ACCESS SAFETY SYSTEMS – NEW CONCEPTS FROM THE LHC EXPERIENCE

T. Ladzinski, Ch. Delamare, S. di Luca, T. Hakulinen, L. Hammouti, F. Havart, J-F. Juget, P. Ninin, R. Nunes, T. Riesco, E. Sanchez-Corral Mena, F. Valentini, CERN, Geneva, Switzerland

Abstract

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.

INTRODUCTION

The access safety system is a vital component of every accelerator facility without which beams cannot be injected and accelerated in a machine. Its principal duty is to ensure that if there is beam in the machine no human being is inside, and if there is a human inside that no beam can be injected.

The Large Hadron Collider access system was put in operation in 2008 following one year of gradual commissioning. It introduced new concepts and safety levels, which were not present in the earlier accelerators at CERN. Within the activities of the LHC injector chain upgrade, the injector complex access safety systems are also being overhauled. Our team is currently involved in the renovation of the Proton Synchrotron (PS) personnel safety system and plans are underway to start the upgrade of the access and safety system of the Super Proton Synchrotron (SPS). These activities should bring the level of safety of the corresponding access systems at least to the level of the LHC system and provide the so much sought after harmonisation of equipment and user experience over the entire accelerator complex of CERN.

SAFETY PROJECT ASPECTS

An access safety system is a complex interlock mechanism acquiring the status of, and acting on, hundreds of Elements Important for Safety (EIS) [1]. We distinguish between EIS-access and EIS-beam. The EIS-access consist of the personnel and material access devices, doors, moveable shielding walls etc. The EIS-beam are accelerator components that can stop the circulation and the injection of beams. The choice of EIS-beam allows redundancy for each interlock chain with technological diversity (e.g. a bending magnet and a moving stopper obstructing the beam aperture). The number of individual components under the responsibility of various organisational units with different approaches to safety provides additional challenges to the overall safety system design and project coordination activities.

In order to achieve the desired level of safety, the safety systems at CERN are designed using the IEC61508 [2] 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 allows 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 occurrence 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 aspects, a project strategy has to take into consideration the following aspects [3]:

- 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.

A vital organizational aspect of a safety project is the independence of teams conducting various project steps. This is often achieved by outsourcing the development tasks to external companies. The CERN team participates in the specification and verification phases, the actual implementation is done by a specialized contractor meeting the tender process requirements. The final validation that the system fulfils its mission is done by yet another independent body – the Departmental Safety Officer of the Beams Department conducts an independent test before permitting any beam operation. In addition, throughout the project lifecycle independent consultants are hired to conduct the safety studies and evaluate the SIL level achieved.

THE LHC ACCESS SAFETY SYSTEM ARCHITECTURE PRINCIPLES

Control and Safety Separation

Following the principle of strict separation of the functional safety part from the process control part, the LHC access system is made up of the LHC Access Control System (LACS) and the LHC Access Safety System (LASS) [4].

The role of the LACS is to provide a physical barrier enclosing the LHC accelerator and dividing it into clearly delimited sectors, and to identify the person and verify his or her access authorisations. The LACS controls the access equipment and provides audio and video links between the control room and the field.

The LASS is an interlock system ensuring that no beam can circulate or be injected in case of access operation and that every intrusion detected during the beam operation leads to an immediate stop of the accelerator in a controlled manner. Its EIS-access comprise 40 personnel and 29 material access devices, 203 doors dividing the underground areas into 82 sectors, 17 mobile shielding walls etc. The EIS-beam which can, in parallel to the LHC beam dump system, stop any circulating beams and any injection of new beams are: the mobile beam dumps, horizontal dipole chains and injection septa in the two transfer lines from the SPS to the LHC, the separation magnets in the two collimator regions of the LHC and two reinforced vacuum valves.

The division into two distinct systems allows the use of different hardware, software and testing solutions, each more suited for the specific needs of the subsystem.

Two Channel System

The LASS control system has a distributed architecture and uses the Siemens 417FH Programmable Logic Controllers (PLC). At each of the LHC points a local controller monitors the state of all the EIS of that point and calculates the site resultants which are transmitted to the global controller. The global controller acquires the information obtained from each of the local units and takes the necessary safety actions, calculating a global resultant to enable or disable the global access safety veto. The controller units are linked via a dedicated redundant fibre network routed in the LHC tunnel.

