ACCESS: LET THEM IN BUT GET THEM OUT ON TIME !

E. Cennini, CERN, Geneva, Switzerland

Abstract

Based on the expected hazards related to the commissioning period and the operation of the LHC, the list of the systems involved in the safety of the LHC will be presented. More specifically the concept of the access control and the machine interlock systems will be briefly presented. A classification of the different constraints associated to the design of the LHC access control and the machine interlock systems will be established and the related consequences, for example on the technical and the operational aspects, will be pointed out. Finally an access scenario will be proposed in order to stress the definition of the user's requirements.

1 INTRODUCTION

The recent documents sent during the drafting of the *Rapport Préliminaire de Sûreté du LHC* (Preliminary Report on the Safety of LHC) [1] to the French authorities responsible for Basic Nuclear Installations have made it possible to re-affirm the access concept employed at CERN, to endorse it and lastly to apply it to LHC. It should be recalled that access to the tunnels and LHC experiment is based on routing through 4 grades of area (Fig. 1) whose inherent risks determine the type of controls instituted.

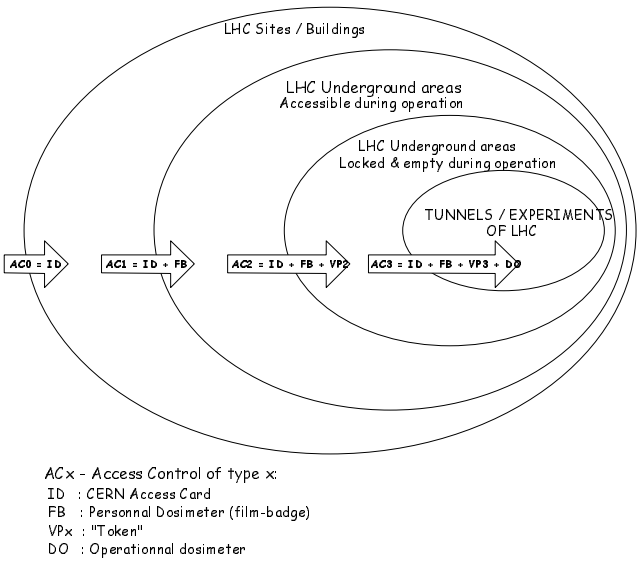

Figure 1: Access to and classification of underground structures in the LHC, the concept.

This document is concerned with aspects of the systems planned for the restricted underground areas of LHC and the tunnels/experiment of LHC, i.e. the safety systems (access control and beam interlock) for the accelerator.

The procedure adopted consists in collecting the intrinsic constraints and defining the performance criteria required for each area identified in this concept. Thus it ends up by specifying the functions required to meet needs. The procedure has been applied to the sites/buildings of LHC and the unrestricted underground areas of LHC. It has resulted, in particular in identifying and setting up traffic islands in the SPS (site access control), individual buildings of the SPS (buildings access control) and earmarking pit-head islands for access to the unrestricted underground areas of LHC.

The aim of this document is to initiate the process for the LHC safety systems. Based on this initial analysis, technical proposals and ways of identifying needs for the Equipment, Control and Supervision layers will be presented and must be submitted for approval by committees responsible for the LHC project (in particular, LHC-TCC and LEMIC).

2 LHC OPERATIONAL MODES

2.1 Main operational modes

The LHC operational modes are listed as follows:

- ***Machine* mode (beams present / machine equipment supplied):**
- Access shall be prohibited and locked in secure position.
- Activation of the emergency entrance/exit system will result in the shutting down of all injected and circulating beams from LHC and in holding them at stop position.
- ***Restricted controlled access or technical stop (no beams / power maintained to certain machines and equipment):***
- The injected and circulating beams shall be shut down and held at stop position but certain of the equipment shall still be under power.
- Access to specific sectors shall be authorised for a limited number of individuals.
- If a locked door to an unauthorised sector is opened (door forced), all the equipment concerned will be put into secure position.

  The duration of a technical stop is set at one hour every 24 hours
- ***Supervised access mode (beams down/machine equipment halted):***

***Short shutdown* mode:**

- The injected and circulating beams shall be shut down and held in secure stop position in the LHC tunnels.
- Access to anywhere in the machine shall be authorised as a function of the inherent risks and take place under the supervision of an operator in the control room.
  The short shutdowns shall be planned to last less than a month.

