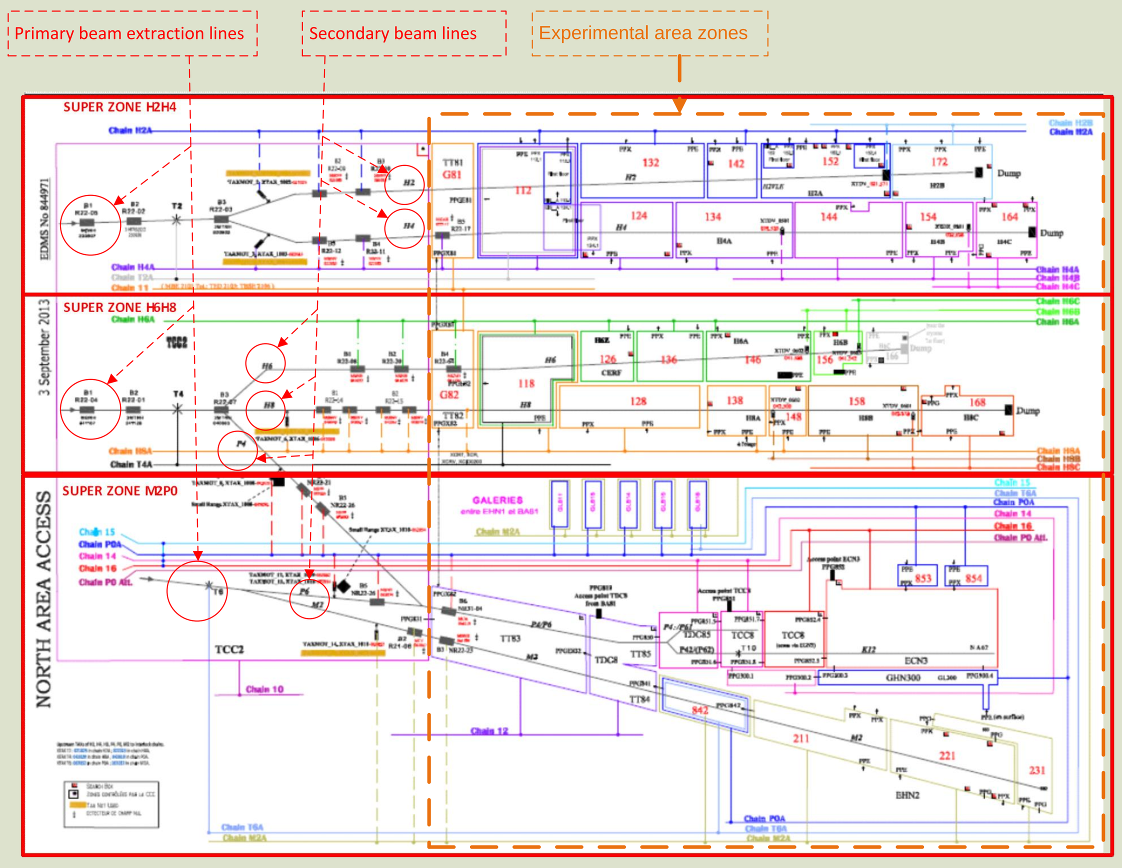
ACHIEVING A HIGHLY CONFIGURABLE PERSONNEL PROTECTION SYSTEM FOR CERN EXPERIMENTAL AREAS

San Francisco, California, USA
6-11 October 2013

Frederic Havart, Rui Nunes, Didier Chapuis, Didier Vaxelaire, CERN, Geneva, Switzerland

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.

The Challenge: To Protect A Very Versatile Environment Layout



- **CERN experimental areas** are dedicated to physics experiments for widely varying durations and layouts. Those characteristics induce a high rate of configuration changes which must be followed by the Personnel Protection System (PPS).
- **The required PPS configuration flexibility** has to be achieved without safety being compromised at any time.

Left: CERN Super Proton Synchrotron (SPS) experimental areas layout, showing beam lines, zones imbrication, EIS-M (Element Important for SAFETY, Machines) and EIS-A (Element Important for SAFETY, Access)positions.