This architecture has been complemented with a relay logic cable loop that provides a technologically redundant logic mechanism to stop the beams in case of an intrusion via the external envelope of the accelerator. In this way, not only the sensors and actuators are provided with sufficient redundancy, but also the central system logic. This goes beyond the commonly used architectures, where a SIL3 system is composed of redundant sensors and actuators and a SIL3 certified logic controller (which is internally redundant providing two execution channels for the safety program). However, the total response time of a system based solely on the PLCs might exceed the needs of the process, as a distributed architecture relies on numerous timeouts before driving the system into a failsafe state in case of a safe failure. Moreover, the IEC61513 standard, a nuclear sector extension of the IEC61508, recommends diversity of means to achieve the safety objectives and thus to minimise a common cause of failure. This is where the simple relay logic steps in.

In the case of the LHC, the relay logic was added to protect the risk of intrusion. For the PS complex this concept has further been expanded to provide redundant logic mechanism that acts also in case of a momentarily lost safe state of an EIS-beam. Contrary to the LHC, which in fact is one accelerator, the PS is divided into several machines with transfer lines providing beam from one to another. In case of a problem with an EIS-beam in one machine, the interlock system immediately acts on the EIS-beams of the upstream accelerator.

External Envelope Inviolability

In a long shutdown period anyone authorised can enter the accelerator. Once this period is finished, all the machine interlocked areas are patrolled to make sure that nobody was left behind. As this process is long, the machines are subdivided into access sectors, each having a binary memory called “search”. The search is armed at the end of a patrol and disarmed only in case of intrusion or an entry in the shutdown period. During beam operation period, short technical stops are often necessary to allow accesses for corrective maintenance interventions. The technicians entering the interlocked zones are not protected by the collective search/patrol mechanism, but instead are given personal protection tokens. As long as all the tokens are not restored, the interlock system will not allow beam operation. This safety concept functions correctly provided there is no possibility of entering the interlocked areas without a token. Hence, the EIS-access of the accelerator external envelope must form an inviolable barrier. In the pre-LHC machines this was achieved by means of video surveillance by the control room operators. The sheer size of the LHC and the number of concerned personnel entering the interlocked areas has put the efficiency of such a solution in question. The external envelope has therefore been equipped with access devices or door-booths, which operate on the same principle as an air-lock chamber. They are small volumes closed at each end with doors, of which only one can open at a time.

In addition to its volume, which is only large enough to accommodate one person, the Personnel Access Device (PAD) is equipped with a complex automatic system based on ground pressure sensors, infrared radar and photo-electric cells surveying the interior at each passage to eliminate piggybacking and tailgating. Furthermore, the usage of a PAD enhances security making it impossible to trespass the interlocked area. Iris biometric recognition system inside each PAD verifies a match between the access badge used and the identity of the access requester. The access control system, in turn, verifies the person's access authorisations and their validity, and checks the status of the periodic obligatory safety trainings and tests.

The Material Access Device (MAD) is also a door-booth, but of much bigger volume, and allows the introduction of bulky material into the interlocked zones. Each MAD is equipped with a human presence detection system. It comprises infrared barriers close to the doors, two volumetric consumer-off-the-shelf detectors and a motion detection system with a millimetre resolution developed at CERN. The later uses a high resolution digital camera (3M pixels) capable of covering the whole MAD volume (approx. 20m3) and a custom algorithm. By analyzing the digital video frames in real time it estimates precisely the quantity of motion inside the MAD on the basis of small luminosity variations in the frame's pixels. A special analysis of any mutated pixels allows discriminating the real movement from the background noise inherent to all digital images.

LHC EXPERIENCE & NEW CONCEPTS

Usability

The LHC access system was built to a higher degree of safety than its predecessors, but the overall ergonomics has not seen major changes with the exception of the introduction of the door-booths. With the explanations on the use of the devices becoming part of the mandatory safety training, the usability problems have decreased and only sporadically users are rejected e.g. because their backpack obstructs the photo-electric cells in the PAD.

Work Acceptance Tool

Passing through a door-booth requires more time than using a door and this fact combined with the extremely high usage rates during the technical stops (see Table 1) may lead to occasional congestion at the access points.

Table 1: LHC Access Statistics from a 5 Day Long Technical Stop (29.08.2011 – 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**

Analysis has shown that the 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. This was largely resolved with 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.

