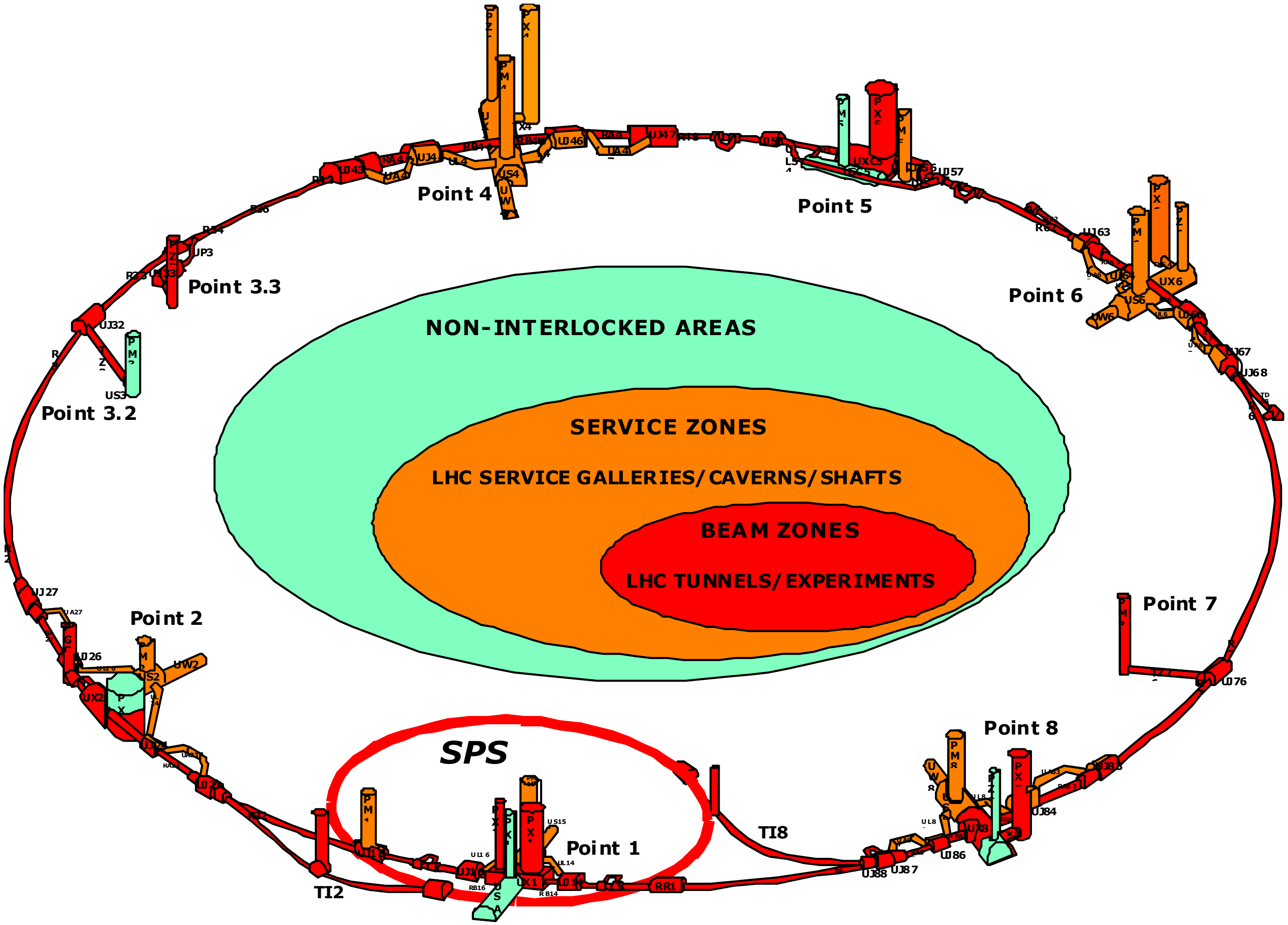
Tomasz Ladzinski

LHC Access Safety System

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

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: person authorisation & valid training
Biometry
Single person passage
Video surveillance
Personnel counting in a zone

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

Access Safety 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:
  - Monitoring EIS-access in Beam/RF operation and stopping the Beam/RF in case of intrusion – SIL3
  - Monitoring the EIS-beam/machine in Access operation and blocking access/evacuation in case of degradation of safety barriers – SIL3
  - 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 v.6.1

