ACHIEVING A HIGHLY CONFIGURABLE PERSONNEL PROTECTION SYSTEM FOR EXPERIMENTAL AREAS

F. Havart, R. Nunes, D. Chapuis, D. Vaxelaire, CERN, Geneva, Switzerland

Abstract

The personnel protection system of the secondary beam experimental areas at CERN manages the beam and access interlocking mechanism. Its aim is to guarantee the safety of the experimental area users against the hazards of beam radiation and laser light. The highly configurable, interconnected, and modular nature of those areas requires a very versatile system. In order to follow closely the operational changes and new experimental setups and to still keep the required level of safety, the system was designed with a set of matrices, which can be quickly reconfigured. Through a common paradigm, based on industrial hardware components, this challenging implementation has been made for both the PS and SPS experimental halls, according to the IEC 61508 standard.

The current system is based on a set of hypotheses formed during 25 years of operation.

Conscious of the constant increase in complexity and the broadening risk spectrum of the present and future experiments, we propose a framework intended as a practical guide to structure the design of the experimental layouts based on risk evaluation, safety function prescriptions and field equipment capabilities.

INTRODUCTION

Secondary beams physics is supported at CERN since the seventies. It has seen several personnel protection systems (PPS) along the years, protecting personnel from radiation hazard.

For historical and organizational reasons, PS and SPS experimental areas (EA) PPS, despite their common role and function, were never identical. Developed by different teams, at different times, and for different groups of users, they always shared the mission, but neither the technology, nor the look and feel.

In 2003, following the obsolescence of the systems in place at the time at both PS and SPS, a decision was taken to renew them completely, using a common design and uniform concept for the first time [1].

The Safety Instrumented Functions (SIF) implemented by the EA PPS should guarantee that:

- If there are people in a zone, there is no beam.
- If there is beam in a zone, there are no people.

Safety is, of course, paramount in the implementation, but availability is not to be overlooked, as the PPS is essential to beam operation. Without an operational PPS, no EA physics is possible.

PS AND SPS EXPERIMENTAL AREAS OPERATION

The experimental areas are a set of physically independent enclosed zones into which one or several beams can be injected. Their size and shape can be adapted to serve the intended purpose. A group of zones, usually located in the same building hall, is called a super zone (Figure 1).

Currently, CERN runs 5 super zones, 2 for PS and 3 for SPS.

Depending on the experimental requirements, the zones are equipped with the needed instrumentation, beam lines, target if needed, and safety protections. They are operated for the required period of time according to the physics planning, and then reconfigured for the next experiments. Duration of a particular configuration ranges from a few days to several weeks.

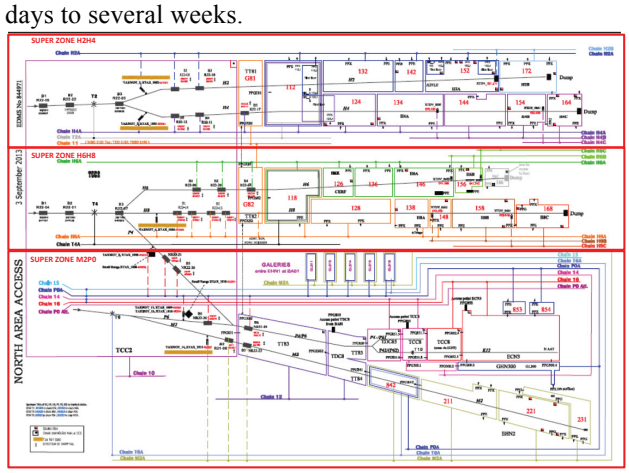

Figure 1: CERN SPS experimental areas, showing beam lines, super zones, zones imbrication, EIS-M and EIS-A positions.

SYSTEM DESIGN

To mitigate the radiation hazard and to achieve a high degree of personnel protection, the super zone PPS interlocks the Element Important for Machine Safety (EIS-M), able to stop beams, and the Element Important for Access Safety (EIS-A), able to stop access.

The following requirements existed for the overall system:

1. Reconfiguration of EIS-A/EIS-M combination had to be possible without any system change, software or hardware.
2. All the control system had to be based on available industrial equipment.

ISBN 978-3-95450-139-7

3. The zones had to be configurable up to a predefined number of components on the spot, without any code change (EIS-A, keys, flashing lights…).
4. The control room HMI had to follow the above reconfiguration without any code change.
5. The system had to be used for both PS and SPS experimental areas.
6. Doors, locks and key distributors had to be reused from previous systems.

