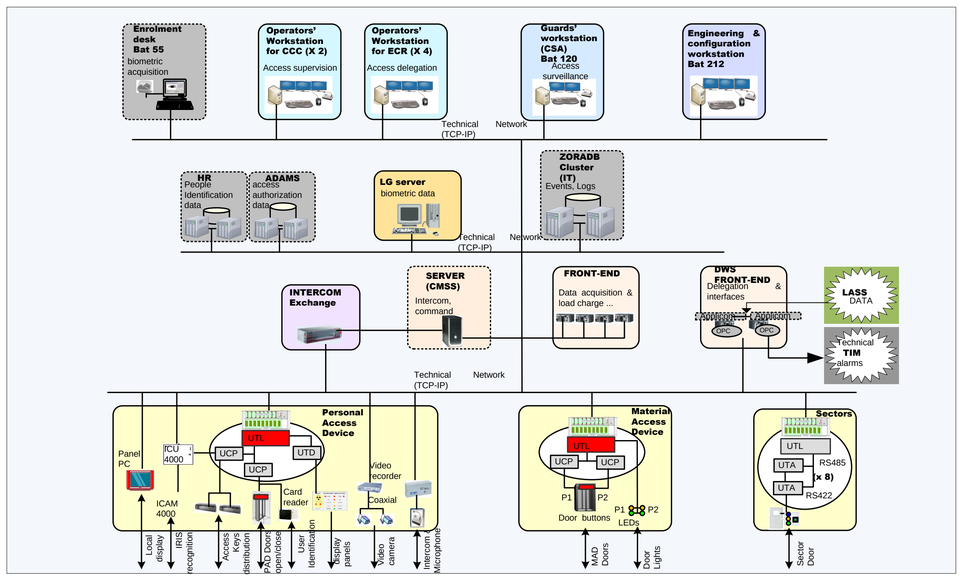
Access Safety Systems

New Concepts from the LHC Experience

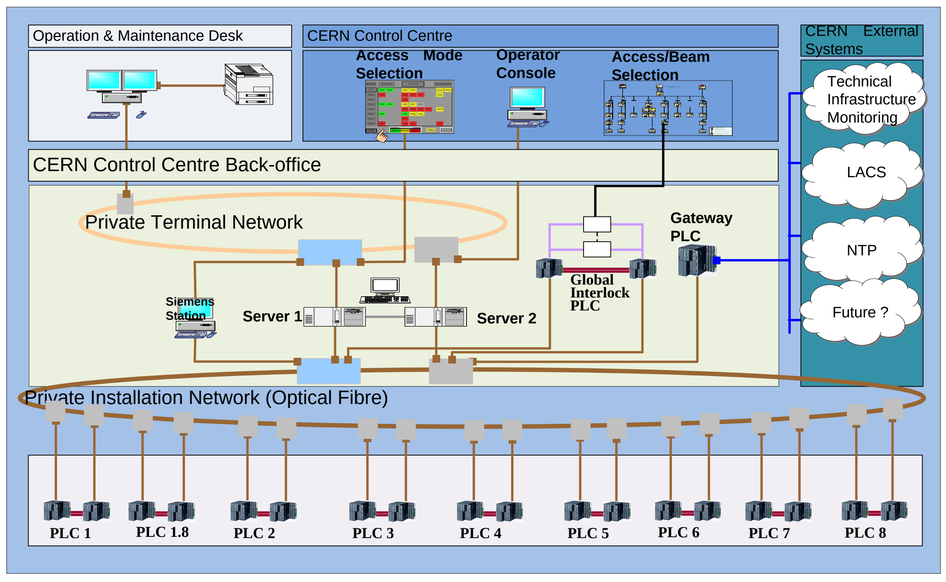
The LHC Access Safety System has introduced a number of new concepts into the domain of personnel protection at CERN. These can be grouped into several categories: organisational, architectural and concerning the end-user experience. By anchoring the project on the solid foundations of the IEC 61508/61511 methodology, the CERN team and its contractors managed to design, develop, test and commission on time a SIL3 safety system. The system uses a successful combination of the latest Siemens redundant safety programmable logic controllers with a traditional relay logic hardwired loop. The external envelope barriers used in the LHC include personnel and material access devices, which are interlocked door-booths introducing increased automation of individual access control, thus removing the strain from the operators. These devices ensure the inviolability of the controlled zones by users not holding the required credentials. To this end they are equipped with personnel presence detectors and the access control includes a state of the art biometry check. Building on the LHC experience, new projects targeting the refurbishment of the existing access safety infrastructure in the injector chain have started. This paper summarises the new concepts introduced in the LHC access control and safety systems, discusses the return of experience and outlines the main guiding principles for the renewal stage of the personnel protection systems in the LHC injector chain in a homogeneous manner.