Monomode fibre ring

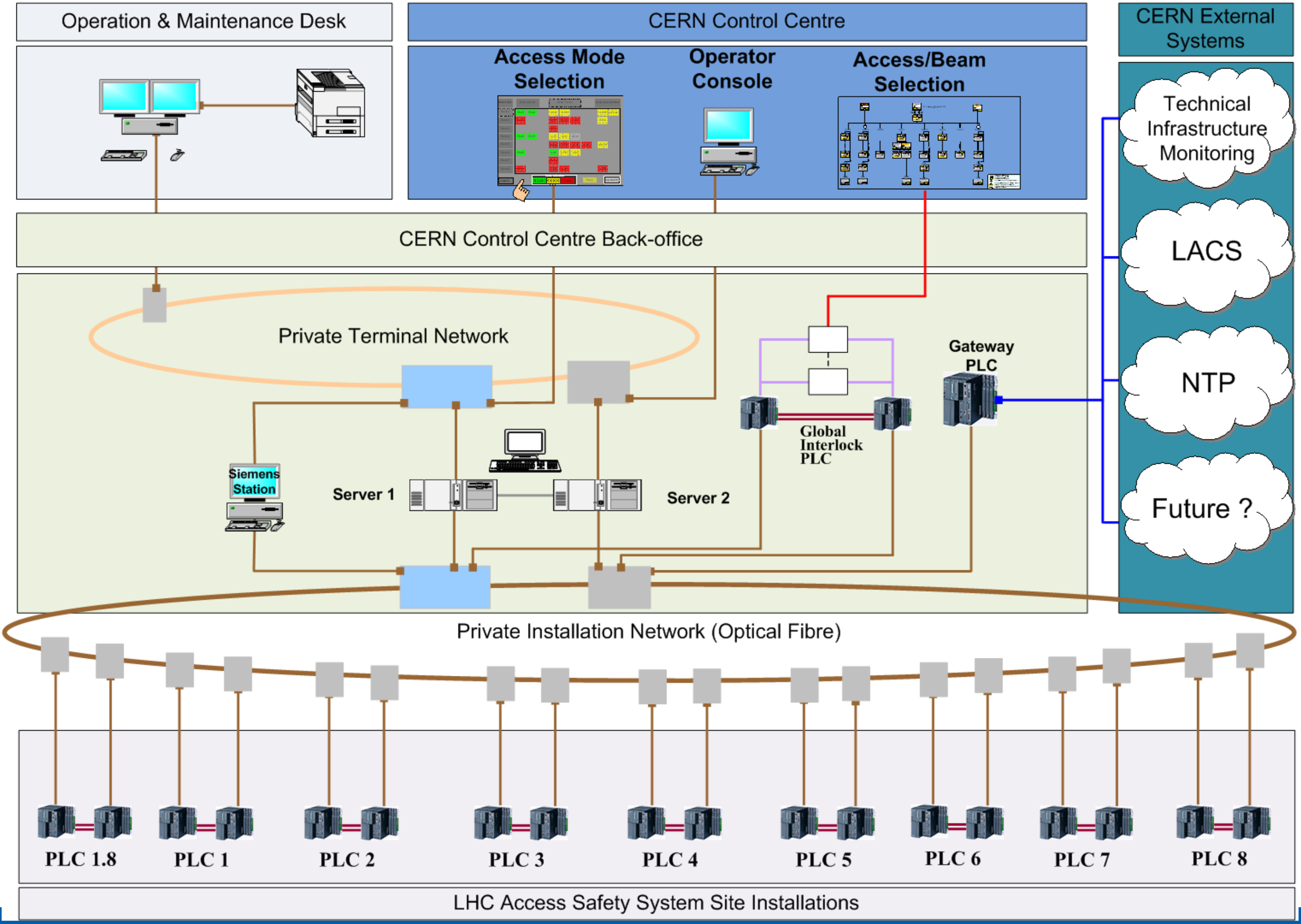
Gateway to CERN TN

Monomode fibre ring

Profisafe

Siemens PLC 417 FH

Profibus



LASS Racks in 9 LHC Sites

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

Access System in Figures

- 34 access points
- 95 interlocked sector doors
- 65 interlocked end-of-zone doors
- 17 interlocked ventilation doors
- 26 interlocked ladder doors
- 17 interlocked mobile shielding walls
- 276 patrol boxes
- 200 junction boxes
- 170 racks
- 110 video cameras
- 200 controllers (PLC, PC, etc.)