The following requirements had been identified for the safety system:

1. Based on previous return of experience and radiation risk assessment, the SIF should fulfill a Safety Integrity Level (SIL) of 2.
2. One experimental area had to be protected at least by one dedicated secondary beam EIS-M and the primary beam extraction EIS-M chain it belonged to.
3. The design had to be done respecting as much as possible the norms for implementations of safety-instrumented systems for process industries, as described in the norm IEC 61508 [2].

The modular nature of the experimental areas and the high configurability need led to a design where each zone was autonomous in terms of computing resources. One concentrator is used per super zone to federate data (Figure 2).

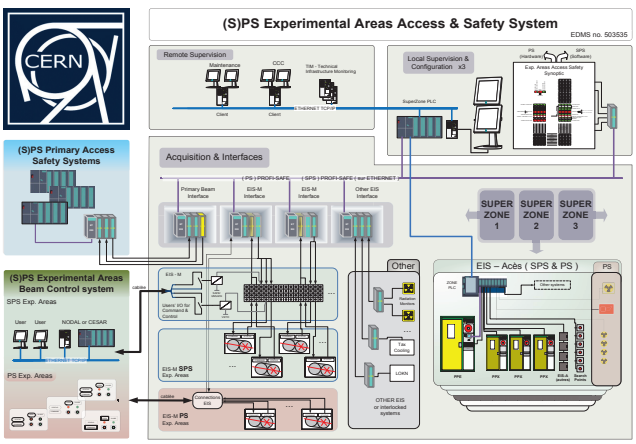

Figure 2: CERN SPS experimental areas architecture.

The general principles of redundant signals and failsafe safety component chains are fully applied in the design by:

- Sensor redundancy and diversity are provided by two separate contacts.
- Any vital safety signal is implemented as two separate signal paths, forming a signal channel. One signal is energized to trip, the other de-energized to trip.
- Any non-doubled signals are implemented de-energize to trip (failsafe).
- The entire system is designed to trip in case of electrical power failure (failsafe).
- Any communication between components is designed with a failsafe protocol, which guarantees a trip in case of communication loss.

The safe-for-beam (S4B) safety condition is evaluated by a state machine running in the zone PLC. This condition is sent to the super zone PLC, through safety communication (Figure 3 and 4). The safety equation is:

S4B=EIS-A SAFE × KEY SAFE × EOA

Where:

- EIS-A SAFE is the sum of all zone access devices safe status.
- KEY SAFE is the resulting signal of all access key tokens present.
- End-Of-Access (EOA) is the validation of the transition from access mode to beam mode, which is only possible after a valid zone patrol.

The safe-for-access (S4A) safety condition is evaluated by the super zone PLC by acquiring all EIS-M positions. The safety equation is (veto being applied at false):

S4A=VETO ACCESS ZONE × ZONE radiation veto

Where:

- Veto access zone is an access veto imposed by one or more EIS-M protecting the zone in unsafe status.
- Zone radiation veto is an access veto applied by detection of an exceeded radiation level.

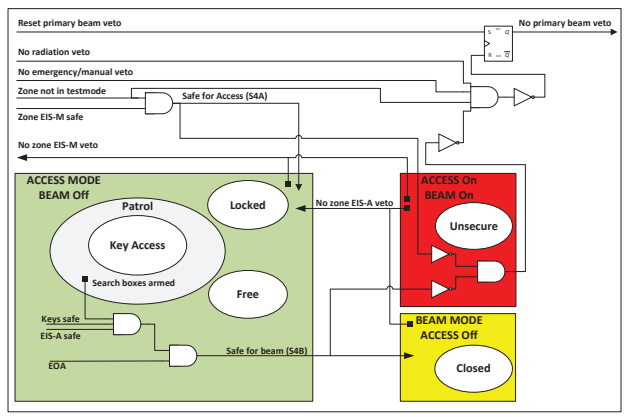

Figure 3: Illustration of PPS safety logic and the different operational zone modes.

