ISBN: 978-3-95450-214-1 ISSN: 2673-5490 doi:10.18429/JACoW-IPAC2021-TUPAB314

SPS PERSONNEL PROTECTION SYSTEM: FROM DESIGN TO COMMISSIONING

T. Ladzinski, T. Hakulinen, F. Havart, V. Martins De Sousa Dos Rios,
M. Munoz Codoceo, P. Ninin, J. Ridewood, E. Sanchez-Corral Mena, D. Vaxelaire
CERN, Geneva, Switzerland

Abstract

During the second long shutdown (LS2) of the accelerator complex at CERN, the access system of the Super Proton Synchrotron (SPS) was completely renovated. This complex project was motivated by the technical obsolescence and lack of sufficient redundancy in the existing system, as well as by the need for homogenisation of technologies and practices across the different machines at CERN. The new Personnel Protection System (PPS) includes 16 state-of-the-art access points making sure that only fully identified, trained and authorised personnel can enter the facility and an interlock system with a rationalized number of safety chains designed to meet the current safety standards. The control part is based on Siemens 1500 series of programmable logic controllers, complemented by a technologically diverse relay logic loop for the critical safety functions. This paper presents the new system and the design choices made to permit fast installation in a period where the access system itself was heavily used to allow vast upgrades of the SPS accelerator and its infrastructure. It also covers the verification and validation methodology and lessons learned during the commissioning phase.

INTRODUCTION

The Super Proton Synchrotron, CERN's second largest accelerator, was put in service in 1976. Its access control and safety interlock system, also known as the Personnel Protection System, was first upgraded in the beginning of the nineties. However, after three decades of use, it has reached its end of life, with further upgrades no longer possible due to lack of spare-parts and more severe safety constraints.

During the second long shutdown of the CERN accelerator complex, the SPS PPS was fully replaced. This major project completed the renovation process of the Personnel Protection Systems, providing the same level of safety and user experience in the PS, SPS and LHC. Whereas the 16 access points, instrumentation of 245 doors and cabling were completely replaced, the sectorisation (division of the facility into access zones and their sectors, positioning of doors etc.) was only slightly modified and practically no civil engineering works took place. The control safety system with some 23'000 I/O channels was also completely replaced: 85 new racks were installed and new software developed using the concepts proven in the PS [1] and LHC [2] personnel protection systems.

SPS SAFETY CHAINS REVISED

The SPS accelerator is a circular machine housed in a 7 km long tunnel 60 m underground. In addition to the main ring tunnel, the SPS complex includes the transfer tunnels linking the ring with the PS and the LHC machines as well as several experimental areas. The SPS is currently used to deliver beams to the LHC and to three experimental regions: the North Area, as well as the HiRadMat and the AWAKE facilities. A risk analysis exercise was conducted and a revision of safety chains performed, bringing their number from 14 to 6 primary chains protecting six interlocked zones, composed of one or several access sites. In addition, three operational safety chains were identified, which are not linked to specific interlocked zones, but where beam operation is only permitted when a specific set of external conditions is met (e.g. the LHC ready to receive beam via the TI8 injection tunnel). The operational safety chains are depicted as arrows in Fig.1, representing the SPS Complex and its safety chains.

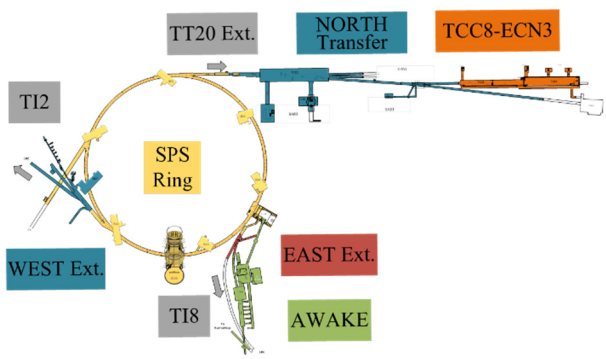

Figure 1: SPS Complex with colour-coded safety chains.

The rationalisation of the safety chains together with the introduction of a modular Operational Key Panel (OKP) for the control room operators was the first big change introduced with the new system. Furthermore, for each safety chain, the interfaces with the Elements Important for Safety (EIS), capable of stopping the beam injection or circulation, were revised and upgraded. The original choice of the elements was kept. The system interlocks the main magnet circuits in the ring and a selection of kicker or injection septa, mobile beam dumps or dipole magnets for the remaining chains, providing at least a triple redundancy for each safety chain and technological diversity of the elements. The improvements in the new system included the definition of a common interface with the EIS-beam, transmitting via two independent cables ambivalent status signals and independent orders. In addition, an upstream protection mechanism was introduced, where in case of a malfunction of two EIS-beam of a given safety chain, the upstream safety chain is solicited.