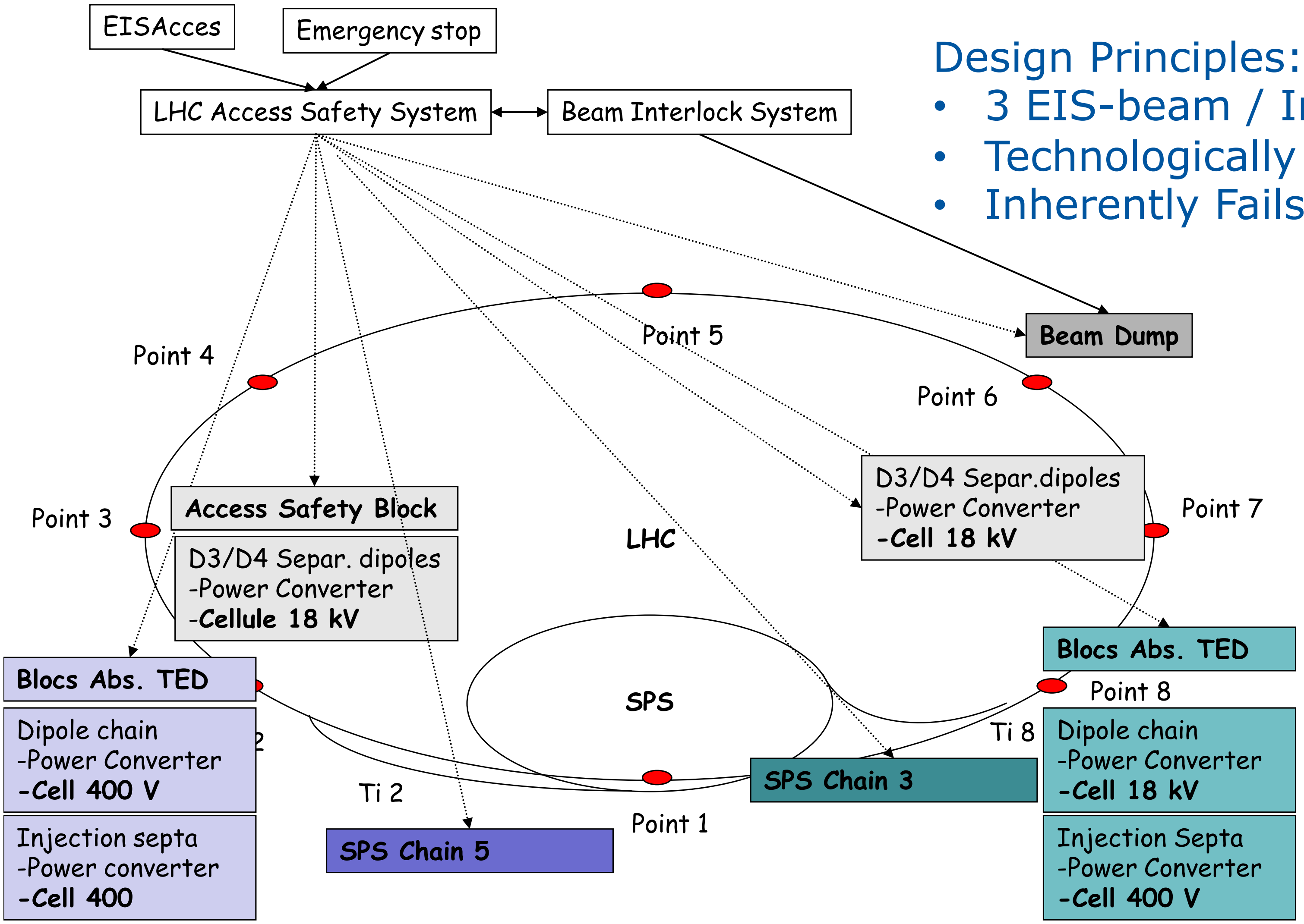
Inputs/Outputs – EIS-Access

- 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



EISAcces

Emergency stop

LHC Access Safety System

Beam Interlock System

Beam Dump

Point 4

Point 5

Point 6

Point 3

Point 7

Access Safety Block

D3/D4 Separ. dipoles
-Power Converter
-**Cellule 18 kV**

LHC

D3/D4 Separ.dipoles
-Power Converter
-**Cell 18 kV**

Blocs Abs. TED

SPS

Blocs Abs. TED

Point 8

Dipole chain
-Power Converter
-**Cell 400 V**

2

