PERSONAL SAFETY SYSTEM IN SESAME

A. Abbadi, A. Hamad, I. Saleh, SESAME, Allan, Jordan

Abstract

SESAME (Synchrotron-light for Experimental Science and Applications in the Middle East) is a third generation synchrotron light source under construction in Allan, Jordan. The personal safety system PSS aims to protect the personnel from radiation hazards coming from accelerator's operation by controlling the access to the radiation area and to interlock the operation of accelerator's sub-systems according to the area status. Phase 1 of SESAME PSS has been installed and commissioned successfully for Microtron and Booster tunnel. Rockwell L72s safety PLC (up to SIL 3 applications) [1] has been used for Microtron, Booster and Storage Ring PSS. Phase 2 includes the Installation of the storage ring's PSS; two new PSS cabinets with remote safety IO modules have been installed for the storage ring PSS and connected to the main PSS PLC via Ethernet safety CIP. Phase 3 is the personal Safety System for SESAME day one beam-lines which is currently under construction. Many procedures and interlocks have been implemented in order to allow SESAME Booster, Storage Ring and Beam-lines personal safety to be managed in a systematic, risk based manner.

PLC BASED PERSONAL SAFETY SYSTEM

In 1998, the first part of a seven-part international standard was published to define the requirements for programmable electronic systems used in the safety related parts of controls systems. This standard is known as IEC 61508, "Functional safety of electrical/electronic/ programmable electronic safety-related systems". This seven part standard is driving the direction for future safety PLC developments [1].

The personal safety system of SESAME is a PLC based control system which provides an easy tool to implement the PSS sequences and procedures in a protected programming tool where all changes are recorded. PLC provide the benefit to control the remote safety Input and Output modules through a safety certified communication bus; this reduces cabling and reduces the risk of cabling errors.

Safety PLC has redundant microprocessors, Flash and RAM that are continuously monitored by a watchdog circuit and a synchronous detection circuit, safety PLCs have an internal 'output' circuit associated with each input for the purpose of 'exercising' the input circuitry. Inputs are driven both high and low for very short cycles during runtime to verify their functionality. Safety PLCs are suited for applications at SIL 2 and SIL 3 where they can be certified for use in most common safety applications so it may prove more cost effective to use the certified package versus taking a new control architecture through the certification process [1].

Figure 1 shows the safety PLC properties in the programming software. The controller can be Locked/Unlocked by a password, no modification is allowed on the safety logic if the controller is locked or working in running mode [1]. Safety signature should be generated after each logic modification; this signature shows the date and time of modification.

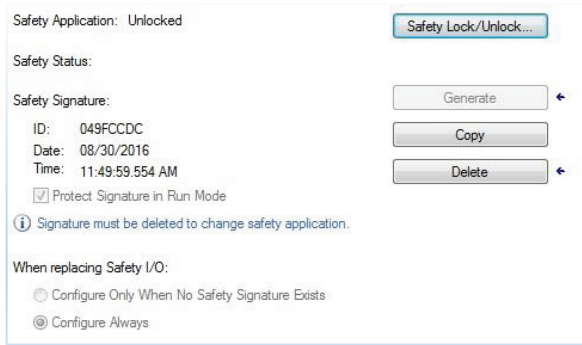

Figure 1: PSS safety PLC (Allen Bradley Guard -Logix L72s) properties.

SIL (SAFETY INTEGRITY LEVEL)

In comparison to similar facilities, the personal safety system at SESAME has been designed and selected to meet the requirements of SIL3, the SIL rating of a safety function is a measure of the degree of confidence in its overall ability to provide the safety function for nearly all of the time and under nearly all circumstances [2]. The most widely adopted functional safety standard is the International Electrotechnical Commission's IEC 61508 [3]. The standard divides SIL ratings into four levels, one through four, each representing an order of magnitude reduction in risk.

SYSTEM LAYOUT

Figure 2 shows the layout of personal safety system PLCs where the safety related functions are performed. A separated PLC for machine PSS and another one for the beam-line PSS.