In Numbers

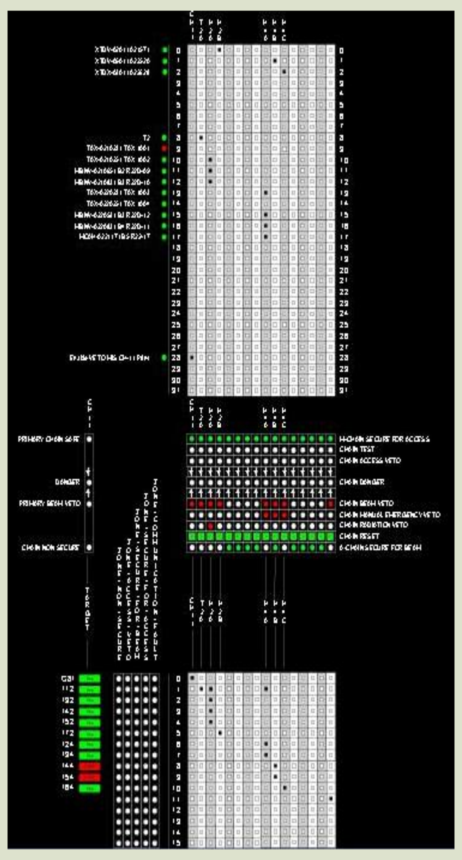
The design limits were set to:
- 64 EIS-M
- 64 EIS-A
- 32 secondary safety chains
- 16 primary safety chains

Siemens hardware type used:
- 317 F (PS) or 400 H CPU (SPS), SM 326 F DI/DO,
- 315 F CPU (PS and SPS) SM 326 F DI/DO

References

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

Supervision From CCC

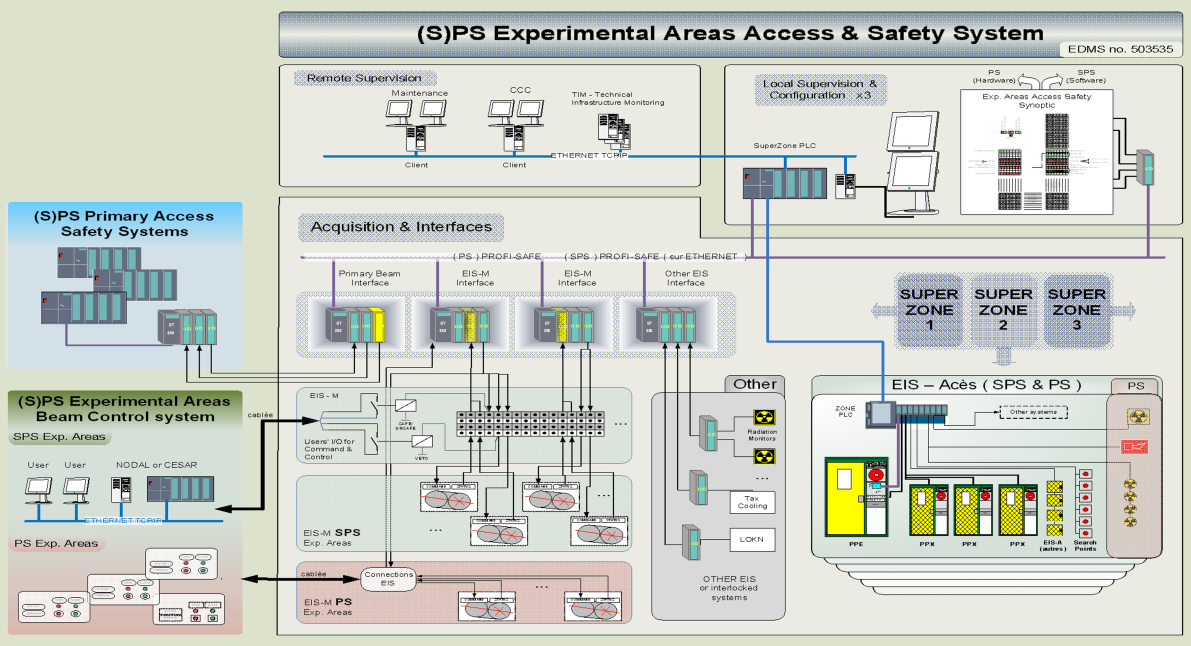


- **Experimental Areas TIM synoptic** are dynamically configured from the chosen setup of the field elements up to the designed maximum.

Left: TIM CCC (CERN Control Centre) matrices synoptic displaying current configuration and status of an experimental area super zone.