Ti 8

Dipole chain
-Power Converter
-**Cell 18 kV**

SPS Chain 3

Ti 2

Point 1

Injection septa
-Power converter
-**Cell 400**

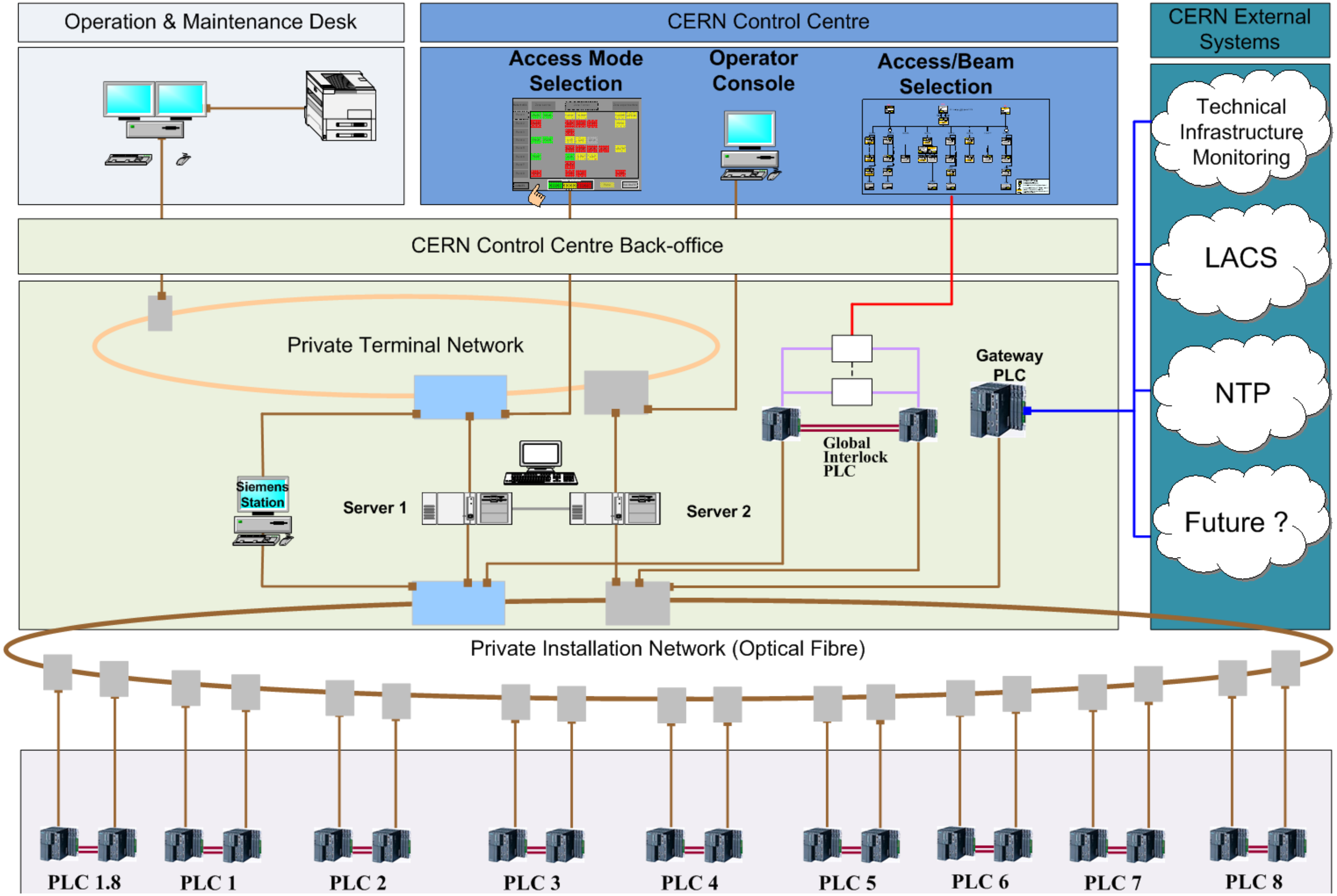
SPS Chain 5

Injection Septa
-Power Converter
-**Cell 400 V**

Inputs/Outputs – EIS-Beam

- Magnet Power Converter & Cell
  - 4 x FDI
  - 1 x FDO
- Mobile Beam Dump (TED)
  - 4 x FDI
  - 1 x FDO
- Vacuum Valves (ASB & ES)
  - 3 x FDI
  - 1 x FDO
- RF
  - 2 x FDI
  - 2 x FDO
  - 2 x DO
- LBDS & BIS
  - 4 x FDO
  - 10 x DI