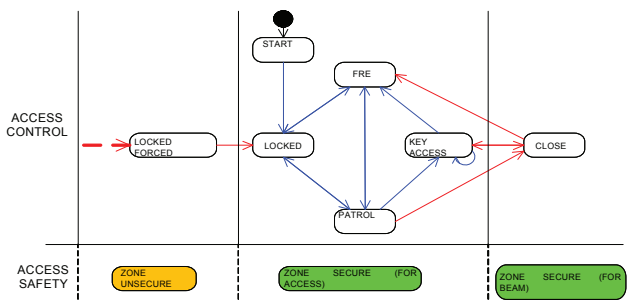

Figure 4: Illustration of PPS safety state machine and associated authorized access modes.

ISBN 978-3-95450-139-7

The configurability requirement of the safety elements has been addressed by using a concept of matrices (Figure 5). The leading design ideas were:

- To be able to associate any of the EIS-A with any of the EIS-M of a given super zone within the same secondary safety chain.
- To be able to associate any of the secondary safety chain of a given super zone within the same primary safety chain.

Three matrices are required to fully configure the system.

The design limits were set to:

- 64 EIS-M
- 64 EIS-A
- 32 secondary safety chains
- 16 primary safety chains.

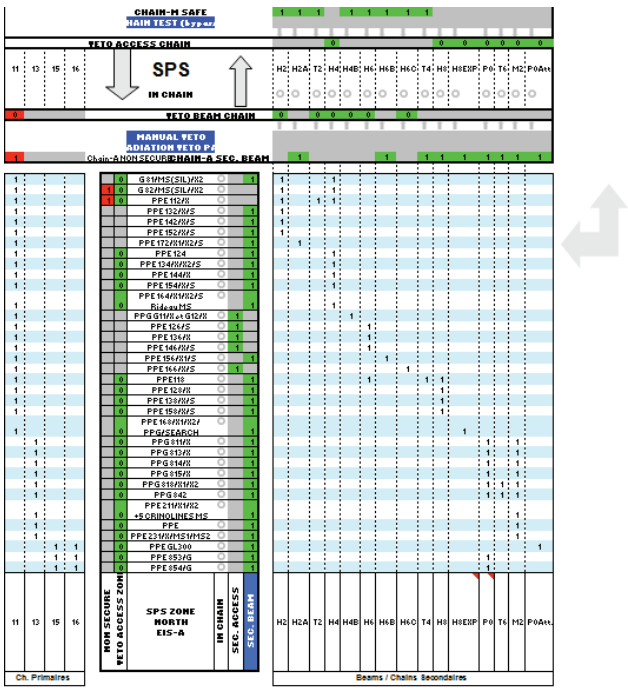

Figure 5: Illustration of PPS configuration matrices, EIS-M in the upper part, EIS-A in the lower part, secondary safety chains on the right, primary safety chains on the left, 1 symbols define an in chain condition.

IMPLEMENTATION

The system has been implemented using SIEMENS PLC [3] and split into two main subsystems, the concentrator PLC, which is the master of the super zone, and the access point PLC s, which manage the zones. The ability to combine both sequential standard code and safety code within the same CPU and hardware reduced the number of pieces of equipment.

The concentrator PLC acquires the state of and outputs the veto signals to EIS-M, reads the configuration matrices, and provides all data to CERN SCADA system TIM [4] to animate the Human Machine Interface (HMI) applications.

The access point, or zone PLC, acquires the state of and outputs the veto signals to EIS-A, calculates the patrol, manages the key distributor and interaction with the user using a local industrial touch screen. A local LED panel provides additional information.

Both PS and SPS experimental areas PPS share the same design and concepts. They also present the same interface, behaviour, and look and feel to the users. The PLC code has been written to isolate the specific PS and SPS parts and to keep a common trunk. Therefore, building a PS or SPS version differs only by including the specific code modules while generating the PLC programs.

PS PPS Implementation

The implementation timeline had the PS PPS deployed before SPS. The previous PS PPS was already using PROFIBUS for zone to super zone communication. Therefore, this medium was reused.

The choice of hardware matrices was made to allow PS operators, who have used similar interface in previous systems, an easy transition to the new one. It also offers a very intuitive configuration interface, and is easy to check visually.

To allow a reliable and safe acquisition of those critical signals, each matrix consists of 4 layers and delivers the column signal on a PLC safety channel, using two ambivalent electrical signals. Inserting a specific connection pin, white for out-of- chain, and black for in-chain, makes the configuration. The pins contain diodes, which prevent the electrical signal from being affected by the matrix lines above the one being read. Once the black pin is inserted, it feeds the cause (line) signal to the PLC logic.