Bottom: TIM CCC detailed synoptic of zones present in a super zone.

Experimental Areas PPS Architecture



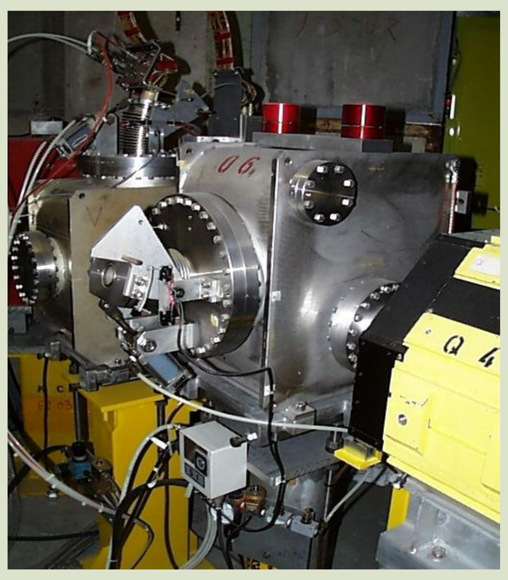
Overall system key requirements:
1. Reconfiguration of EIS-A/EIS-M combination had to be possible without any system change, software or hardware.
2. All the control system had to be based on available industrial equipment.
3. The zones had to be configurable up to a predefined number of components on 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.

Safety key requirements:
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.

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].

Signals Treatment

- 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.
- Sensor redundancy and diversity are provided by two separate contacts.



Top: Experimental area beam stopper
Bottom left: Access point control hardware
Bottom right: Zone access point

The Safety Logic

The safe-for-access (S4A) safety condition is evaluated by the super zone PLC by acquiring all EIS-M positions.

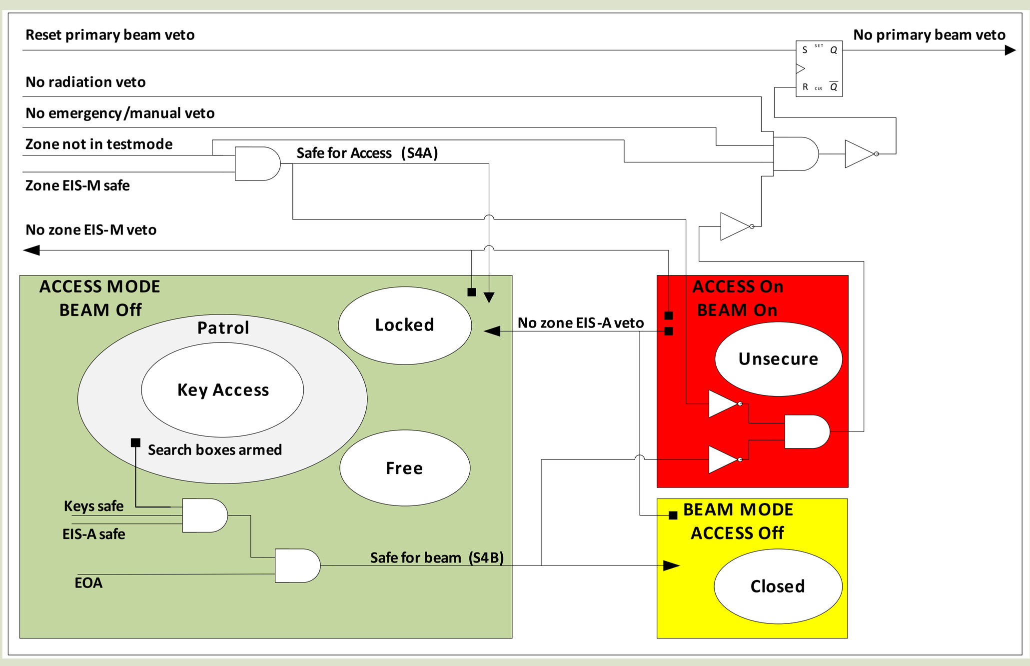
The safety equation is (veto being applied at false):

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.



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.