ISBN: 978-3-95450-214-1 ISSN: 2673-5490 doi:10.18429/JACoW-IPAC2021-TUPAB314

INSTALLATION CHALLENGES

The SPS PPS project had to face stringent constraints: contrary to many machine systems, which are no longer in use when the beam operation stops, the access systems become indispensable during shutdown periods. Thus, during the entire duration of the LS2 and replacement of the PPS, at any moment in time each of the access sites had to remain accessible, access controlled, the number of people inside the facility and their identities known, external envelope of the facility monitored for intrusion. Moreover, the AWAKE experiment's R&D program continued through major part of the LS2 with electron beam and laser hazards. These additional constraints led to several design and organisational choices aiming at:

- minimising access unavailability to each site;
- maintaining the old system operational until the last site was renovated;
- being able to install and operate the new central infrastructure from a temporary location;
- having maximally standardized hardware and software components to facilitate possible schedule changes.

NEW ACCESS POINTS

Beam operation in SPS is permitted only in the absence of personnel and any long-term access period is followed by a systematic patrol of the facility. Short accesses thereafter are allowed only to those in possession of a token interlocking the beam operation. The protection concept assumes inviolability of the access points. To this end, CERN introduced in the LHC an access point made of a Personnel Access Device (PAD) and a Material Access Device (MAD). The PAD allows only one person to enter at a time, contrary to the turnstiles, which were used in the past. By further integrating access control mechanisms within the device, only identified, authenticated, authorised and trained personnel, with an approved intervention, is allowed access with minimum supervision from the control room. Similarly, bringing material into the facility is no longer subject to video monitoring of the intervention by the operators. Instead, the material is introduced into the MAD, where a complex video recognition algorithm scans the interior and allows opening of the internal door only when no person was detected inside.

A number of electronics devices are necessary to implement the access control protocol. In the SPS these are: a commercial badge reader, identifying the users from their passive dosimeters; an iris biometric scanner verifying the user's identity, an access database unit checking the user id against a constantly refreshed list of users allowed access; a custom made reader verifying that the user is in possession of an activated operational dosimeter. Each PAD is also equipped with a touchscreen, 32 interlocked tokens, intercoms to allow communication with the control room and CCTV cameras. All the equipment together with access point controller units and I/O modules require one or two racks to be placed adjacent to the PAD. In the SPS PPS the space constraints did not permit easy integration of racks in the existing volumes close to the shaft entrances. Moreover, having access control equipment mounted in independent racks implies numerous electrical connections, which take time to be installed and tested.

The PAD used in the SPS PPS is a novel solution [3], where all the auxiliary equipment is incorporated inside the PAD mono-block structure. Figure 2 shows the original design and the installed PAD with equipment drawer opened. This design permitted the device to be fully assembled and tested at the factory. Once delivered on-site, it only required positioning in the final location and connection of the 24 VDC power supply and two network cables. With this plug-and-play concept, the installation and commissioning time of the access devices was significantly reduced.

Figure 2: SPS PPS Personnel Access Device.

CONFIGURABLE SAFETY SYSTEM

The SPS PPS safety-interlock part is based on the Siemens F1500 series of Programmable Logic Controllers (PLC). It is composed of the Global Interlock (GI) controller forming the Central Layer and 16 Site controllers at the Site Layer. In addition, at the Equipment Layer, each PAD is equipped with a Siemens F Open Controller. The GI and Site controllers are linked together by a dedicated fiber ring using Ethernet Profisafe protocol. Figure 3 shows a vertical slice of the PLC architecture with only one site represented.

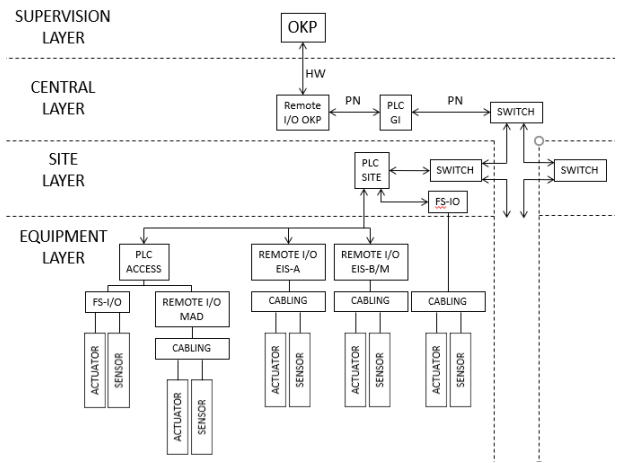

Figure 3: Safety PLC architecture overview.

ISBN: 978-3-95450-214-1 ISSN: 2673-5490 doi:10.18429/JACoW-IPAC2021-TUPAB314

Each site controller holds information about the different safety elements (access, beam) constituting the site. It is stored in several configuration tables describing the structure of the site, e.g. indicating which doors belong to which sector. The core of the safety program was developed using interlock matrices. A status matrix is calculated locally in each site controller and is permanently fed to the GI controller, which constantly evaluates what action should be applied to the elements of each safety chain. The main program for every site is identical, the differences between the sites being managed with the configuration tables [4]. Once tested for the first site, the PLC program could be rapidly instantiated for other sites and required less verification efforts. This approach permitted rapid adjustments of the deployment strategy, and allowed keeping the important project milestones by changing the order of site development (mostly limited to setting of configuration bits) to accommodate unexpected situations.

