REFURBISHING OF THE CERN PS COMPLEX PERSONNEL PROTECTION SYSTEM

P. Ninin, D. Chapuis, F. Chapuis, C. Delamare, J.- L. Duran Lopez, S. Di Luca, T. Hakulinen, L. Hammouti, J.-F. Juget, T. Ladzinski, B. Morand, M. Munoz Codoceo, E. Sanchez-Corral Mena, F. Schmitt, G. Smith, R. Steerenberg, F. Valentini,
CERN, Geneva, Switzerland

Abstract

In 2010, the refurbishment of the Personnel Protection System of the CERN Proton Synchrotron (PS) primary beam areas started. This large scale project was motivated by the obsolescence of the existing system and the objective of rationalizing the personnel protection systems across the accelerator complexes at CERN to meet the latest recommendations of the regulatory bodies of the host states. A new generation of access points providing biometric identification, authorization and co-activity clearance, reinforced passage check, and other radioprotection related functionality will allow access to the radiological areas. Using a distributed fail-safe PLC architecture and a diversely redundant logic chain, the cascaded PS Access Safety System guarantees the personnel safety in the 17 machine zones of the PS complex by acting on the important safety elements of each zone and on the adjacent upstream ones. It covers radiological and activated air hazards from circulating beams as well as laser and electrical hazards. This paper summarizes the functionalities provided, the new concepts introduced, and the functional safety methodology followed to deal with the renovation of this 50 year old facility.

INTRODUCTION

The Proton Synchrotron (PS) is the backbone of CERN's accelerator complex, accelerating particles to 26 GeV/c. The PS is part of the Large Hadron Collider injection chain. As represented in Figure 1, the PS accelerator complex is made of several machines, some of which can work independently and have specific operation modes.

The project deals with the design, realization, integration, installation, test, commissioning and transfer to operation and maintenance of the Personnel Protection System of the Proton Synchrotron (PS) complex of particle accelerators. The PS Personnel Protection System (PS-PPS) is a regulatory requirement and is essential for the protection of personnel working in the PS accelerator complex mainly against radiation hazards.

The system interfaces numerous Elements Important for Safety (EIS) of the PS machine and will gradually replace the existing access system during the CERN 2013-2014 Long Shutdown. It will be fully operational in the spring 2014 when the LHC injectors will be restarted.

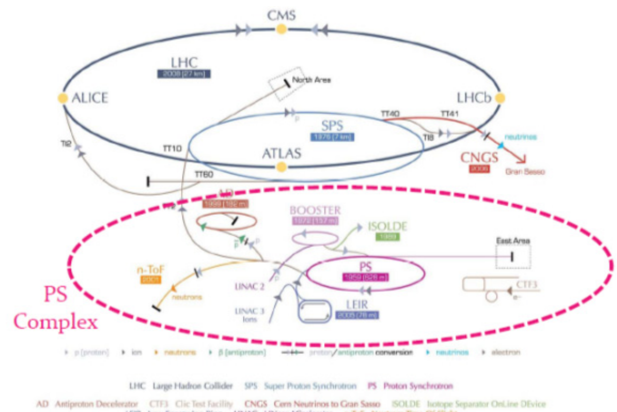

Figure 1: CERN Accelerator complex.

MOTIVATION

The present access system, which supervises the 17 different zones, has followed the evolution of the PS as much as possible, but has now reached a point where a thorough renovation is necessary to cope with the new needs of operation and legislation applicable to this type of facility, assimilated to an "Installation Nucléaire de Base" (INB) that could be translated to "Primary Nuclear Facility".

The PS-PPS will protect personnel from radiological dangers at all times in the radiation-controlled access zones of the PS accelerator complex. Moreover, some additional hazards such as those related to the use of lasers or unprotected high-voltage equipment are covered in specific areas. A Preliminary Risk Assessment of each zone has been carried out, leading to the definition of the required safety functions and their associated Safety Integrity Level that will protect the persons against all the identified hazards.

The PS-PPS will be composed of two complementary subsystems, the PS Access Control System (PACS) and the PS Access Safety System (PASS). The PACS equipment will be installed in all the PS access points and in areas around the PS machines and experiments. The PACS will ensure a physical barrier and will control access by means of automatic or remotely controlled security gates for personnel and material.

On the other hand, the objective of the PASS is to ensure that at any time and in every operation mode of the various machines, the PS complex is safe for the machine users. In Access mode, all the EIS of the accelerators are maintained in a safe state. In Beam mode, any intrusion

ISBN 978-3-95450-139-7

within the PS complex will immediately interlock the EIS of the machine where the incident occurred and the EIS of the up-stream machine, to protect personnel from exposure to the radiation. To complete this mission, the PASS acquires on-line information from the Access and Beam EIS.