CERN/GS/ASE Access Project Team:
C. Delamare, S. Di Luca, T. Hakulinen, L. Hammouti, F. Havart, J-F Juget, ***T. Ladzinski****, P. Ninin, R. Nunes, T. Riesco, E. Sanchez-Corral Mena, F. Valentini*

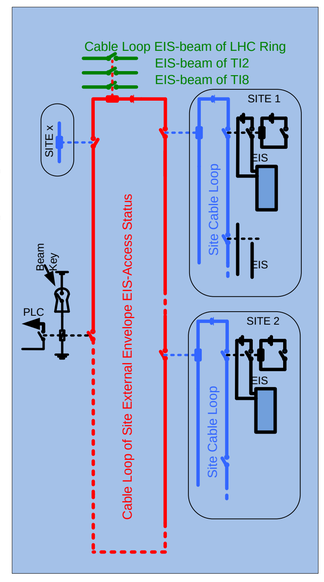
The LHC Access System : Access Control and Access Safety Architecture Concepts



Control & Safety Separation



Two Channel Safety System



Material Access Device (MAD)

An EIS-access assuring the inviolability of the LHC external envelope and a barrier between the interlocked zones.
29 units installed in the LHC

Allows the introduction of bulky material.

Human presence detection system comprising:
- Infrared barriers;
- Two volumetric detectors
- Video motion detection with a millimetre resolution.

Personnel Access Device (PAD)

An EIS-access assuring the inviolability of the LHC external envelope and a barrier between the three types of interlocked zones (Service, Tunnel and Experiment).
Next to each LHC PAD (40 in total), there is a Safety Token (also called "Restricted mode key") distributor.

User Identification with verification of access rights and the status of periodic compulsory training and tests.

Biometry Iris Scan to validate user identification.

A complex automatic system based on ground pressure sensors, infrared radar and photo-electric cells surveying the PAD at each passage to eliminate piggybacking and tailgating.

Functional Safety Methodology

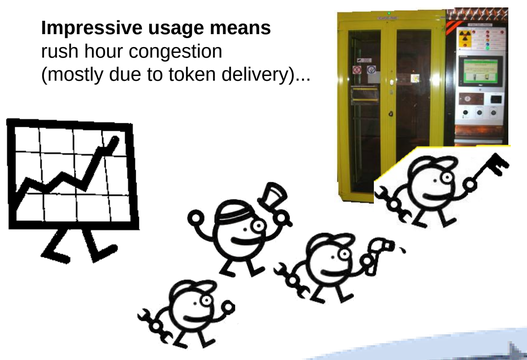
In order to achieve the desired level of safety, the safety systems at CERN are designed using the IEC61508 family of standards as a methodology framework. The IEC61508 uses a probabilistic approach to quantify the risks and to check that a system can cope with the requirements defined for each safety function. To this end it introduces the notion of Safety Integrity Level (SIL), which is a measure of safety. It permits to determine the target level of risk reduction that a safety instrumented system should provide. It is scaled from 1 to 4. The higher the occurrences rate of a hazardous event or the severity of its consequences, the higher the SIL level and the implementation constraints. In order to deal with the functional safety, a project strategy has to take into consideration the following aspects:

- Preliminary Risk Analysis.
- Specification of the Safety Instrumented Functions with their corresponding SIL level, e.g. stopping the beam in case of an intrusion has been evaluated as a SIL3 function.
- Preliminary Safety Study based on the first version of the functional analysis of the architecture.
- Design and implementation of the system based on V-shaped lifecycle model.
- Verification and Validation of the system.
- Organisation of operation and maintenance.
- Definitive Safety Study of the "as built" system, verifying that the SIL of each safety instrumented function has been achieved.

The LHC Experience

Access Statistics – 5 days of Technical Stop (29.08 – 2.09.2011)

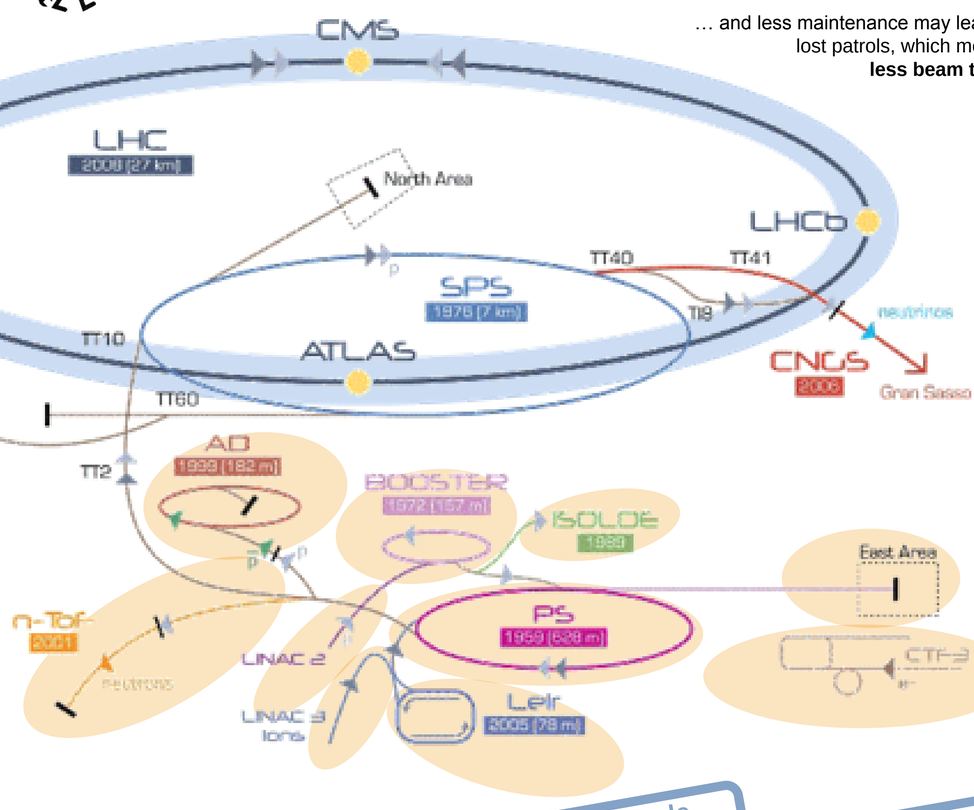
Area	Entry & Exit Passages	Refused Passages	Total
Service Area	5'831	243	6'074
Tunnel Area	1'766	13	1'779
Experimental Area	3'209	55	3'264
Total	10'806	311	**11'117**



Impressive usage means
rush hour congestion
(mostly due to token delivery)...

… but also less time to perform the even more needed maintenance...