***Long shutdown* mode:**

- The injected and circulating beams shall be stopped and held at secure stop position.
- Access to anywhere in the machine shall be authorised as a function of the inherent risks and take place either in automatic mode or under the supervision of an operator in a control room.
  A long shutdown shall last approximately three months.

Moreover, when controlled access mode ends, all restricted areas of the LHC will be subject to a close-down inspection patrol.

2.2 Proposed access modes

CLOSED + VETO (access denied)

Applied/removed manually (key) by the radio-protection technicians.

CLOSED

Corresponds to the machine operation mode. The LHC machine is running or is about to start.

TEST

This mode is equivalent to the CLOSED mode but it is applied on specific LHC test areas.

PATROL/SURVEY

This is an access mode with a very restricted Personnel database (radio-protection technicians, patrol teams).

SUPERVISED RESTRICTED

This is an access mode with a restricted Personnel database (e.g. RF people only…).

SUPERVISED

This is the "normal" access mode with the main Personnel database.

CONTROLLED AUTOMATIC

During Long Shutdown, it might be possible (if approved) to access in an automatic mode (without human supervision), in very specific areas (to be defined).

3 IDENTIFICATION AND CLASSIFICATION OF CONSTRAINTS

3.1 Characteristics of users

All persons working for the Organization must possess non-transferable access cards in their own names, issued by the Administrative Services (AS) in accordance with *Operational Circular No. 2* (October 1994) published by the then Personnel Division. As access to LHC underground structures (restricted and unrestricted areas) requires a film badge, these are issued by TIS/RP Group to individuals who have undergone the relevant medical tests and attended the appropriate safety courses. Moreover, the special authorizations for LHC must be issued through the *Authorization Management System - AMS*, by duly appointed CERN officials.

3.2 Organizational constraints

Operational project management

The LHC project uses an operational management project tool [2] broken down organizationally into the following roles (Fig. 2):

- **Client:**

⇨ Product Owner
  - purchases the product,
  - can halt the project at any moment.

⇨ Product Manager
  - identifies the final milestone of the project,
  - is the project director,
  - represents the users of the product to be supplied.

- **Supplier:**

⇨ Project Owner
  - is financially responsible for due completion of the project,
  - he may allocate additional resources to the project after agreement with the Product Owner.

⇨ Project Manager
  - manages the project until completion,
  - is the project leader,
  - represents the contributors and is in regular contact with the Product Manager to ensure that the supplies are those that meet users' needs.

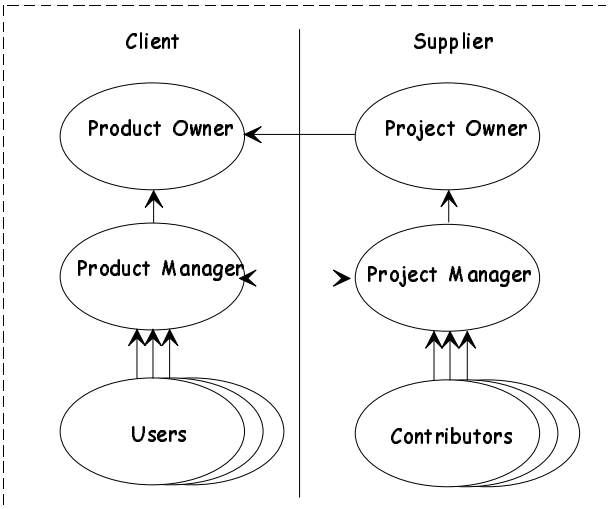

Figure 2: Operational project management.

Organization of the LHC Project

The way the above-mentioned organisational model is applied to the LHC is shown in Figure 3. The responsibility of contributors to the LHC project is shared by all the different divisions in CERN. On the other hand, the various trades and/or technical skills depend on services provided by other divisions (for example: IT, SL-CO, ST-EL , etc.). To that end *LHC Project Engineers* have been appointed to lead what might be called LHC *sub-projects*. It is their task to provide the different equipment, machinery and services necessary for the completion of LHC and to arrange for co-ordination with the CERN services they need to draw on.