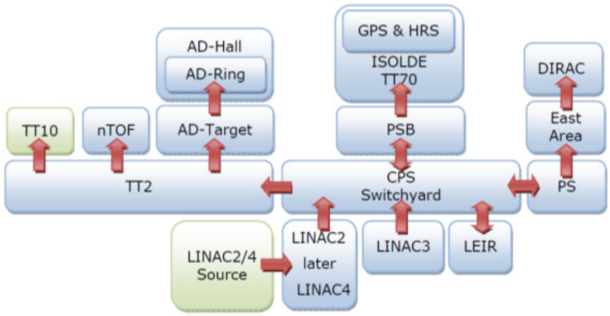

Figure 2: PS complex accelerator zones and beam paths.

The project covers the refurbishment of 17 accelerator zones shown in Figure 2, the control of 141 interlocked doors and access points and 180 Beam and Machines EIS.

SYSTEM DESIGN

PS Access Control System

Using Personnel Access Device (PAD) and Material Access Device (MAD), the PACS ensures automatic or remote control of access to the primary beam areas of the PS complex. At the access point level, it identifies, authenticates and verifies the user's authorizations by means of a Biometric Iris Reader and an interface with the CERN Human Resources Databases.

Figure 3: User at the new PS access point.

As shown in the Figures 3 and 4; each access point is composed of the following elements: a PAD, a MAD, one PACS electrical cabinet hosting also the public address amplifiers, one PASS electrical cabinet including a mini-MAD, one emergency door and one maintenance door.

The system is designed to provide the specific functions of the two main operation modes: "BEAM" or "ACCESS". In the latter, we distinguish several system behaviours: "General Access" where an access point runs without operator supervision, "Special Permit" used for EIS test purposes, "Patrol" and "Restricted Access" to deal with short accesses.

In Restricted Access mode the machine operators remotely operate the access points using a dedicated Human Machine Interface (HMI) with integrated audio and video capabilities. In this mode, as no patrol of the zone will be done before moving back to the Beam mode, safety tokens are delivered to each user entering the primary beam areas. The Beam mode is only allowed when all the safety tokens are back in their safety racks.

Using the public address system, the operator or the system automatically, broadcasts safety messages in each machine zone. This functionality is particularly useful at the end of the access period.

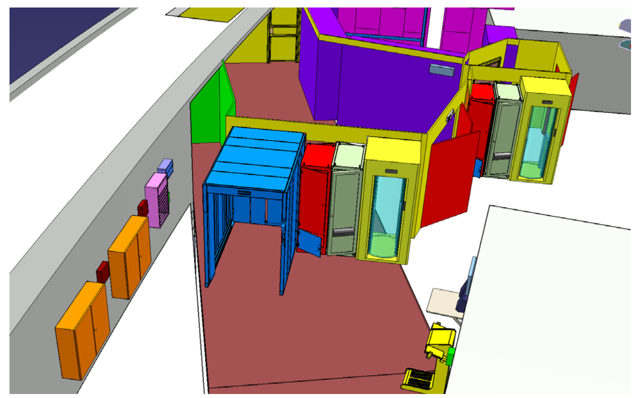

Figure 4: 3D model of the Ntof access points.

The biggest challenge in designing an access point is certainly the integration of numerous heterogeneous components such as a PLC to control the logic of the access point and to acquire the safety signals of the PASS, the access control Front-End to deal with the real-time authorization management, the Biometry for authentication of the user, the Video for remote visualization of the access points, the Public Address system for broadcasting of audio messages, an Interphone system for communication between the Machine operators and the users of the access points, and the display of HMI necessary to the different user categories. Located in the vicinity of the access point is also the radiation protection equipment, such as an active dosimeter reader or a hand-foot monitor [1].

At the access point level, a particular effort has been done to minimize the number of CPUs that need to exchange information with each other. In this context a new type of device, the Siemens Microbox, ensures the dual functionality of a PC managing the access point data processing and a PLC managing the logic of the access sequence.

PS Access Safety System

The mission of the PASS is to ensure that at any time each accelerator zone is safe for personnel. As each zone is operated individually, the safety of personnel shall be

ISBN 978-3-95450-139-7

ensured at all times whether there are beams or not. The principles of the basic interlocking are:

- in access mode: no beam in the zone;
- in beam mode: no personnel in the zone and the beam shall be stopped immediately in case of an intrusion.

In order to implement its safety functions, the PASS is interfaced with several external systems such as ventilation, beam imminent warning, emergency stops, radiation monitoring system, etc. As shown in Figures 5 and 6, the PASS consists of two diversely redundant interlock systems, designed according to the functional safety principles of the IEC 61513 and IEC 61511 standards:

- a PLC channel based on Siemens S7 PLC architecture,
- a hard-wired channel based on relay logic.