In addition, the SPS PPS incorporates a technologically diverse redundant cabled loop. It is a relay logic mechanism monitoring dedicated sensors on the external envelope doors and token distributors and, in parallel to the PLC program, interlocking the beam elements. This simple and robust solution satisfies the nuclear sector normative requirement of technological diversity.

VERIFICATION & VALIDATION METHODOLOGY

The verification and validation of the SPS PPS followed a well-established process, as required by the functional safety standards IEC61508/61511. It started with factory acceptance tests of major system components, followed by test platform verification of each site controller program and each PAD, prior to the on-site installation.

A dedicated test platform was constructed at CERN. It is made up of a vertical slice of the system and incorporates a complete access point (PAD and MAD), a test bench for additional PAD, 3 site controllers, as well as the Global Interlock controller and all IT infrastructure (access control database servers, video and audio communication servers, network devices) and control room HMIs. Each PAD was fully tested in the test platform to verify that it operated correctly in the CERN IT environment. In parallel, every site controller program was exhaustively tested in the test platform, in particular all the safety functions and HMI views. Moreover, formal verification techniques to check that the PLC program fulfils the specification have been tried for the SPS PPS safety software.

Once a site installation completed, the contractor performed detailed hardware wiring tests and functional tests on a site by site basis, complemented by functional tests of the site by an independent CERN team. This approach allowed the project to progressively commission parts of the system, which could be used to control access or even local hazards, as was the case with the AWAKE experiment, within days of installation works completion.

In parallel, as the interfaces with external systems or beam elements became operational, they were tested to assure conformity with the specification. Given the installation schedule and the structure of the safety chains spanning several sites, the commissioning of the interlock part could only be done at a later stage. It required the readiness of all sites forming a chain, the completion of interventions on the EIS-beam elements, and the general advancement of the LS2 works in the SPS to permit the removal of electrical lockouts. Two testing sessions, lasting one week, were organized, one for the SPS ring and the LHC transfer tunnels and one for the safety chains of the North Area. These were complemented by an independent validation of the safety functions by the Beams Department Safety Officer.

OPERATIONAL FEEDBACK

In summer 2019 the first complete access site was commissioned and delivered to the physics community to secure the AWAKE operation. Several availability problems were detected with the PAD in the following months and a new version of the PAD controller program was prepared, tested and deployed. The operation of AWAKE in parallel to the installation of the remaining sites posed additional challenges, but also served as a full scale exercise for gradual deployment and commissioning with limited impact to the already operational sites.

In summer 2020, following the installation of the last access point, the central IT infrastructure was placed in its final location in the CERN Control Centre with only a one day “access blackout” in the SPS, proving the correctness of the architectural and methodological approaches. From December 2020 the system was intensively used to secure the Hardware Commissioning activities of the SPS following the end of the LS2 works. All the sites were patrolled and tens of accesses with interlocked tokens monitored per day. This running-in phase underlined the need for regular PAD maintenance as many electromechanical parts needed re-adjustment. Further improvements to the PAD software were also requested, to allow more user friendly error handling and diagnostics. In addition, on a few occasions, the system was brought to a safe state due to spurious passivation of Siemens I/O modules, resulting in a firmware update campaign. No safety critical issues have been reported and the system passed to the next stage of securing beam operation in the SPS.

CONCLUSIONS

The SPS Personnel Protection System was successfully renovated during the LS2. In spite of very tight schedule constraints, the works were completed on-time and with very limited impact on access to the SPS. The system was extensively tested and used during the Hardware Commissioning period of the SPS and is today protecting the personnel from beams circulating in the SPS complex.

ISBN: 978-3-95450-214-1 ISSN: 2673-5490 doi:10.18429/JACoW-IPAC2021-TUPAB314

REFERENCES

[1] P. Ninin *et al.,* "Refurbishing of the CERN PS complex personnel protection system", in *Proc. ICALEPCS'13,* San Francisco, USA, Oct. 2013, paper MOPPC059, pp. 234-237.

[2] P. Ninin *et al.,* "LHC access system: from design to operation", in *Proc. EPAC08,* Genoa, Italy, 2008, paper TUPC129, pp.1371-1373.

[3] T. Ladzinski *et al*., "New concepts for access devices in the SPS personnel protection system", in *Proc. ICALEPCS'17*, Barcelona, Spain, Oct. 2017, pp. 1608-1612, doi:10.18429/JACoW-ICALEPCS2017-THPHA099

[4] T. Ladzinski *et al.,* "Renovation of the SPS personnel protection system: a configurable approach", in *Proc. ICALEPCS'19*, New York, USA, Oct. 2019, pp. 395-399, doi:10.18429/JACoW-ICALEPCS2019-MOPHA078