Tomasz Ladzinski

LHC Access Safety System: from Design to 10 years in Service

LHC Access Project Team past & present collaborators:
P. Ninin, C. Delamare, S. Di Luca, G. Godineau, S. Grau, T. Hakulinen, L. Hammouti,
F. Havart, J-F Juget, T. Ladzinski, M. Munoz Codoceo, R. Nunes, T. Riesco,
E. Sanchez-Corral, L. Scibile, G. Smith, F. Schmitt, P. Sollander, F. Valentini & Cegelec/Semer

Agenda

- Personnel Safety Concepts at CERN
- Safety Lifecycle Approach
- LHC Implementation
- Testing & Commissioning Strategy
- Return of Experience
- Evolution Management

Organization

BE/ICS provides CERN's systems for **personnel safety and access control**

A centre of competence for large scale safety critical projects:

- project and contract management
- functional safety methodology
- conception and project management for LHC, PS and SPS PPS, SPS Fire Safety renovation, Laser rooms

CSE

Critical Safety Engineering

Pierre Ninin

Michael **Dole**
Timo **Hakulinen**
Louis **Hammouti**
Frédéric **Havart**
Jean-Francois **Juget**
Tomasz **Ladzinski**
Miriam **Munoz Codoceo**
Eva **Sanchez-Corral**
Anna **Suwalska**
Francesco **Valentini**

Installation, maintenance, operation, renovation and support of all:

- access & video systems including all the accelerators and the different CERN sites

AC

Access Control

Rui Nunes

Amadou **Anne**
Didier **Chapuis**
Serge **Di Luca**
Pablo **Gaviglio**
Grégory **Godineau**
Boris **Morand**
Nino **Rama**
Vitor **Rios**
Franck **Schmitt**
Grégory **Smith**
Didier **Vaxelaire**
Nouchigy **Yang**

- safety alarm systems; detection and protection systems (Fire, Flammable Gas, Oxygen Deficiency, Toxic Gas and Emergency telephones) and the safety alarm transmission systems to the relevant control rooms

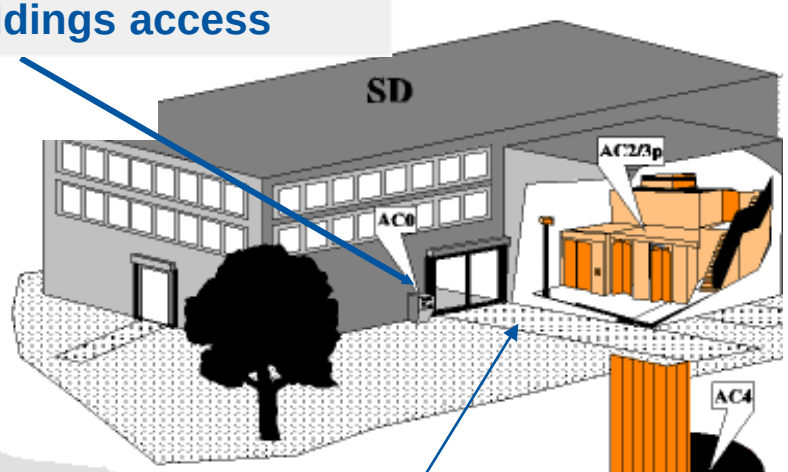
AS

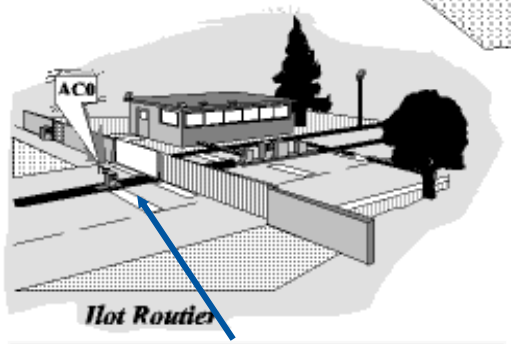
Alarm Systems

Silvia Grau

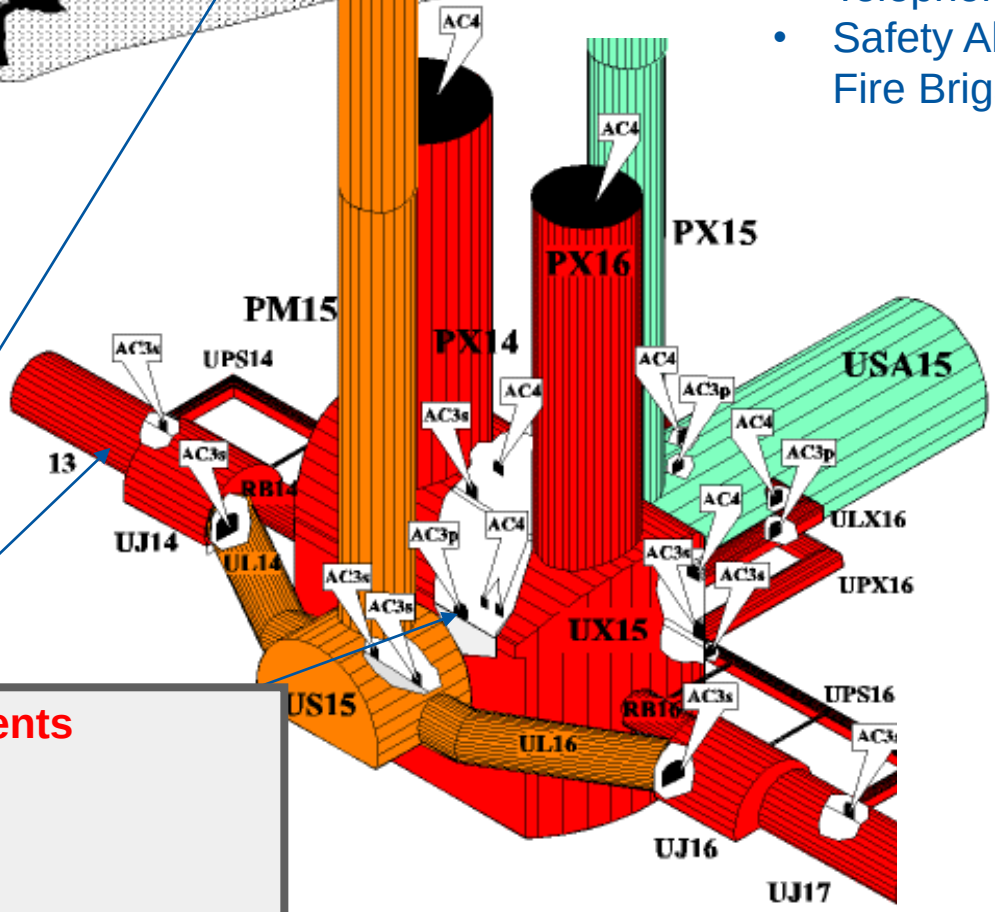
Fabio **Alfeo**
Melania **Averna**
Nicolas **Broca**
Pierre **Durand**
Henrik **Nissen**
Jean **Oliveira**
Denis **Raffourt**