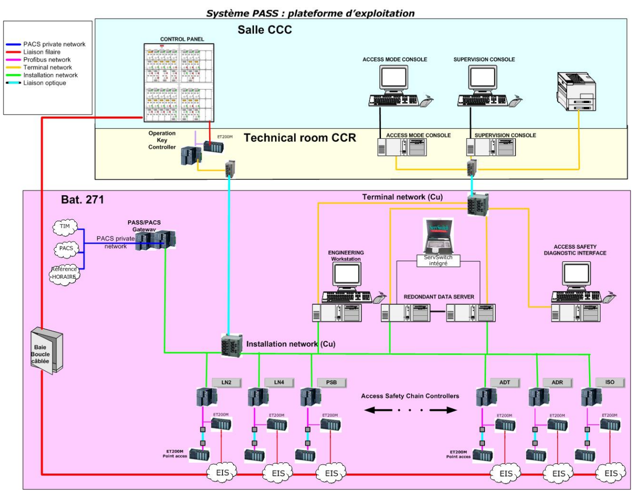

Figure 5: PASS PLC based interlock system.

The PLC channel consists of Siemens S7-400 F PLC. Based on experience from the LHC Access System, where most of the failures appeared in the hot-swappable redundancy mechanism, it has been decided to use a non-redundant PLC, complemented by an external mechanism to memorize the status of the patrol of each zone, avoiding unnecessary patrol and staff exposure to radiation.

A new functionality has also been introduced to allow maintenance of the access point in beam mode. This functionality allows the withdrawal of an access point from an interlock chain by transferring its function to the maintenance door located upstream of the access point.

In the first stage of the design of the redundant path, a PLC based solution was studied, but later discarded, as it was difficult to demonstrate to the Nuclear Regulatory body that no Common Mode of Failure exists in the underlying IT technology.

The PASS is structured on an "installation network" to which all the zone controllers, engineering workstations and PCS7 servers are connected. The latter are also connected to the terminal network used for remote operation.

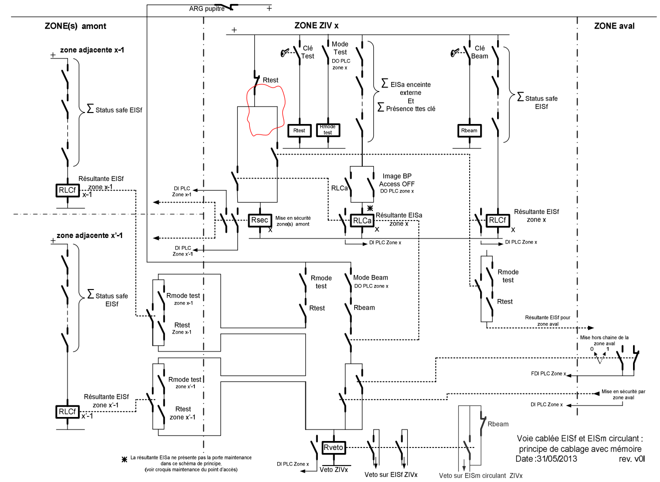

Figure 6: PASS hardwired redundant interlock system.

Implementation

The implementation has been organized in two stages. The first one deals with the design of the system and the setup of a PASS and PACS test platform, allowing simultaneous testing of three adjacent cascaded zones. The objective was mainly the validation of the technical solutions as well as the reliability and safety testing of the system. The second stage deals with the development and installation of the complete control and safety infrastructure deployed in the CERN Control Center and the deployment of the access and safety system on each zone. All installed equipment and software are tested and validated on the test platform prior to their on-site installation.

In addition, the project also deals with civil engineering, power supplies, cabling of the long distance copper cables and optical fibers, networking, renovation of doors, locksmithing, radiation shielding and area renovation.

IT Architecture

The PS-PSS is conceptually divided into four layers. Human-Machine Interface layer provides the operators with the necessary functionality to manage user access as well as the engineering workstations and the diagnostic tools [3]. The Remote Control layer hosts the servers of the various subsystems and interfaces. The Local Control layer hosts the access point control CPU and the PASS zone safety controllers. The Equipment Layer controls all the Access or Beam EIS. As described in Reference [2], all the PACS servers have been virtualized on a robust and redundant standard hardware allowing simplified system administration, optimized backing-up and system snapshotting. As shown in Figure 7, it has been decided for safety and maintenance reasons to use two dedicated private networks: one for the PACS data and one for the PASS data. The networks are isolated from the external world by a dedicated gateway that allows only interfacing to the Human Resources Database and the synchronization of time. In the electrical cabinet of each

ISBN 978-3-95450-139-7

access point, a dedicated network switch ensures the interface between the PACS network and the equipment of the access point: a biometry Iris Reader, a PACS controller that hosts the virtual PLC and local WinCC SCADA, access control Front-End that manages the authorization distribution as well as video and public address equipment.