LASS PLC Architecture

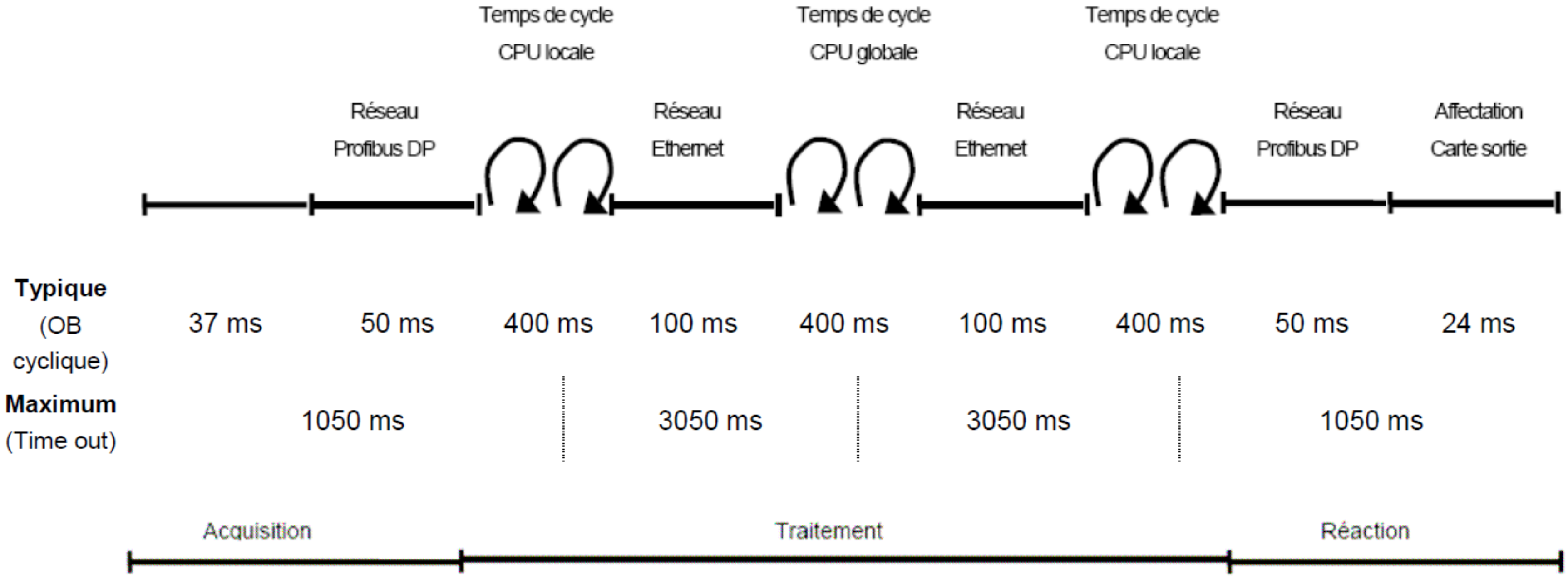


Total: ~3’800 digital inputs & ~800 digital outputs

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
  - 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



		Réseau Profibus DP	Temps de cycle CPU locale	Réseau Ethernet	Temps de cycle CPU globale	Réseau Ethernet	Temps de cycle CPU locale	Réseau Profibus DP	Affectation Carte sortie
Typique (OB cyclique)	37 ms	50 ms	400 ms	100 ms	400 ms	100 ms	400 ms	50 ms	24 ms