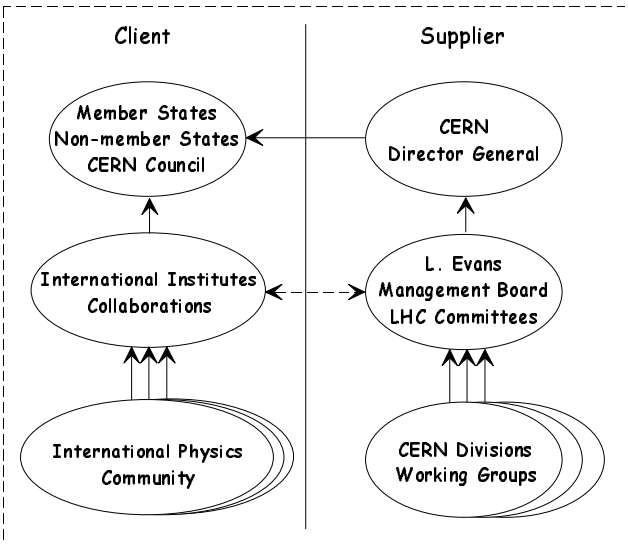

Figure 3: Organization of the LHC project's operational management.

Organizational arrangements for the sub-project providing security systems for LHC

The sub-project to provide security systems for LHC concerns a major part of the LHC project organisation as well as identifying needs associated with access. In fact, if the beam interlock system interfaces are to be defined, the accelerator shut-down scenarios have to be identified. This system must provide equipment safety functions, and so the services and working groups dealing with the accelerator itself are represented as safety system users.

The contributors involved in providing the LHC security systems come from different CERN services and groups such as ST-EL, for supplying power to the systems and for audio-communication networks, IT, for public data communication networks…

Although essential, this project management structure displays certain constraints, *inter alia* for the precise identification of needs. For this reason the security system functions proposed need to undergo successive phases of validation by different committees in the LHC project

3.3 INB constraints

Operation of LHC requires licensing from the French authorities in the person of the *Direction de Sûreté des Installations Nucléaires* (DSIN). Such licensing stems from a convention whereby CERN is committed to providing precise documentation [3].

- ✓ Impact study on SPS, LHC (project launch phase)
- ✓ Preliminary safety report on SPS, LHC (study phase)
- ✓ Interim safety report on SPS, LHC (start of operational phase)
- ✓ Final safety report on SPS, LHC (initial experimental feedback)

The final safety report will be subjected to an expert inspection commissioned by the DSIN from the French *Institut de Protection des Installations Nucléaires* (IPSN) [Institute for the Protection of Nuclear Installations] The conclusions of the inspection and the recommendations deriving therefrom will be presented to a meeting of the *Groupe Permanent Usine des Installations Nucléaires de Bases* (GPU). This latter body will approve, approve subject to reservations or refuse an operating licence. The contribution of the Access Control Section to the INB documentation consists in detailed functional and operational descriptions of the access control and beam interlock systems together with the summary and conclusions of the safety analyses for these systems.

Although from the INB standpoint, the LHC is not comparable with LEP, the recommendations made for the LEP safety systems act as indications and major constraints with regard to LHC systems design:

- redundant signals from the *Eléments Importants de la Sûreté (EIS)* must be sent by physically

independent paths anywhere in the safety system architecture,
- where programmable logic controllers are used in establishing safety systems, they must be self-regulating;
- the accelerator restarts must be preceded by a signal indicating “beams imminent”.

3.4 Operational constraints

Definition of access modes (§ 2) reveals a major constraint in the LHC access control system, namely the absence of a free mode. In plain language this means that the restricted areas of LHC are under constant control (supervision). Corrective and preventive maintenance must be carried out without hindering controlled access to the accelerator. High availability is therefore required at access points.

In machine mode, the safety systems must ensure that all areas can be locked and, in particular that beams can be immediately shut down and stopped from circulating should an emergency door/gateway device be inadvertently activated. High reliability is therefore essential for the specialised safety control systems.

3.5 Environmental constraints

When beams are running, radiological, magnetic, and electromagnetic disturbances, etc. created by the accelerator form non-negligible constraints in protecting the accelerator components. Within the safety systems, these constraints are particularly critical given that breakdowns following alterations set in train by these disturbances will cause the accelerator to shut down and may harm major machine components.

