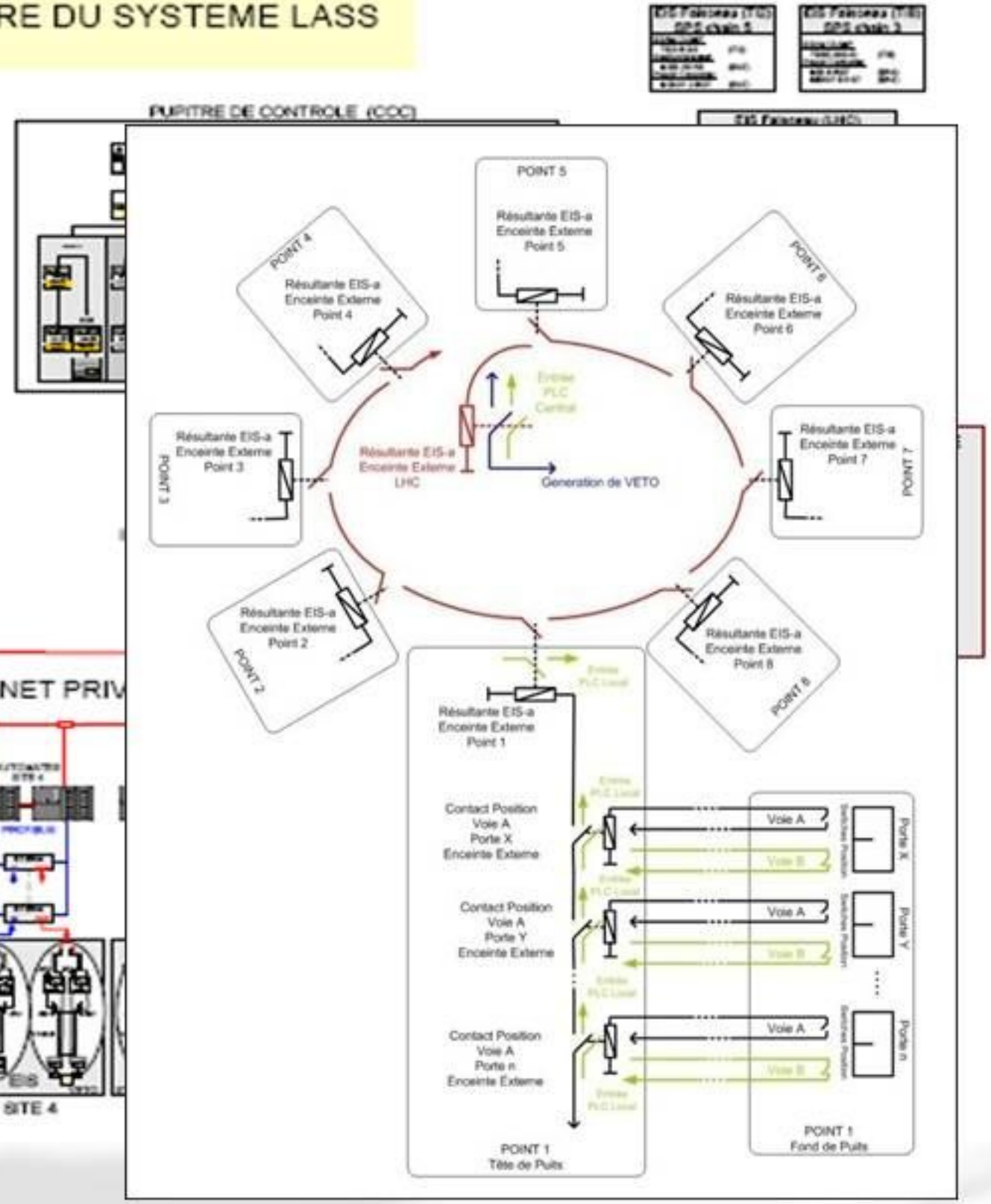
Preliminary Safety Study

- First analysis verifying that the safety objectives can be met with the selected architecture
  - Functional analysis
  - Analysis of the failure mode, effects and severity
  - Quantitative analysis verifiying that the defined SIL levels are achieved (failure rate)
- Final Study « as build »