LHC buildings access





LHC sites access

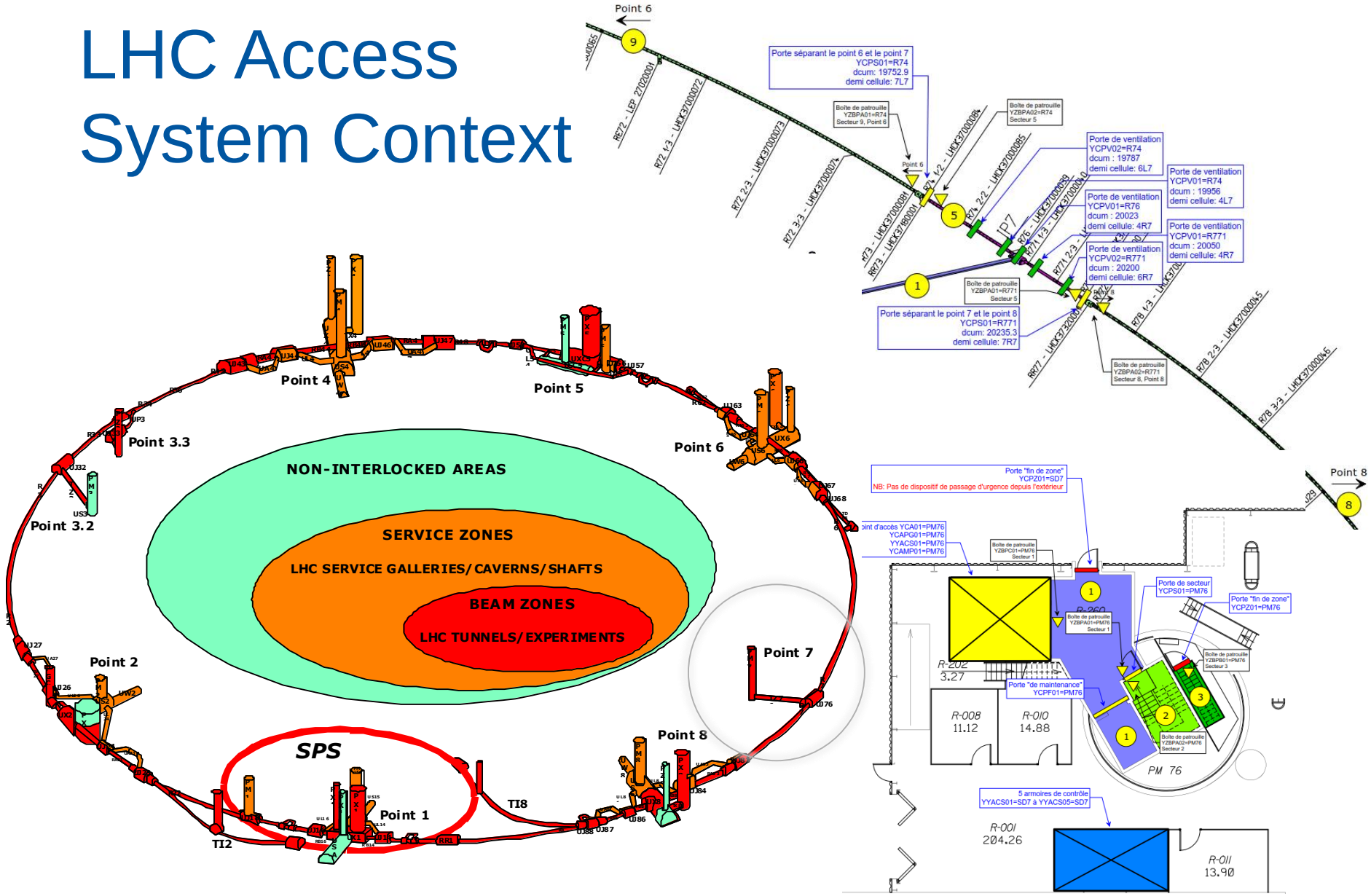


LHC accelerator and experiments
Access to Service areas
Access to Tunnel areas
Access to Experimental areas
NON ACCESSIBLE during beam operation

Conventional Alarm Systems required:

- Fire Detection
- Evacuation Systems
- Flammable Gas & ODH Detection Systems
- Emergency Telephones
- Safety Alarms to the Fire Brigade

LHC Access System Context



Goal of the LHC Access System

LASS – LHC Access Safety System

Main Interlocks:

Beam => No Access

Access => No Beam

Input: position sensors of the EIS
Output: Veto to EIS

Channel1: Siemens PLC
Channel2: Hardwired relay loop

LACS – LHC Access Control System

Main functions:

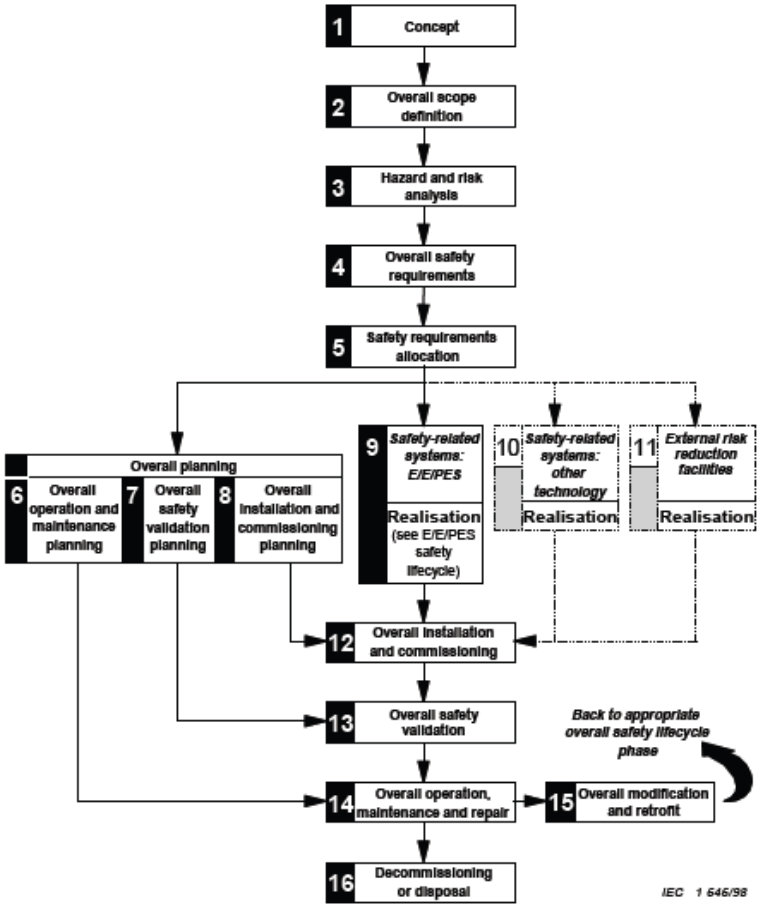
Authorisation verification
Person identification and authentication

Physical Barrier
Database: access authorisation, valid training & approved activity
Biometry
Single person passage
Video surveillance
Personnel counting in a zone

Integrated concept for LHC Machine & Experiments to protect personnel against the radiation hazards.

Safety Lifecycle

- Approach based on IEC 61508 & (61511/61513)
- Consider from early design stage aspects related to:
  - Operation & maintenance
  - Safety validation
  - Installation & commissioning
- Particular attention to two key concepts:
  - Single-failure criterion
  - Diversity (defense against common mode failures)
- Strict and procedural management of maintenance and modifications



NOTE 1 – Activities relating to ***verification***, ***management of functional safety*** and ***functional safety assessment*** are not shown for reasons of clarity but are relevent to all overall, E/E/PES and software safety lifecycle phases.

NOTE 2 – The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 – IEC 61508-2 and IEC 61508-3 deal with box 9 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

System Requirements

- Preliminary Risk Analysis
  - LHC Access Working Group
  - Consultant from Schneider Electric
  - Scope limited to radiation hazards (prompt and remnant from beam operation, as well as X-rays from the RF cavities)
- Instrumented Safety Functions specified – three major families:
  1. Monitoring EIS-access in Beam/RF operation and stopping the Beam/RF in case of intrusion – SIL3
  2. Monitoring the EIS-beam/machine in Access operation and blocking access or evacuation, in case of degradation of safety barriers - SIL3
  3. Subdivision of the LHC into smaller access zones and sectors and monitoring their state so as to force human patrol of the areas where the system is not sure of the absence of personnel – SIL2
- Performance Requirements:
  - Safety Integrity Level 3
  - Slow process – response time of 1-2s
  - Interlock availability non-stop (reliable maintenance and monitoring tools required)