Separation of Token Distribution from PAD Cycle

The LHC access system seldom uses the shutdown access mode ("general" in the LHC terminology), as the day-time maintenance is often interweaved with night-time testing activities requiring the interlocked areas to be patrolled and free of personnel. Hence, in most cases the person entering is in possession of a safety token to preserve the sector search. The delivery of a safety token is integrated with the 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.

Maintainability

Maintenance has always been an issue for the access systems as they are required 24 hours a day, 7 days a week; when the accelerator is operating with beam and even more so, when it is in access mode.

Maintenance Doors

Traditionally, the accelerators at CERN had been operated in annual cycles of 7 to 8 months of beam followed by 4 to 5 months of maintenance shutdown. In LHC the long superconductive magnet warming and cooling time has led to a change in the operation calendar strategy with the introduction of short annual shutdown periods and a long shutdown once every few years when the magnets are being repaired. The annual maintenance periods have thus become much shorter making it very difficult to perform the necessary maintenance and verifications activities, especially of the complex access devices of the external envelope. This has resulted in ongoing studies with 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, thus providing the maintenance teams the time to do preventive interventions on all surface access points while the accelerator is in beam operation.

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 interlocked areas. 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 recently introduced. As long as all the EIS-beam are not connected, the upstream chain interlock will not allow beam operation.

Extensibility

An extension of an existing safety system requires the same rigorous approach as the original development project. This strictness filters non-justified *ad hoc* demands and preserves the safety integrity of the system. Until now one major extension has been identified for the LHC access system. It concerns extending the scope of the system not only to cover the radiation hazards, but also risks related to a major helium release in the tunnel and an upgrade is planned for the first long shutdown.

New SIMBA/SIMIT Test Platform

Any change, whether an addition of one EIS or a big extension requires a big testing effort. The LASS test platform [5] provides a test-bed for 2 out of 9 LHC sites at a time. The drawbacks of this test platform 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.

Reliability and Availability

During the past three years of LHC operation, the access interlock has only once caused a spurious beam dump and has been available all the time. The LASS has reacted correctly on all occasions and the safety of the personnel has never been compromised. However, the availability of the LHC for physics has been slightly affected by several spurious sector search drops in access mode, resulting in lengthy patrols. There is no single explanation to the origin of the lost patrols, but they can be attributed to one of the following origins:

- electromagnetic compatibility (EMC) issues;
- lack of synchronisation between control and safety;
- data exchanges between the access point controllers.

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.

PAD Control and Safety Synchronisation

In the rest position the LHC PAD inner doors are open. Hence, a safety action applied in the middle of a PAD entrance cycle may in some cases result in the LASS briefly registering both the inner and outer 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.

Simplified Access Point Control Architecture

An LHC access point composed of one PAD and a MAD is equipped with a total of 5 industrial controllers and a PC which adds to the above mentioned synchronisation issues all the problems of communication between the tasks running in the different controllers. The PS personnel safety system architecture will use only 2 controllers and one PC, as the architecture chosen supports process level integration and not integration of many consumer-off-the-shelf solutions.

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 several local 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 provides less internal volume making it virtually impossible to fraud.

CONCLUSIONS

The LHC Access System has been in production since early January 2008. The past four years have shown that it has met the desired safety integrity level, thus confirming both the project organisation and the design choices.

In this paper the IEC61508 based methodology used in the project lifecycle phase was presented as well as the important technical principles of the LHC access system. The experience gathered during the operation and maintenance phase was further discussed focusing mostly on improving the system in order to reduce accelerator downtime resulting from access related issues. New concepts have been identified and discussed. They currently start being introduced in the access safety systems of the LHC and its injector chain.

REFERENCES

[1] International Standard IEC 61513 "Nuclear Power plants – Instrumentation and control for systems important to safety", IEC, 2001-03. The term EIS originates from the French *Elément Important pour la Sûreté* used in this standard. Its English equivalent - Item Important to Safety - is not in use at CERN

[2] International Standard IEC61508 "Functional safety of electrical / electronic / programmable electronic safety-related systems", IEC, 1998, 2000

[3] P. Ninin "IEC61508 Experience for the Development of the LHC Functional Safety Systems and Future Perspective", ICALEPCS'09, Kobe, October 2009

[4] T. Ladzinski *et al.*, "The LHC Access System", ICALEPCS'09, Kobe, October 2009

[5] F. Valentini *et al.*, "Safety Testing for LHC Access System", EPAC'08, Genoa, June 2008