The safety equation is:

S4B=EIS-A SAFE × KEY SAFE × EOA

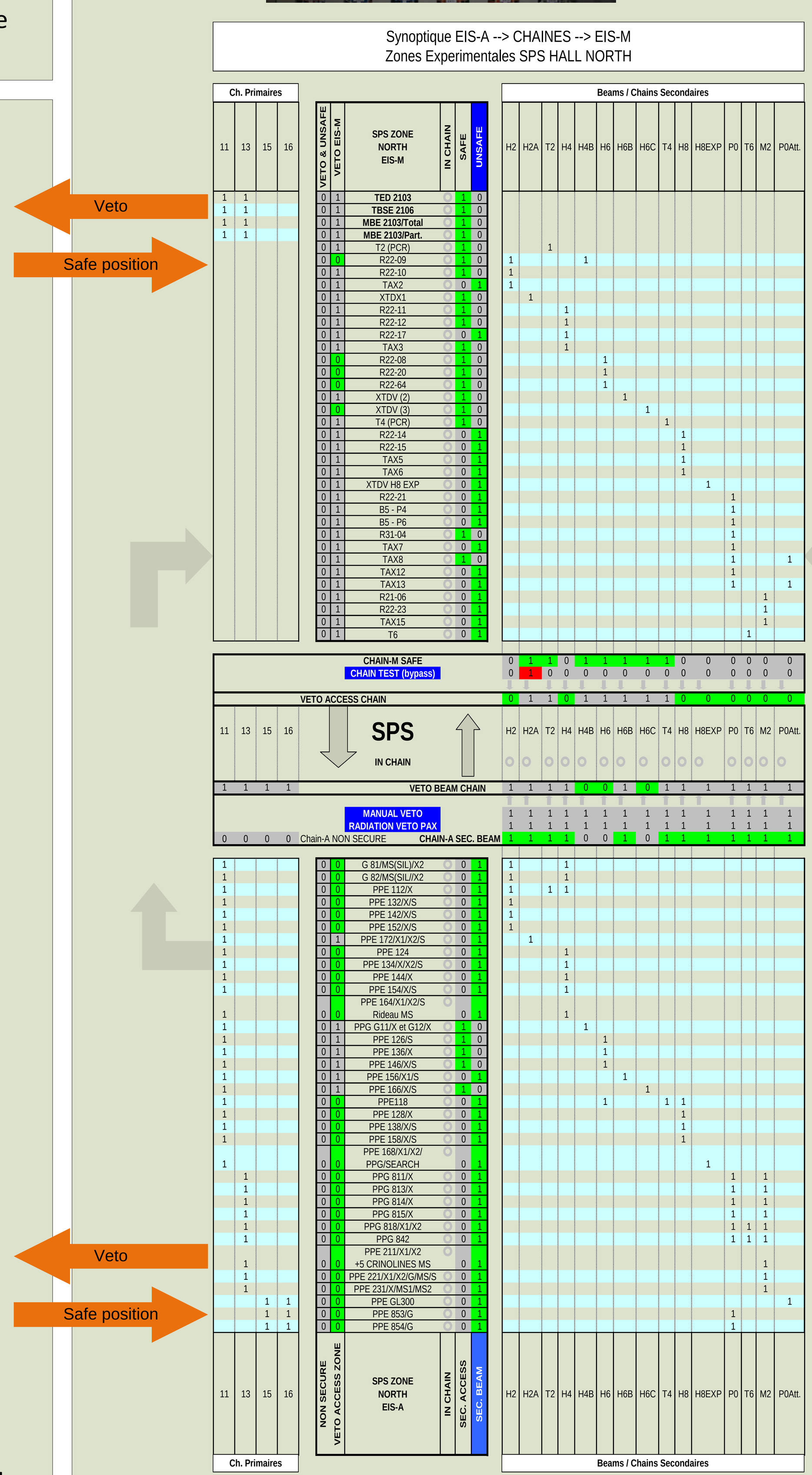
Where:

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.

PPS Configuration Mechanism – The Heart Of The System



Top left: Concentrator PLC, PS implementation, using hardware matrices

Top right: Concentrator PLC, PS implementation, hardware matrices view

Left: Configuration matrices concept representation:
- Top part, X axis, EIS-M safe position status
- Bottom part, x axis, EIS-A safe position status
- Left part, Y axis, primary chains safe status
- Right part, Y axis, secondary chains safe status

Bottom left: Concentrator PLC, SPS implementation, using software matrices, note the IO modules reduction, despite accommodating four times as much elements

Bottom right: Concentrator PLC, SPS implementation, SIEMENS Safety matrix tool used to configure interlock