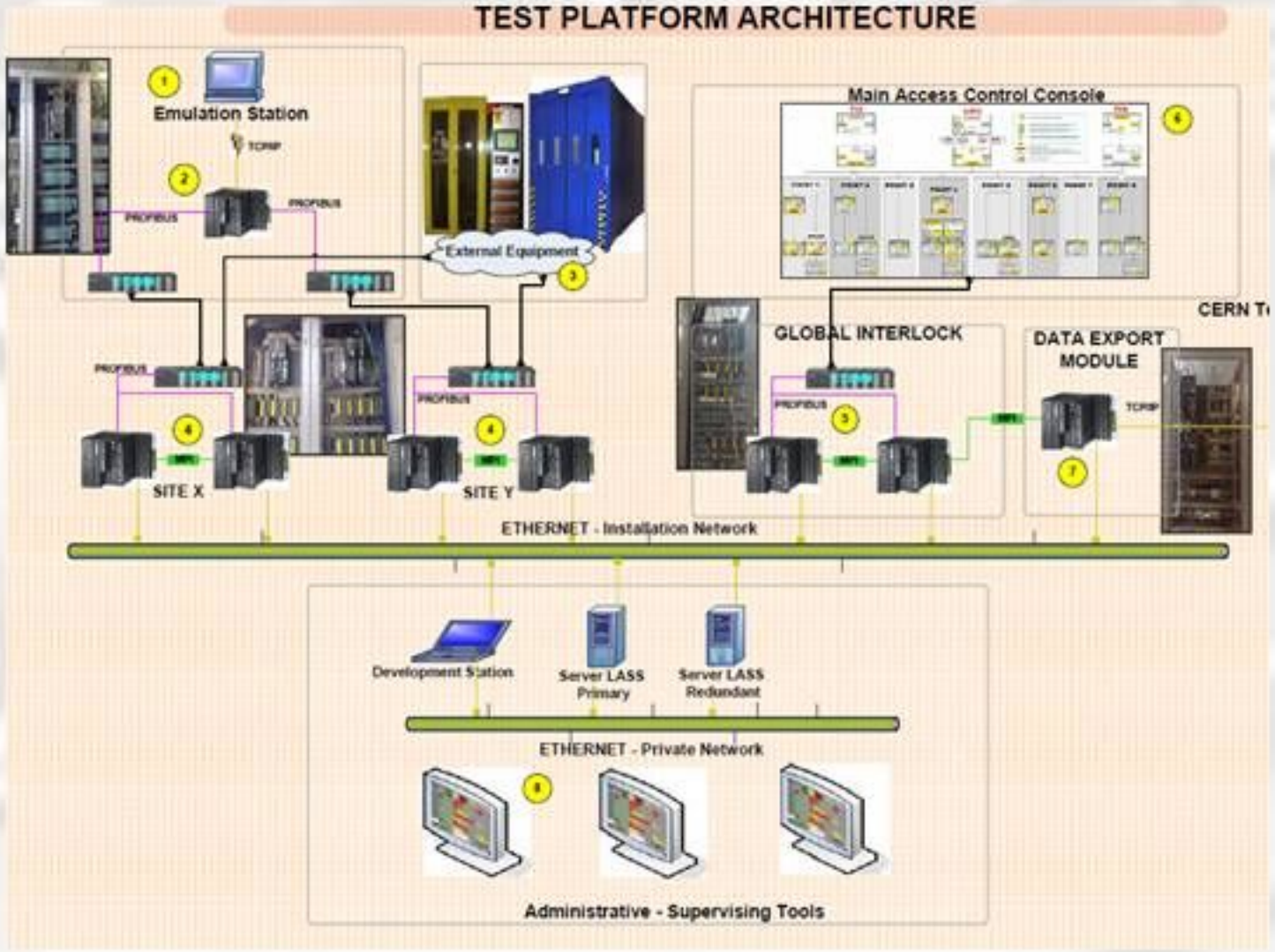
ARCHITECTURE DU SYSTEME LASS





Test Strategy

- V cycle software development
- Independent testing team
- Test platform
  - 2 LHC sites + all HMI
- On site test
  - Electrical, interfaces
  - Remote control of EIS from CCC
  - Site testing of safety functions
  - LHC wide testing of safety functions
- Validation by Regulatory body



Experience

- The IEC 61508 life-cycle is global but:
  - SIL qualification concerns only hardware and simple software modules
  - Need a qualification strategy for the software and the communication
  - Probabilistic analysis is not enough to guarantee the performance of the system, requires specific expertise
- Test strategy and coverage shall be carefully considered
  - Independant testing team
- Environmental conditions
  - Radiation tolerance, electromagnetic fields, EMC, and other aggression
- Safety demonstration for the regulatory body
  - Common cause of failure, diversity, redundancy
- Difficulty to calculate the SIL Level of some functions
- Evolution of the system to cope with new risk
  - Complete iteration on the life-cycle -> slow process

New perspective

IEC 61511

- Process industry
- Global life-cycle for safety functions management from risk analysis to dismantling
- Methodology for risk analysis, definition of the safety function severity and system architecture performance verification
- Probabilistic approach
- Concept of Layer of Protection (LOPA)
- Certification for the safety engineers

IEC 61511 Layer of protection Analysis

IEC 61513

- Does not use the SIL concept
  - Severity of safety function (A,B,C)
  - System class (1,2,3)
- Instead of protection layers, notion of physical barriers
- Better coverage of aspects such as configuration management, computer security, testing, IHM, data communication
- Focus on environmental constraints such as radiation, EMC and other internal or external hazards
- Diversity of means to achieve the safety functions:
  - Common cause of failure & single mode of failure criteria
- Provide guidelines for the audit of the Nuclear Authority

Conclusion