3.6 Assembly constraints

Geographical constraint

As in the case of LEP, the distances to be covered and the number of signals to be sent constitute major constraints, in particular for the architecture of the control network associated with safety through the fact that the safety systems signals must be routed to the interlock system situated in the control room.

Topological constraint

The configuration of the underground structures of LHC and the concentration of *EIS* access points in the straight sections also act as constraints on the architecture of local control systems associated with safety and those associated with operation.

Material constraints

The major constraints governing access facilities stem from the following considerations :

- access by personnel and equipment in bunches (stress peaks on access facilities),
- the volume occupied by the machine in the LHC tunnels and the need to leave a minimum of clearance for lifting vehicles to pass through.
- reliable and sturdy mechanical locking of access gates/doors,
- in machine mode the various disturbances generated by the environment have to be taken into account.

Constraint associated with system design

To minimize any risk of LHC safety systems failure, experience together with analyses of safety factors for LEP systems shows that redundant routing of current looping and positive security signals alone provide the best performances. This characteristic implies that high availability and high reliability automation systems must be used. Back-up power for such systems must also be taken into consideration.

Constraint associated with the installation and testing of machine equipment parts

In the LHC installation planning schedule, a beam injection tests phase has been projected for mid 2004. As a result, temporary safety systems must be set up for the sites and *EIS-machine* in question.

4 IDENTIFICATION AND CLASSIFICATION OF MAIN FUNCTIONS

4.1 Safety systems at LHC: reminder

As noted, the LHC safety systems are as follows :

- The purpose of the *Système de contrôle des EIS-accès (SCEa)* is to control and command any dedicated system/equipment/element/device… (called *EIS-accès*)… used to prevent access in dangerous areas, sectors marking the perimeter limits and restricted areas of the LHC.

- The purpose of the Système de contrôle des EIS-machine (SCEm) is to control and command any dedicated system/equipment/element/device… (called *EIS-machine*) from the machine generating a risk for human life.

- The purpose of the *Système de Gestion et de Configuration de l'Interverrouillage (SGCI)* is to manage and configure all the Safety Chains. A specific set of *EIS-accès* interlocked with their related *EIS-machine* constitute a Safety Chain. Following the operation modes, VETOs (inhibition commands) are generated by the Safety Chains and sent either to the *SCEa* and to the *SCEm.*

4.2 Architecture and main functions of the safety systems

The safety systems architecture has three distinct layers:

- the **Equipment layer** corresponds to the process to be controlled, it is involved with all the *EIS* in the LHC,
- the **Control/Communication** layer covers the procedure's management and control components. For the safety systems, an industrial network based on the use of specific Programmable Logic Controllers is planned.
- the **Supervision layer**, as its name indicates, contains the equipment and communications infrastructure providing for supervision and monitoring of the processes.

Within the different layers, each constituent element of the safety systems fulfils specific dedicated functions with regard to either access control or beam interlock. They are broken down according to the following two main characteristics:

- **safety** ensuring accelerator shut-down in case of inadvertent intrusion and protection of machine components during such emergency stops. Switching on of interlock commands for one of the safety systems to another must be automatic and highly reliable (fail-safe, redundancy, etc.),
- the operation of the access control system during machine shut downs to supervise access procedures. The fact that there is no free mode for LHC implies that access functions and equipment must have a high degree of **availability**, in particular during technical stops (1 hour of access every 24 hours).

4.3 Functions associated with the Equipment layer

The LHC *EIS-accès* functions are mainly as follows, the detailed breakdown for them to be laid out under the technical specification for the safety systems.

- barrier for personnel and material access to different areas and sectors of restricted areas of the LHC,
- locking and unlocking in line with the access procedure associated with the access mode applied,
- emergency entrance and exit using a mechanical system,
- validation/verification that the shutdown patrol has made its inspection,
- accounting for persons gaining access and guarantee that the *EIS-machine* cannot be activated (token).

The safety signals

Signalling of an EIS state is defined by :

Safe position:

simultaneous display of *SAFE* and $\overline{UNSAFE}$ safety signals,

Unsafe position:

simultaneous display of $\overline{SAFE}$ and *UNSAFE* safety signals,

These paths are picked up by microswitches or independent contacts placed and activated directly by the position that a given component is in.

An *EIS* is locked by a command or priority inhibition path of the *VETO* type generated by the control/command organs of the component to keep it in safe position. This command is initiated by default irrespective of the access mode, and is inhibited during access procedures.