LASS PLC Architecture

Siemens PCS7

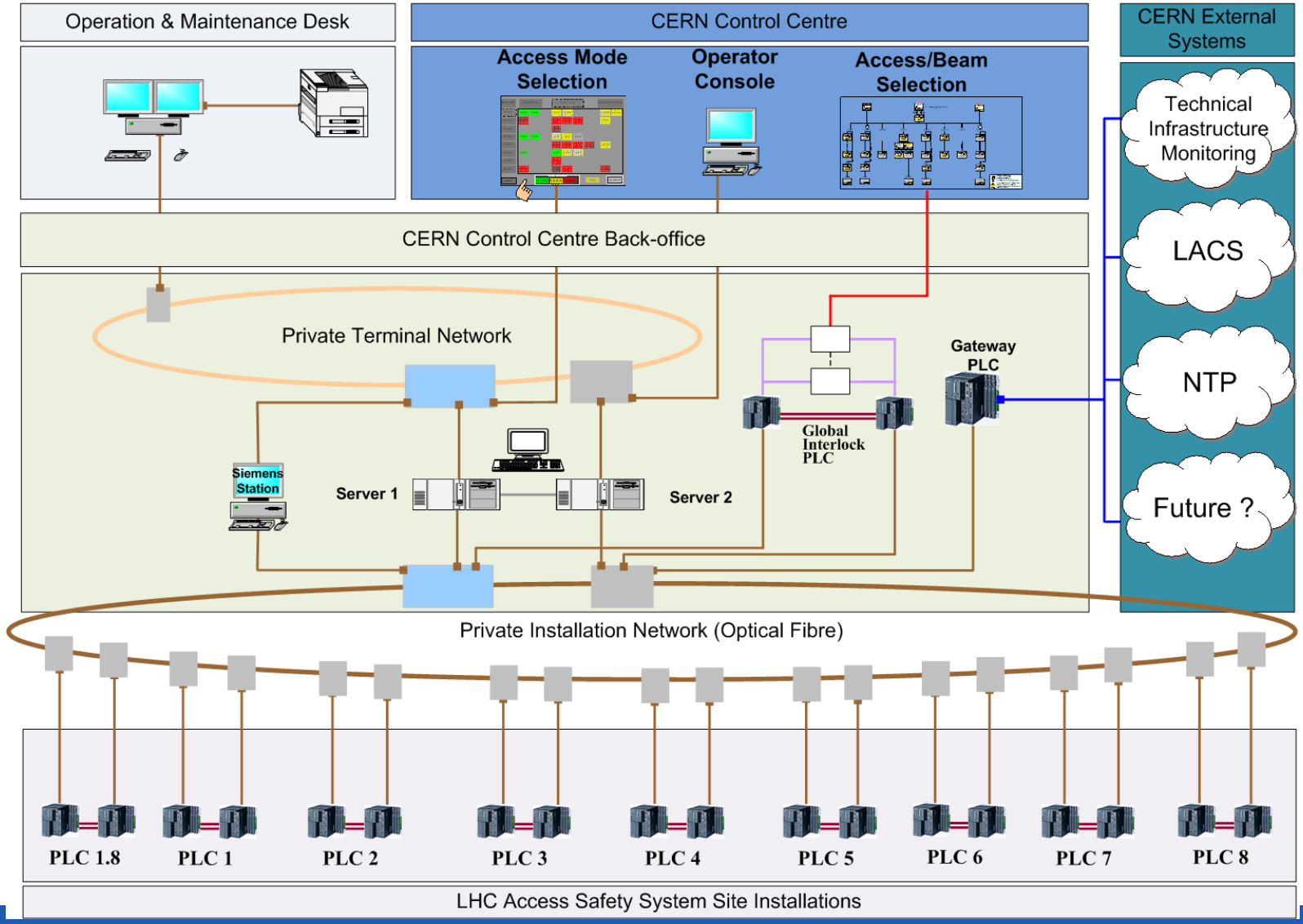
Monomode fibre ring

Gateway to CERN TN

Monomode fibre ring Profisafe

Siemens PLC 417 FH

Profibus



LASS Racks in 9 LHC Sites

- Five access racks in each LHC site hosting PLC + I/O modules
- Equipment at surface level
- Powered from CERN normal and secured networks via Benning Power Supplies - batteries with 8 hours autonomy

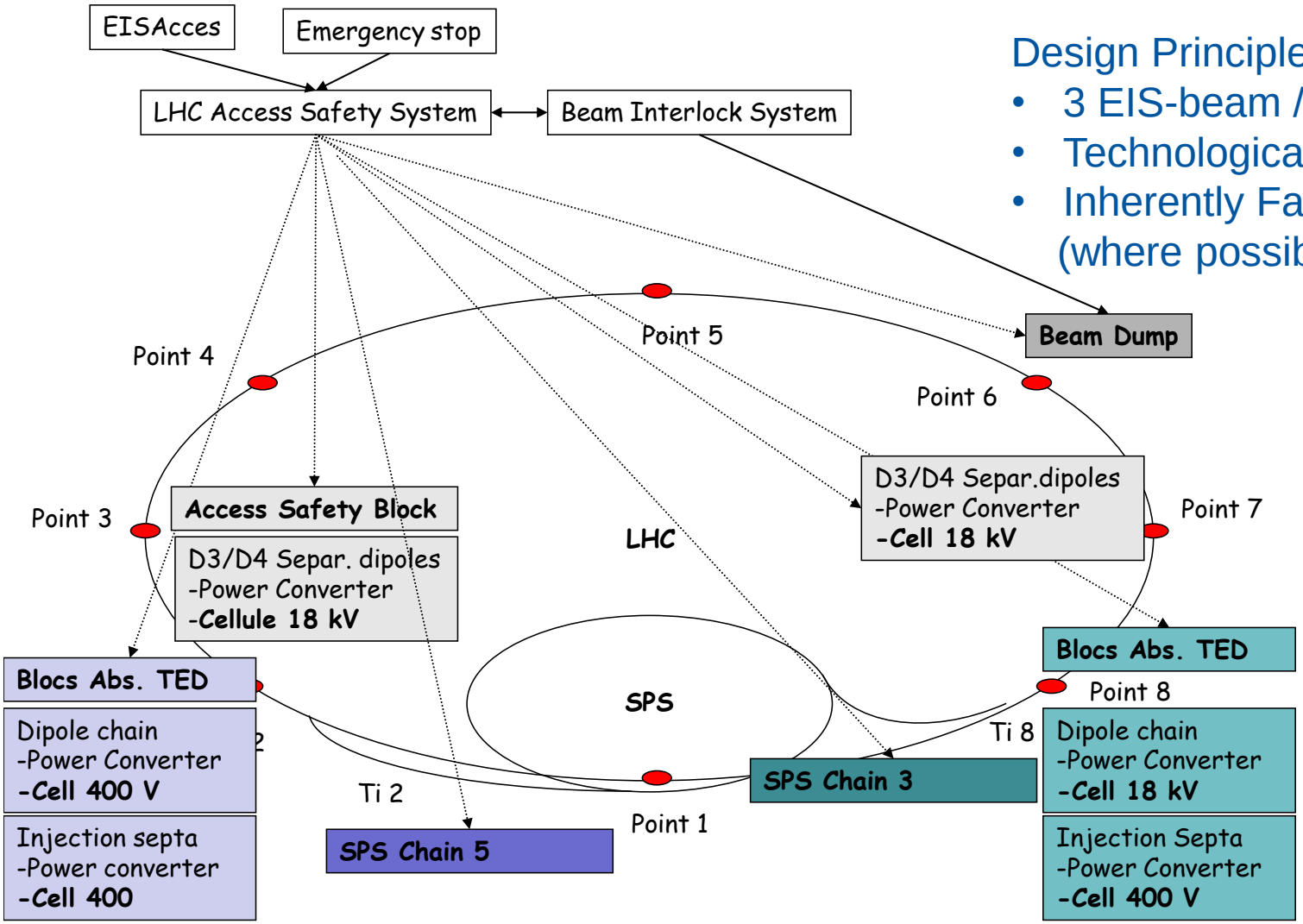
LHC Access System in Numbers

- 35 access points
- 95 interlocked sector doors
- 67 interlocked end-of-zone doors
- 20 interlocked ventilation doors
- 26 interlocked trap doors
- 17 interlocked mobile shielding walls
- 53 monitored ventilation doors (Helium discharge)
- 280 patrol boxes
- ~200 junction boxes
- ~170 racks
- ~110 video cameras
- ~200 controllers (PLC, PC, etc.)