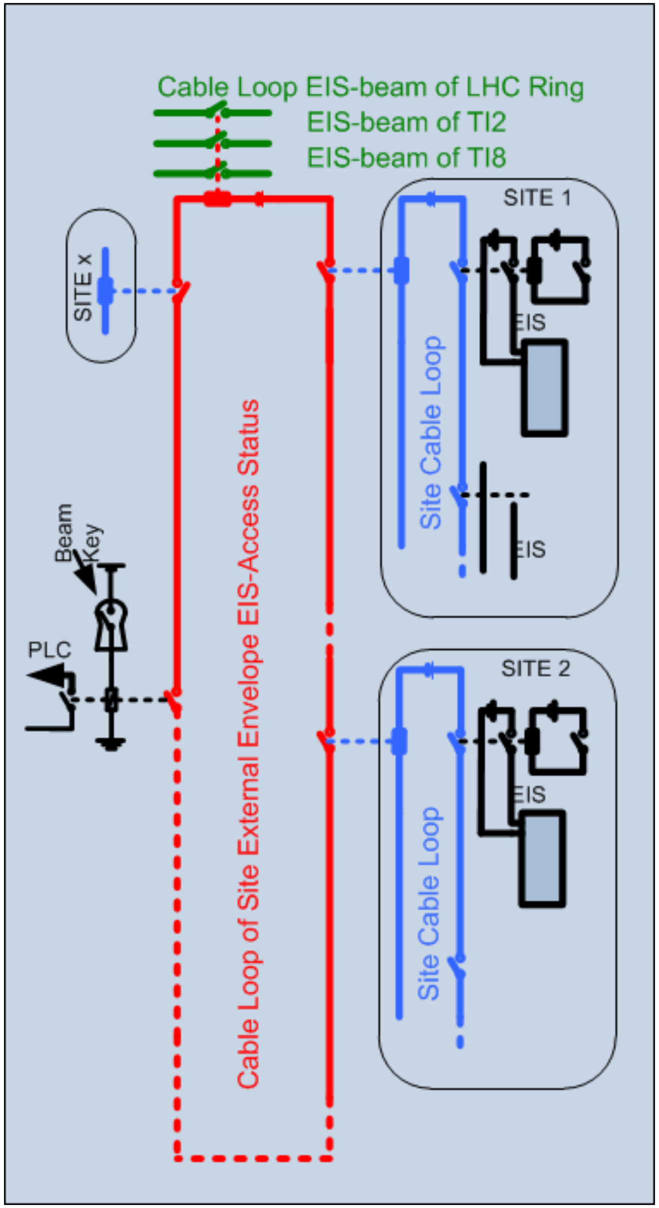
Maximum (Time out): 1050 ms | 3050 ms | 3050 ms | 1050 ms

Acquisition — Traitement — Réaction

- The French nuclear safety authorities encourage the use of technologically diversified systems.
- Moreover, in case of 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

Hardware

- All signals tested by the contractor (one by one)
- Reception tests of individual pieces of equipment (LACS)