Routing of safety signals

Safety signals are connected by direct cables routed down two separate physical paths towards the interface modules with the control network. The distances travelled (straight sections of the accelerator to shaft heads) require signal relays. At the repeaters, an abbreviated display of the signal states in transit is also required.

Signals acquisition interface with the next highest layer

The acquisition of safety signals at site level is done by means of cabled logic modules designed to provide an interface with the local concentrator logic controllers. The functions of the input and interface modules and crates are as follows:

- relaying (upwards) and interface of signals for both safe and unsafe positions,
- relaying (downwards) of the various locking and closing-off commands,

- signaling the above-mentioned signal states and commands.

4.4 Functions associated with the Control/Communication layer

Spheres of use of automation systems

The features of the safety systems listed in § 4.2 themselves give the spheres of use for the PLC's that are to be installed. In this way, the automation systems ***1 on 2*** and ***2 on 2*** (c.f. Fig. 4) can be identified. Switching between them is accompanied by additional measures but the compatibility of the hardware and software for programming the controllers is ensured.

Functions associated with the Control/Communications layer dedicated to safety

4.4.1 Acquisition and processing of safety signals

The site concentration PLC's (2 on 2 system) used for access control and beam interlock have the following main functions:

- acquisition and reporting of safety signals,
- organization of signals for developing the main interlocking , local and test runs,
- setting up interlocks for local and test run chains,
- generation of site results for use by the central interlock system.

4.4.2 Routing of safety results

The results produced in this way must be routed via two independent physical paths to the LHC site concentrators affected by the *local* and *test* interlock chains as well as to the main interlock system. The distances to be covered (curved sections, distances between sites) require the same functions as those described in § 4.3.

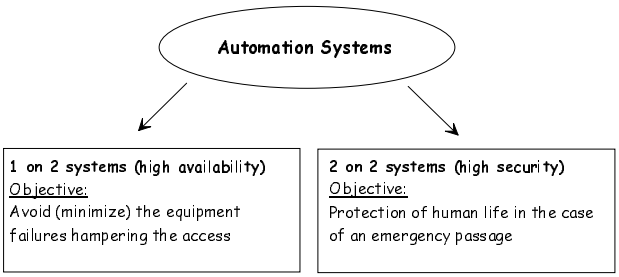

Figure 4: Field of use of automation systems.

4.4.3 Result acquisition interface

Result acquisition takes place at the main control room by means of cabled logic modules providing an interface with the central concentrator PLC's. The functions of the acquisition and interface modules and crates are as follows:

- relaying (upwards) and interface of both safe and unsafe results,
- relaying (downwards) of the various interlock commands,
- signaling the above-mentioned result states and commands.

4.4.4 Acquisition and processing of results

The central concentrator PLC's (2 on 2 system) in the access control and beam interlock systems have the following main functions:

- acquisition and signaling of safety results,
- organization of signals for developing the main locking, local and test chains,
- setting up interlocks for main, local and test chains,
- generating global results for use by the central interlock system

4.4.5 The interlock system

The main functions fulfilled by the interlock system are stated hereunder:

- Accounting for the position of the central security keys and management of transitions between the *SCEa* and *SCEm* systems,
- key release commands and manual activation /inhibition commands for VETO signals,
- accounting for the position of dedicated central safety keys for use in testing equipment and test clearance management,
- automatic generation of different locking commands implicit in safety systems.

All the different communications in the Control /Communication layer dedicated to safety are made using a cabled logic based on current loops (de-)activated by the safety PLC's.

Functions associated with the Control/Communications layer dedicated to operations

4.4.6 Management and control of *the main access points*

The main LHC access points differ depending on whether they are concerned with access to the machine or to the experimental caverns. The distinction resides simply in the fact that the access points to the experiment are fitted with tokens given their position within an unrestricted area of LHC. The other access points are considered as forming part of the machine test area and hence also govern all the *EIS* in the given area.

The principal functions of AC3 systems are summarized hereunder:

- access barriers to test areas in machine operation mode,
- access barriers to areas during tests,
- emergency exits/entrances using a mechanical system in case of evacuation,
- checking whether a film badge is held,
- issue of a personal interlocking device (solely for access to experiment),
- checking whether there is a functioning dosimeter,
- accounting for numbers of persons with access to the area.