Inputs/Outputs – EIS-Access

- Personal Access Device:
  - 6 x FDI
  - 2 x FDO
- Material Access Device
  - 4 x FDI
  - 1 x FDO
- Sector Door (Other doors)
  - 4 x FDI (2 x FDI)
  - 1 x FDO
- Shielding Wall
  - 1 x FDI
  - 1 x FDO
- Patrol Box
  - 1 x FDI
  - 1 x DO

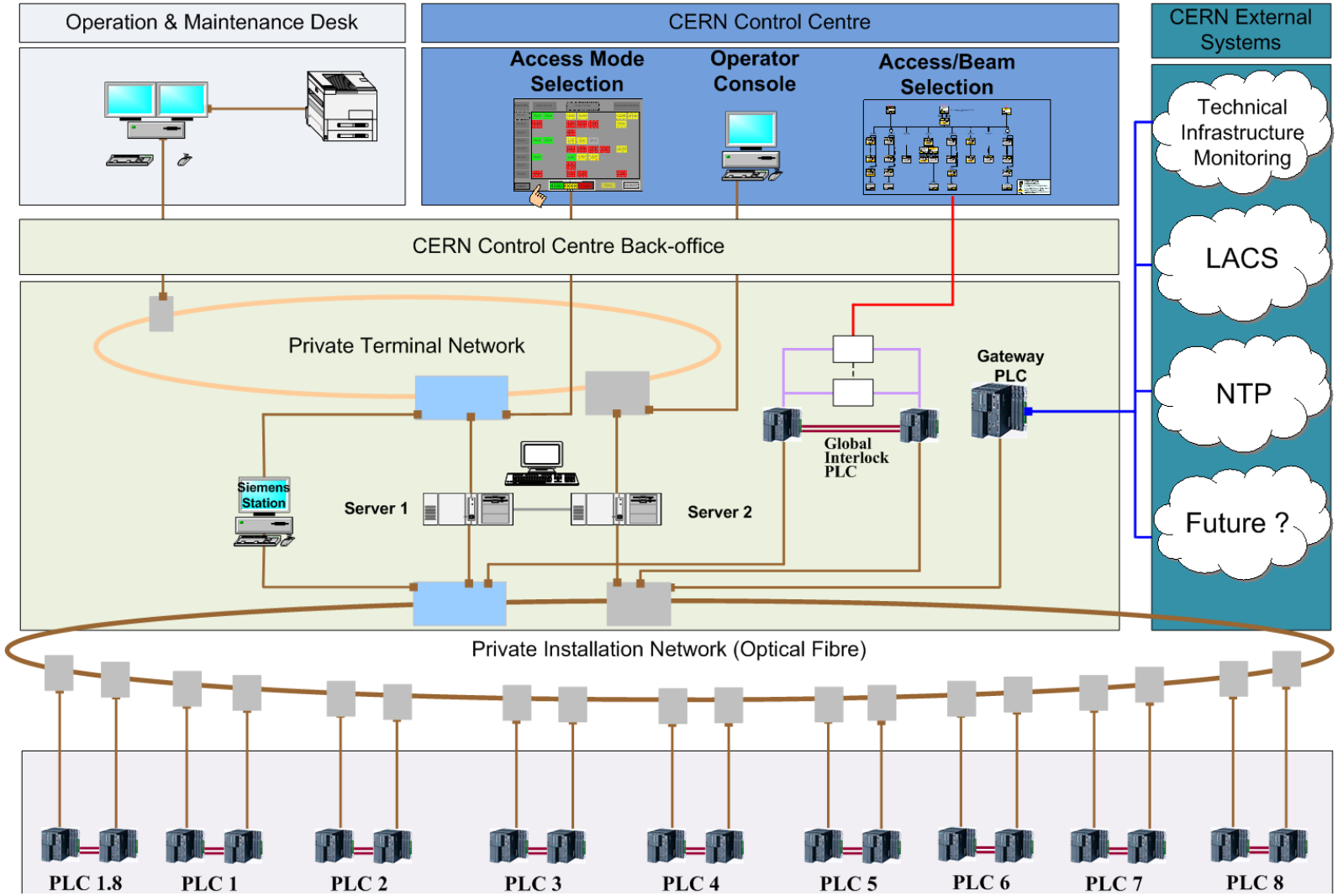
Important Safety Elements for Beam



Design Principles:

- 3 EIS-beam / Interlock Chain
- Technologically Diverse
- Inherently Failsafe (where possible)