… and less maintenance may lead to lost patrols, which means **less beam time.**



The New Concepts

The unexpectedly high usage rate of the LHC Access System in the *restricted* mode has led us to seek ways of improving the system to cope with the high demand. The *restricted* mode is particularly complex as the accesses are supervised by the control room operators, the users are given safety tokens (keys) and the search patrols are preserved in normal conditions. New concepts have been identified and new solutions proposed. They currently start being implemented in the access safety systems of the LHC and its injector chain.

Work Acceptance Tool

Major congestion factor was the relatively long time it took for the operator to verify if an entry request was in relation to a planned maintenance activity. Hence, the introduction of the Work Acceptance Tool (WAT), linking an intervention planning tool and the access control system. During technical stops, the WAT automatically limits access to planned maintenance interventions only.

LHC: in Production

Separation of Token Distribution from PAD Cycle

The delivery of a safety token is integrated with the LHC PAD entry cycle and thus a new token cannot be delivered until the previous person has successfully entered. In the PS, the two actions will be decoupled, with the user first taking the token under the supervision of the operator and then entering the PAD, while the operator can already treat another request.

PS: Specification

LHC: Upgrade Spec

Maintenance Doors

The goal of moving the external envelope to a second line of protection (e.g. the ventilation doors behind the access devices) during beam operation is to provide the maintenance teams the time to do preventive interventions on all surface access points while the accelerator is in beam operation.

PS: Specification

LHC: Modif Done

EMC Improvements

In the LHC, most of the originally installed magnetic door sensors have been recently replaced by more robust electromechanical contacts. These are not affected by the magnetic fields, but need delicate adjustments. For the PS, a thorough campaign of EMC measurements has been done prior to choosing the access equipment locations.

PS: Studies OK

Access Point Controller Rationalization

PAD Control and Safety Synchronisation
A safety action applied in the middle of an access cycle may in some cases result in the LASS briefly registering both the inner and the outer PAD doors opened, which results in a patrol drop. The separation of process control and safety does not preclude synchronisation of the control tasks with the safety actions and the currently designed PS access devices should have one PLC running the two tasks in two processes, with safety having a higher priority, but the control being well synchronised.

Less Controllers in the Access Devices
An LHC access point composed of one PAD and a MAD is equipped with a total of 5 industrial controllers and a PC. The PS personnel safety system architecture will use only 2 controllers and one PC.

Anti-Fraud Detection as a Safety Function
The critical detection of a fraudulent passage in access devices - human presence in a MAD and multiple persons in a PAD - is currently performed by local Industrial controllers. This may lead to the unavailability of the devices in case of failure of one of the controllers. To improve the dependability of these processes it was decided to implement them as new safety instrumented functions of the PS safety system. Moreover, the PS PAD model chosen is more rigid and provides less internal volume making it virtually impossible to fraud.

LHC: Upgrade Studies

PS: Proto 4Q 2011

Removing the EIS-beam from an Interlock Chain

The EIS-beam are surveyed by the LASS permanently. Should they quit their safe state in access mode, the LASS blocks access and, in case of multiple failures, orders evacuation of the LHC. EIS-beam can only undergo maintenance during a complete shutdown of the accelerator complex. This is regulated by a strict procedure. In order to facilitate their disconnection from the system using special "out-of-chain" keys, additional safety functions have been introduced. As long as all the EIS-beam are not connected, the upstream chain interlock will not allow beam operation.

LHC: in Production

New Simba/SIMIT Test Platform

Any modification – a new functionality, addition of an EIS or a scope extension – requires thorough testing of the safety code. To this end each system is accompanied by a test platform. The LASS test platform provided a test-bed for 2 out of 9 LHC sites at a time. The drawbacks of this testing solution are the need for hardware reconfiguration of the I/O modules when changing the simulated LHC sites and a very basic simulator user interface. In the PS, composed of 19 different machines, each with specific configuration, a more versatile test platform is needed to be able to cope with testing of possible extensions. It will be based on Siemens SIMBA module which allows emulation of any I/O configuration without costly hardware reconfiguration and SIMIT software tool facilitating simulation scenarios.

PS: Proto 4Q 2011