The need for high availability in the utilisation of the access points implies the use of Type 1 on 2 automation systems. The systems peripheral to those described above are listed as follows :

Functions associated with management of an access point:

- updating of on-line data bases relating to personnel with access rights,
- provision of a back-up data base in case the main communication network fails,
- communication with the site concentrator PLC's (condition read-out).

Functions for the user interface

- test area panel display,
- signaling of access modes applied,
- list of names of persons issued with tokens,
- on-line description of access procedure.

Functions associated with maintenance of an access point:

- local record of past events,
- by-passing of access point for preventive and corrective maintenance work.

4.4.7 Management and control of *pits-head access points*

As noted, such controlled access systems are the access points to the restricted machine-dedicated areas. The system's functions are summarized hereunder:

- access barriers to restricted areas in machine operation mode,
- emergency exits/entrances using mechanical systems for evacuation

for operational access modes:

- verification of film badge possession,
- issuing a personal key system,
- accounting for persons with access to underground structures.

The need for high availability in operating the access control system implies the use of Type 1 on 2 automation systems. Functions peripheral to those described above are as follows :

Functions associated with management of an access point

- updating of on-line data bases for personnel with access rights,
- provision of a back-up data base in case of outages on main communication networks,
- communication with the site concentrator PLC's (condition read-outs).

Functions for the user interface

- panel display of local situations (signalling of all on-site ISC states)
- signalling of access modes applied ,
- list (giving names) of tokens issued,
- on-line description of access procedure.

Functions associated with maintenance of an access point

- local record of past events,
- by-passing of access point for preventive and corrective maintenance work.

4.4.8 Routing of communications and SCADA

The LHC's high volume communication networks are at present being defined. The Communication Infrastructure Working Group - CIWG is in charge of compiling the needs of the different services. To operate the safety systems it has been requested that a high-availability network be made available with communication channel switch-over in case of power failure. For accelerator safety purposes, a private network should be specified.

Likewise, the dedicated SCADA for use in operating LHC safety systems will be identified and specified

through the studies and recommendations made by ST-MO Group.

4.5 Functions associated with the Supervision layer

Supervision of the LHC safety systems from the main control room or possibly from other control rooms requires the following main functions, depending on the operational mode:

In *machine* mode

Functions associated with the management of safety systems:

- updating and display of on-line data bases relating to personnel with access rights,
- consultation and individual checking of access authorizations,
- communication with central concentrator PLC's (condition read-outs).

Functions for the operator interface

- detailed display of general and local panels (signaling of all LHC *EIS* states)
- general and individual display of situations associated with interlock chains installed (interlock system),
- video selection and acquisition of all LHC controlled access systems,
- automatic audio selection and communication with displayed access points.

Functions associated with the maintenance of safety systems:

- records of past events,
- generation and monitoring of technical alarms,
- help in diagnostics.

For *access* modes

Above functions, plus

Functions for operating the access control system:

- application and management of access modes,
- commands dedicated to access procedures,
- signalling and state of decentralized supervision systems,
- on-line help for access procedures.

5. SCENARIO FOR ACCESS TO THE LHC MACHINE

In access mode, an authorized person wishing to enter the LHC tunnel will be subject to the following main controls:

Entry to site # and to Building SD# will be gained by reading the person's CERN magnetic card, checking the authorization will activate the access control systems (road islands and buildings).

Inside Building SD is the pits-head access point, denoting and controlling access to restricted areas. Under the supervision of an operator he/she will go through the entry procedure.

Within the restricted area (Shaft PM), caverns and service galleries in the tunnel), the individual may move around freely and pass through any other sector barriers/doors encountered.

Access to the main tunnel or the test area will be governed by an unique access point.

6. CONCLUSIONS

The introduction of safety systems for the LHC involves taking into account a large number of characteristics associated with the accelerator's operation and above all, the safety of personnel and equipment. These characteristics require the introduction of reliable functions that take the different constraints into account. As the human element is the weakest link in a safety system, it is essential for technical architecture to be designed that can take account of the constraints inherent in the environment and operation of an accelerator like the LHC. At the same time, if too much stress is placed on removing the constraints, the performances really required run the risk of being changed. Thus, the discipline of the users and operators of the LHC has to be achieved through simple instructions that will make the safety systems work most effectively.