LASS PLC Architecture

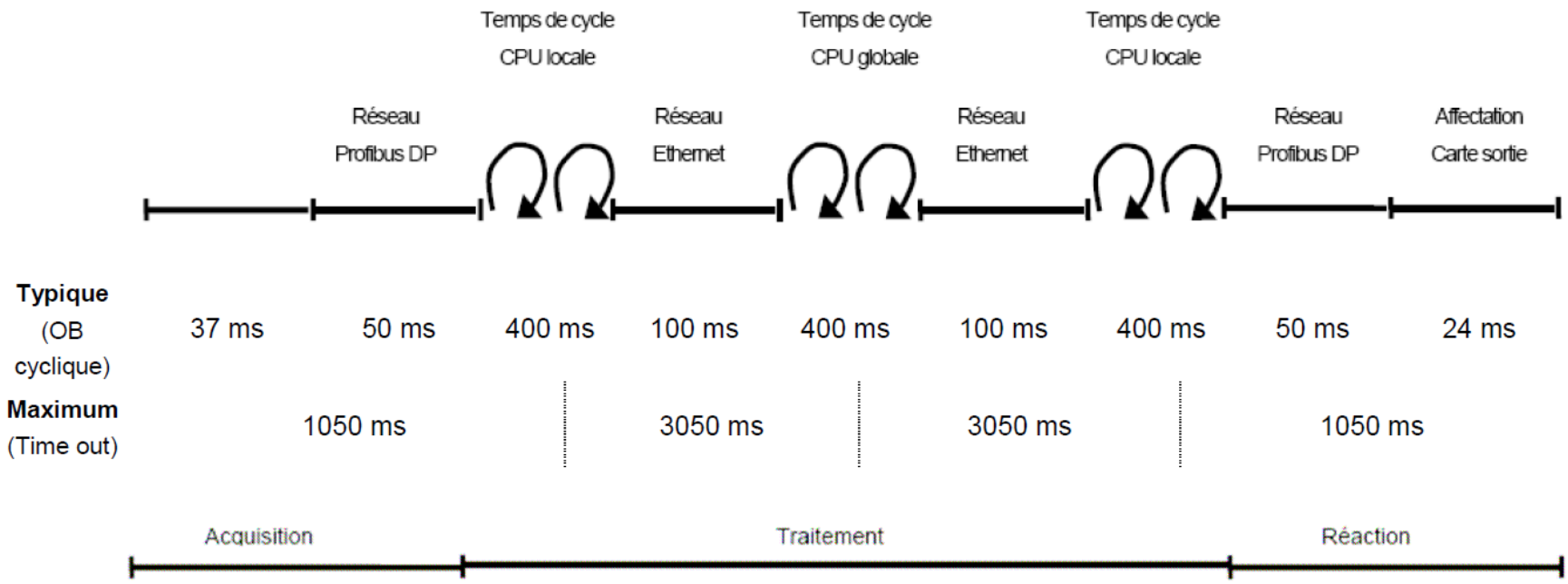


Total: ~3'800 digital inputs & ~800 digital outputs

Design Principles for I/O

- All I/O modules in dedicated closed racks at the surface level.
- Inputs:
  - Complementary signals (NC and NO) acquired over independent cabling (separate cables and cable trays)
  - 48 V intermediate relay boards – distance imposed
  - 1oo2 voting – Siemens FDI set with zero substitute value
- Outputs:
  - Two dry contacts acting in series on the power supply of an actuator. Contact opened = veto applied.
  - 48 V intermediate relay boards
  - Siemens FDO modules

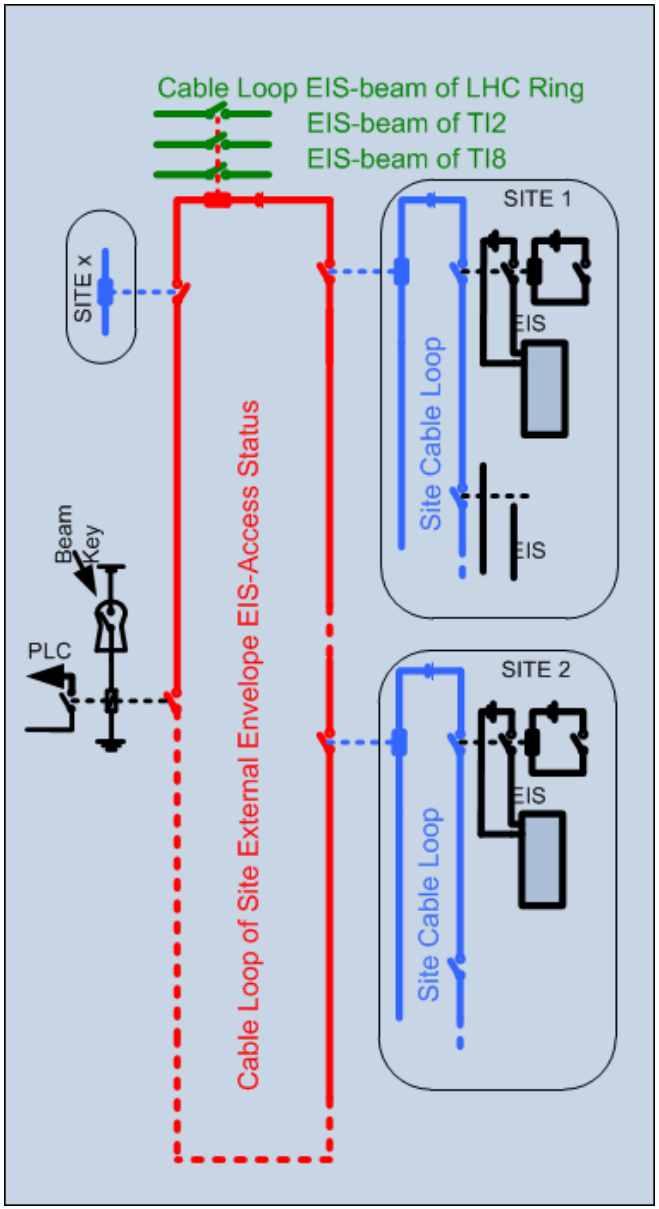
PLC Performance Constraints



- The French nuclear safety authorities encourage the use of technologically diversified systems.
- Moreover, for LASS, the maximum PLC response time of ~8s was judged too long in case of an intrusion.