Turning a dedicated key located in the rack triggers an automatic system reconfiguration. The PLC applies a veto on all EIS-A and EIS-M and scans the matrices by alternatively energizing each line, reading the result of the column to build an image of the configuration. Included safety checks guarantee that only one line is energized at any given time. Once the configuration is acquired, the PLC carries out the safety equation calculations and releases or maintains the EIS-A and/or EIS-M veto signals accordingly.

The complete PS PPS implementation has been done using SIEMENS STEP 7 and distributed safety add-on suite.

SPS PPS Implementation

The SPS experimental super zones are bigger and geographically much less centralised than the PS. There was also no inherited previously installed fieldbus or network. The original plan was to deploy the same system for PS and SPS, but during the 3 years separating the two campaigns, the design team gathered experience with another SIEMENS product used in the LHC PPS, the

ISBN 978-3-95450-139-7

software SAFETY matrix. This software allows the same functionalities as the PS hardware matrices, but removes the need for inputs, outputs and cabling required by the PLC to read them. Moreover, it offers traceability of the configuration changes, and the matrix system tool suite is certified by its editor and the TUV for safety control applications.

The transition to the software matrices had the following implications on component choice: a move from S7-300 to S7-400 PLC series for the super zone CPU, which imposed de facto Ethernet as fieldbus, as PROFIBUS F communication for safety data exchange is not available with S7-400 series CPU running safety programs.

While most of the zone PLC software has been kept the same, with the exception of the standard and safety communication modules, the new implementation direction required a complete rewrite of the super zone PLC code. However, the logic and signal treatments remain the same across both implementations.

The SPS PPS implementation has been done using SIEMENS STEP 7 and distributed safety add-on suite for the zone PLC. STEP 7, F-system and SAFETY MATRIX add-on safety suite for the super zone PLC

A NEW FRAMEWORK PROPOSAL

Motivation

Since the implementation of the first generation of PS & SPS Experimental areas PPS, several new zones and projects have been assigned to the experimental areas. In considering the physical zone design and PPS configuration, users consider the same types of issues, and arrive invariably at different conclusions. The perception of risk & hazard being specific to each individual, it is common to arrive at conflicting designs.

One common pitfall is to choose a specific design because the experiment setup is physically located in an experimental/secondary area and this is the way we have always done in these areas.

As the risks and complexity of the experiment setups increase, and the safety regulations become stricter, it is important to define a framework that can help the CERN safety officers decide on the actual implementation of the Personnel Protection System for each experiment, and eliminate as much as possible the subjective analyses.

In line with Functional Safety prescriptions inspired by IEC61508, we propose to set up a risk-based framework that imposes minimum design prescriptions, taken from a design catalogue.

PPS Design Framework

All safety system design phases shall be preceded by a risk analysis phase. A simple checklist should allow a systematic check of the most common factors such as:

- Radiation from beams
- Radiation from sources or activated material
- Cryogenic risks (ODH or burns)
- Electrical risks
- Magnetic field risks
- Lasers or X-rays

Each risk shall be classified on a scale that can range from 0-3 (Non-existent, negligible, significant, important), considering consequence and frequency of possible undesired events.

The SIF for the PPS shall be defined as a function of the risks and attributed a SIL Level. They shall include at least the following:

- Interlock of EIS-M/other during access
- Interlock of EIS-A during beam
- Interlock of beam upstream elements in case of hazard
- Assistance to Zone Patrol
- Warning of Imminent Danger

Furthermore, some common access control features shall be mapped on to the SIFs such as:

- Single person passage devices (turnstiles/airlock versus door)
- Multi-factor versus single-factor authentication (biometric versus card)
- Safety Token usage during Key-Access mode
- Surveillance of material passage

When agreement is reached, a general guide shall be available for design of the new zones. We expect to conclude a final proposal for this framework in 2014.

CONCLUSIONS

The developed PPS solution fulfils all the identified safety requirements and has proven very reliable. The achieved high configuration flexibility allows an adaptability, which should accommodate the proposed framework with minimal architectural and design changes.

REFERENCES

[1] Experimental areas PPS URD and SRD
[2] http://www.iec.ch
[3] http://www.automation.siemens.com
[4] TIM monitoring system

ISBN 978-3-95450-139-7