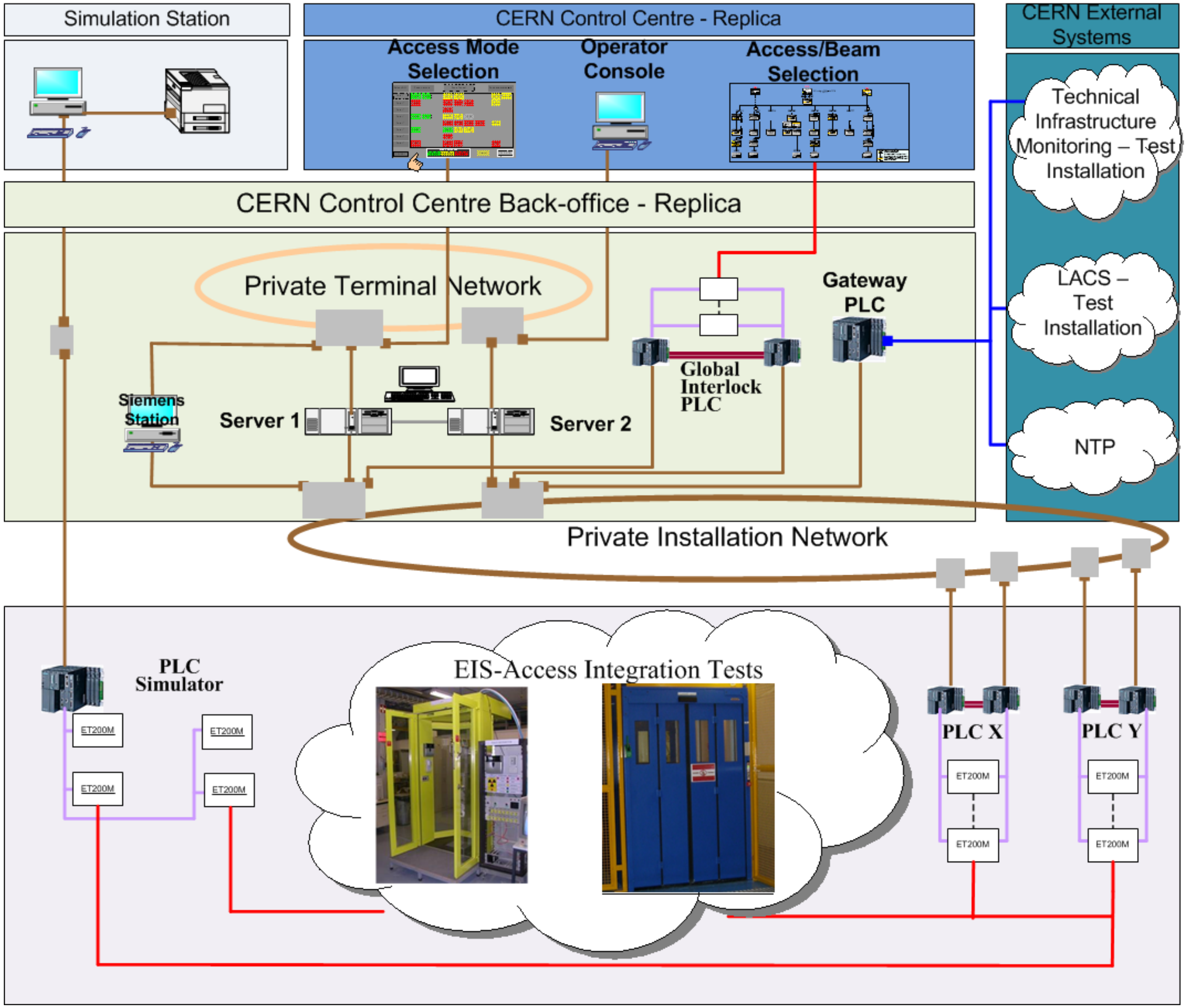
- Deployment (new site / version) – checksum verified
- Tests on site by CERN team (~15pers/2days/site) of all newly added equipment/functionalities *(normally no surprises…)*
- Beams Department Safety Officer conducts independent tests at the end of each annual shutdown (random moving sample).

Process for new system and any upgrade (1 in 2009, 1 in 2010).

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 max.
    - Origin 1: field equipment position switches
    - Origin 2: hardwired connection with another safety system
    - Improvement 1: adjustment of the switches
    - Improvement 2: possible 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 1: adjustment of the switches
    - Improvement 2: better synchronisation of access device inner and outer doors
    - Impact non negligible as organising a patrol and conducting it can take a few hours

Return of Experience - Maintainability

LASS is operational in Beam and in Access modes:

1. Very difficult to get time for annual system maintenance
2. 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)
3. Signals from EIS-beam have to be bypassed to allow maintenance - tricky

Improvements:

1. Planning/organisation
2. Introduced now: shifting the external barrier to an additional "maintenance door" behind the access points to allow maintenance of complex access devices while in Beam mode
3. Introduction of keys disconnecting the EIS-beam from interlock chain (with strict procedure and approval process)

Return of Experience - Sustainability

- Expected system life-time: 15-25 years
- 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, being sorted out with the contractor and vendor

Return of Experience – Redundant PLC

- LHC Commissioning Phase
  - In June 2008 during the LHC commissioning without beam a new LASS version was installed with "improved" diagnostics. This generated saturation in LASS PLCs leading to subsequent blocking of access to the LHC.
  - Error was not detected on the test platform.
  - Partially solved by correcting the badly written diagnostics software.
  - Unveiled an issue with synchronization of software between two redundant PLCs and fine tuning of the safety communication parameters.
- LHC Operation Phase (Fall 2008 – today)
  - 4 occurrences of one PLC stopping, the second PLC continued to work, no impact on the LHC
  - 3 occurrences traced to faulty communication between the two redundant PLCs

Conclusions

- LASS operates 24h/365d
- Designed to meet SIL3 (IEC 61508/511)
- Core system based on Siemens 417 FH PLCs complemented with a simple relay loop
- Outsourced to an external company
  - 2 years of design, development and installation
  - 1 year of gradual commissioning and tests
- Approved by the French nuclear safety body
- No major problems detected, good performance and availability record.

- Injector chain access safety systems are currently refurbished based on similar principles, with the return of experience leading to:
  - Use of the same PLC for access device control and safety
  - No redundant PLCs
  - Improved test platform to allow load testing and fast configuration

www.cern.ch