Hardwired Relay Loop

- Intrusion detection in beam mode and action on the EIS-beam in parallel to the PLC system
- Only the external access envelope of the LHC is monitored
- Local loop of NC contacts for each LHC site
- LHC loop with a result contact per site
- Simple to demonstrate the correct behavior



Safety Development Process

- Preliminary Risk Analysis
  - Analysis of the risks that will be covered by the system
- Definition of the Safety Instrumented Functions
  - It goes further than the classical interlock definition
  - SIL allocation
- Preliminary Safety File
  - Based on system functional analysis and architecture definition
  - Verifies that the defined SIL level is achieved for every function (sensor to actuator)
  - Failure Modes and Effects Analysis
  - Common cause failure, Single failure criterion
- System design and realisation based on the V life-cycle
- Update of the Safety File
  - Based on the as-built, verification of the SIL level achieved
- Verification and Validation Strategy
- Organisation and description of the Operation and Maintenance
- Definition and test execution by an independent testing team

Testing Stages

Software

- Contractor:
  - HMI soft on test platform
  - Safety soft by the developer
  - Safety soft by dedicated tester on the test platform – checksum recorded
- CERN on the test platform
  - Deployment (new site / version) – checksum verified
  - Tests on site by CERN team (~15pers/2days/site) of all newly added equipment/functionalities *(normally no surprises…)*
  - Beams Department Safety Officer conducts independent tests at the end of each annual shutdown (random moving sample).

Hardware

All signals tested by the contractor (one by one)

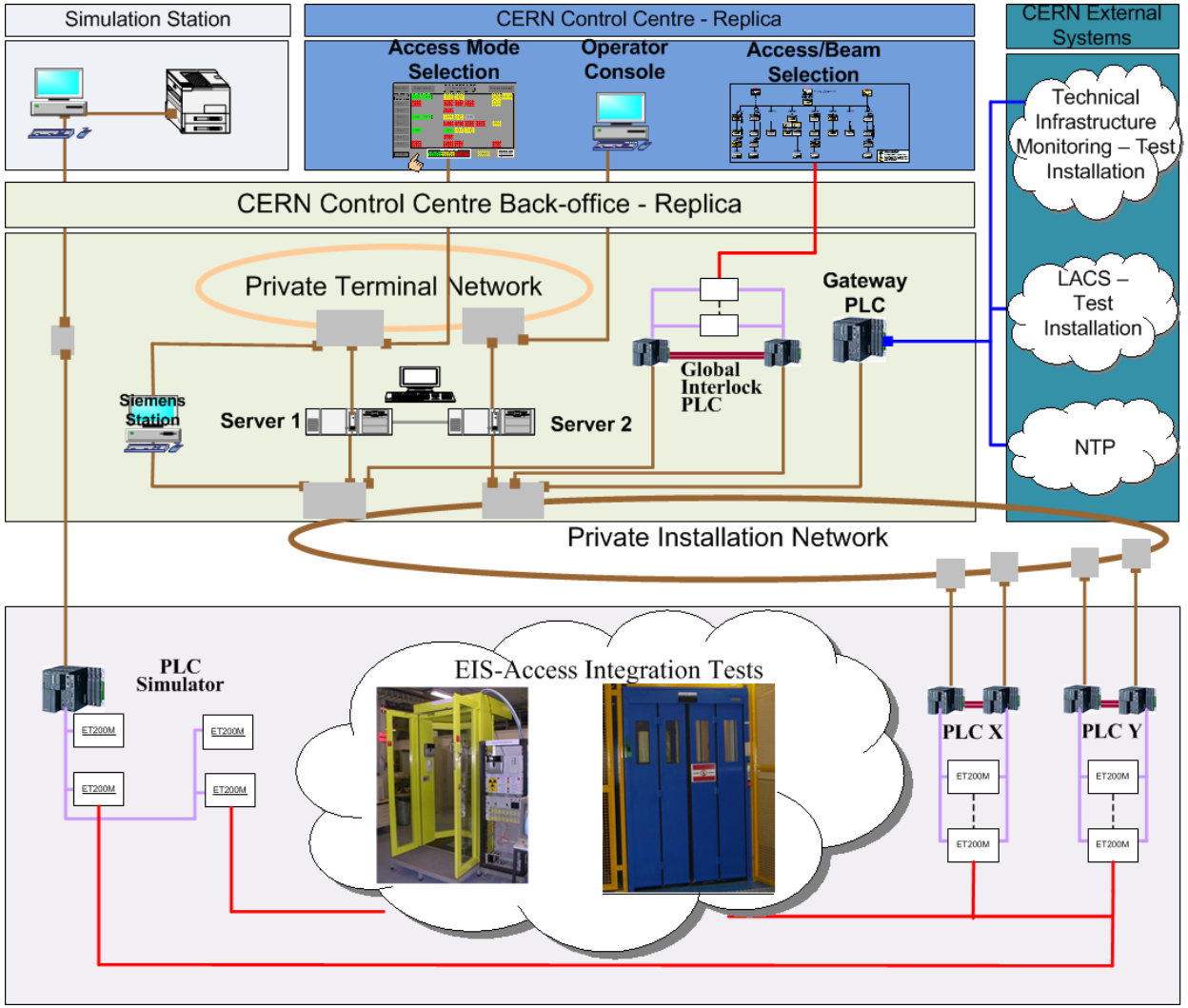
- Reception tests of individual pieces of equipment (LACS)

Process for new system and any upgrade (2009, 2010, LS1…).

Annual maintenance and tests (essential to maintain SIL level)

LHC0 Test Platform

- Test software
- Test integration with access equipment
- Reproduce errors
- Learn how to operate the system
- Limits:
  - load tests
  - reconfiguration



Return of Experience - Availability

- Safety (LASS availability)
  - Until today safety has never been compromised, the system has always been available
- Process (LHC availability)
  - Very few spurious trips ~2 beam dumps / year.
    - Origin: field equipment position switches/relays, hardwired connection with another safety system, I/O card
    - Improvement: adjustment of the switches and introduction of Last Valid Value filtering
  - Indirect impact when patrols lost during access due to glitches of position switches
    - Origin: field equipment position switches
    - Improvement: adjustment of the switches and better synchronisation of access device inner and outer doors (PAD)
    - Impact non negligible as organising a patrol and conducting it can take a few hours
  - Redundant PLCs – beam never lost due to a PLC error, but switchover time vs safety timeout a difficult compromise
    - On a few occasions the switchover was due to an error in the optical communication module linking the two CPUs...