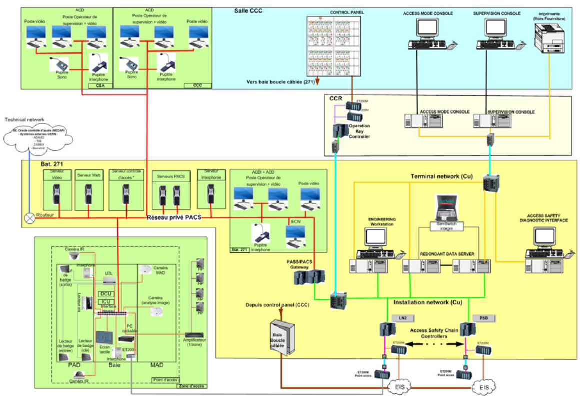

Figure 7: PACS and PASS integrated architecture.

At the CCC desk, operators use three types of HMI; the first HMI is a hardwired console allowing selection of Beam or Access mode of each machine, the second HMI based on Siemens PCS7 architecture allows controlling each machine zone, and the third HMI based on Siemens WinCC and Omnicast offers all the necessary functionality to manage each access point. Omnicast from Genetec is used as the video management system to survey the 27 access points. The other users use the PCS7 and WinCC HMI.

Considering the great number of heterogeneous CPU and equipment distributed amongst the 17 zones, a special effort has been made with the integrated remote monitoring of all these devices. To face this challenge, a diagnostic tool based on an open source framework for monitoring of networks and applications, SSM, has been set up to monitor the performance of each device connected to the networks [2]. Nevertheless, it must be noted that an ergonomic integration of the diagnostic features of all the off-the-shelf components of the system remains a challenging project.

Functional Safety Perspective

This project has been conducted along the same methodological lines as the LHC Access System that was approved in 2008 by the French Nuclear Regulatory body. The selected functional safety standards were IEC 61511 for the Process Industry sector, used for the development lifecycle of the project, and IEC 61513, applicable to nuclear power plants, particularly useful for the specific prescription for the realization of the system; as common cause of failure, diversity, and robustness to external hazards. The main steps of the methodology can be summarized as follows: a Preliminary Risk Assessment of each zone was conducted to determine the safety objectives of the system, allowing in a second stage the definition of the safety functions and the allocation of their Safety Integrity Level. A preliminary safety study based on the first version of the architecture allowed verifying the achieved SIL level of each function. Design and realization of the system are based on the V lifecycle tailored to the functional safety context [4][6]. Particularly important are the final stages of the methodology related to the verification and validation of the system, the final safety study based on the "as-built" system, the documentation and the organization of the maintenance.

In contrast to some previous projects where literal language was used to describe the safety functions, in the PS PSS a mathematical formalism has been used to describe each safety functions, with an important added value for the test definition, verification and automatic scripting [5] [6].

CONCLUSION

The refurbishing of the PS Personnel Protection System, whose design has been based on experience from the LHC Access system, has allowed the implementation of a highly secured and automatic access system for the PS complex of accelerators. Among the new concepts that have been introduced, we can underline the formal methods used for the PASS testing, the improved maintenance feature, such as the SSM diagnostic, the server virtualization, the access point maintenance functionality, as well as the dedicated networks and the integrated access point architecture. The challenge was also in the reliable integration of the numerous technologies and equipment involved. The project methodology based on the IEC 61508 Functional safety standards, as well as testing facilities and stages, promises a smooth system commissioning at the end of the CERN Long Shutdown scheduled during the spring 2014.

REFERENCES

[1] Eva Sanchez-Corral Mena et al., "Data management and tools for the access to the radiological areas at CERN", MOPPC057, ICALEPCS 2013.

[2] T. Hakulinen, et al., "Revisiting CERN Safety System Monitoring", MOPPC055, ICALEPCS 2013.

[3] T. Hakulinen et al., "Application of Virtualization to CERN Access and Safety Systems", MOPPC054, ICALEPCS 2013.

[4] P. Ninin, "IEC61508 Experience for the Development of the LHC functional safety systems and future perspectives", ICALEPCS 2009 proceedings.

[5] F. Valentini et al., "Formal Methodology for Safety-Critical Systems Engineering at CERN", TUCOCA04, ICALEPCS 2013.

[6] P. Ninin et al., chapter 12, "Safety of Computer Architectures", WILEY, ISBN 978-1-84821-197-1.

ISBN 978-3-95450-139-7