Return of Experience - Maintainability

LASS is operational in Beam and in Access modes:

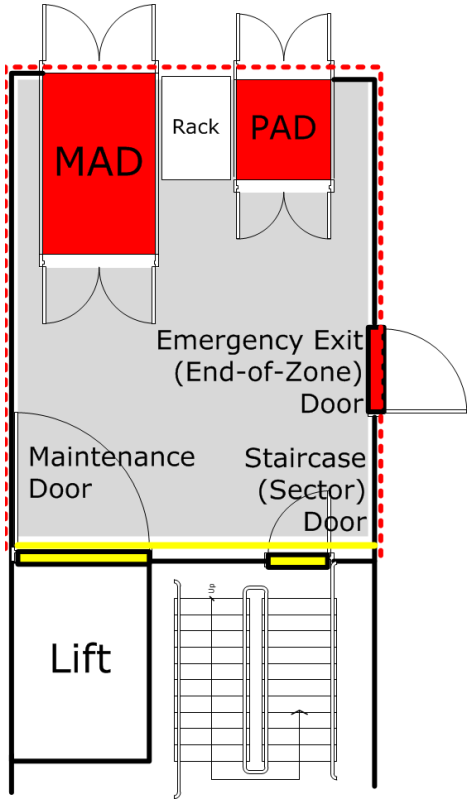
- Very difficult to get time for annual system maintenance
- Very difficult to get a slot for corrective maintenance
  (e.g. recurrent lost patrols due to the same access device, but no slot granted to intervene)
- Signals from EIS-beam have to be bypassed to allow maintenance - tricky

Improvements:

- Planning/organisation
- Introduced modification: shifting the external barrier to an additional “maintenance door” behind the access points to allow maintenance of complex access devices while in Beam mode.
- Introduction of out-of-chain procedure with keys to disconnect an EIS-beam from its interlock chain

Maintenance Improvements

Maintenance Doors



Out-of-chain mechanism

- The requester fills in a ticket, which is electronically approved by all concerned.
- The Departmental Safety Officer takes the required compensatory measures.
- Once approved, the out-of-chain intervention can take place only in Access mode – turn a key.
- **Supplementary safety function does not allow switching over from Access to Beam mode**, as long as all elements are not back in the original safety chain.

Return of Experience - Sustainability

- Expected system life-time: 25 years
- FS-PLC lifetime limited by standard to 20 years max
- PLCs have long technological and support lifetime
- Servers and PCs running SCADA need regular migrations/exchanges
  - PCS7 migrated from v.6.1 to v.8.0 (WinXP -> Win7, MS Server 2003 -> MS Server 2008)
  - Underlying safety library changed: impact on all safety checksums, long sorting out with the contractor and vendor on the tests required.

Change Management

- CERN wide: any change must first be approved
  - Engineering Change Request template.
  - Strict approval process managed by a baseline coordinator
- For safety systems:
  1. All concerned are aware of future modifications and approve them
  2. Any modification to a subsystem with impact on a safety system is analyzed and adequate actions taken (e.g. power converters upgraded)

ECR Template

6. IMPACT ON OPERATIONAL SAFETY

[This chapter aims at assessing the impact of the modification on people safety, on the environment, and on the safety of operations, including maintenance, access, egress, circulation and evacuation.]

6.1 ÉLÉMENT(S) IMPORTANT(S) DE SECURITÉ

[Indicate if the change will have an impact on an *Elément Important de Sécurité* (EIS). The list of EIS components is available in EDMS document: 1182293 – "Définition et Inventaire des EIS-Faisceau et EIS-Machine en Opération".]

Requirement	Yes	No	Comments
EIS-Access	X		Creation of new EIS-Access of the ECA5 access point.
EIS-Beam		X	Indirectly, as the access point equipment is interlocked with EIS-beam of SPS Chain 1.
EIS-Machine		X	

LHC Access LS1 Modifications

- Sectorisation changes
  - Relocation of three access points (R2E effects)
  - Displacement of inter-machine door, addition of a new one, displacement of patrol boxes
  - Addition of a new access zone with its access point
  - New controlled and limited stay areas (radiation veto signals)
- Scope enlargement
  - Monitoring of Helium confinement doors and interlocking magnet powering
  - Monitoring of doors important to the release of activated air and interlock of injection from the SPS
- Availability Enhancements
  - Introduction of maintenance doors to facilitate access point maintenance while in beam mode
  - Upgrade of OS, PCS7 migration etc.

LS1 Modifications cont.

- A total of 9 approved ECR requests.
- Testing strategy as for the initial system installation:
  - Unit tests by the contractor
  - LHC0 tests
  - On-site tests for each new feature e.g. for the access-powering interlock: 5 days of tests involving ~15 people
  - DSO tests
- Entire documentation updated.
- Upgrade of the system is a full project.

Conclusions

- LHC Access Safety System operates 24h/365d protecting the personnel from radiation hazards, as well as contributing to protection from massive Helium discharge.
- Fire, flammable gas, oxygen deficiency hazards are taken care of by dedicated systems.

- Designed to meet SIL3 following a functional safety methodology based on the IEC standards.
- Core system uses Siemens 417 FH PLCs complemented with a simple relay logic cabled loop for technological diversity.
- Realization outsourced to an external company.
- Accepted by the French nuclear safety body.
- Periodically upgraded, following the same strict functional safety methodology and V&V process.
- No major problems detected, good performance and availability record.

www.cern.ch