ISBN 978-3-95450-189-2

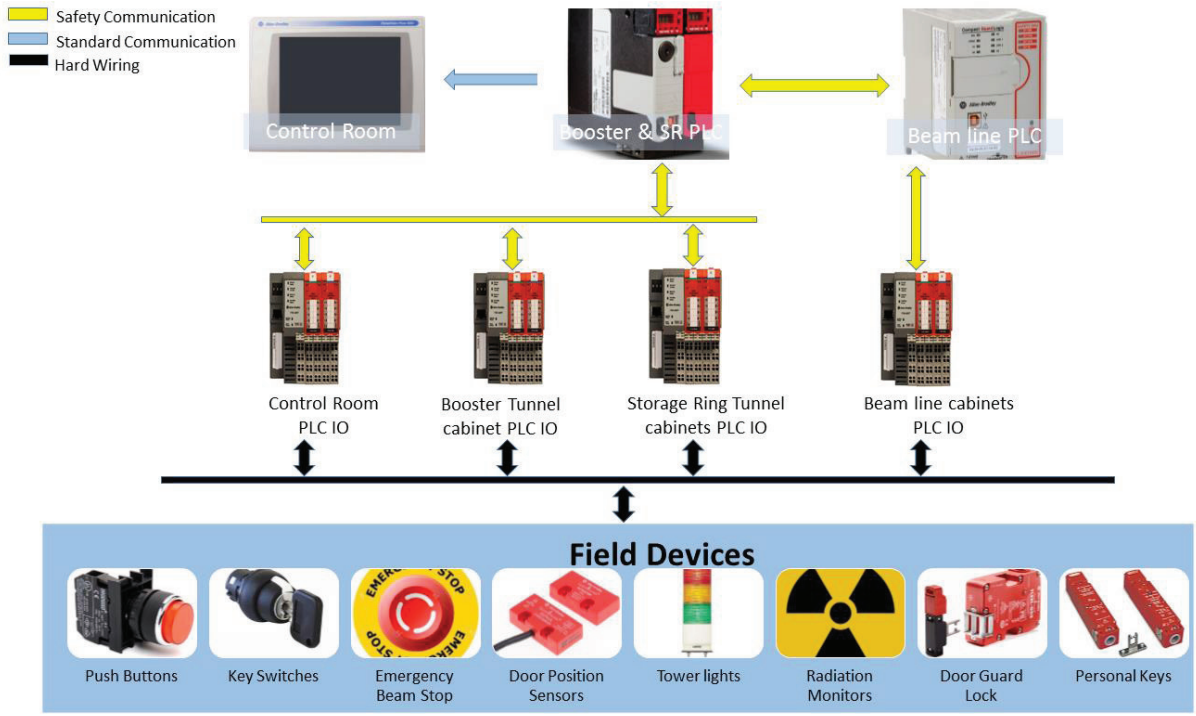

Figure 2: Layout of SESAME's personal safety system.

PSS FUNCTIONS

The PSS functions have been implemented by a combination of software routines and a set of devices dedicated for PSS. The interlocked areas are divided into three parts: Booster tunnel, Storage Ring tunnel and Beam-lines each part has its own emergency stop buttons, search points buttons, horns, flashing lights, door locks, door position sensors and status panel, Fig. 3 shows the personal safety system components in the storage ring area.

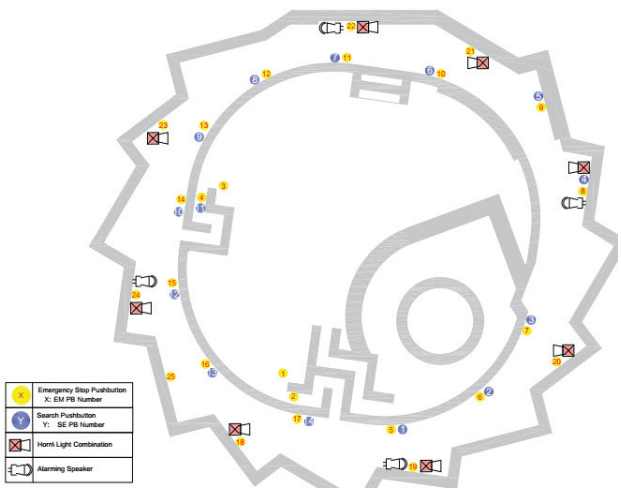

Figure 3: Personal Safety System components locations in the Storage Ring Tunnel.

The personal safety system has many functions:

- It's provide a search (Sweep) and personnel evacuation procedure from radiation area prior to accelerator operation by three trained people, the PSS PLC monitor, controls the search sequence and visualizes the steps on HMI at control room for operator monitoring, a set of search buttons inside the radiation area should be pressed by a predefined sequence and pre-defined time range and the sequence.
- Audible and visual warnings during tunnel search and prior to machine operation, a set of loudspeakers annunciate a recorded message for tunnel evacuation and another message prior to operation in addition to alarming flashing lights with horn.
- Visual indication of machine status at each door of radiation area and at control room.
- Redundant and diverse locking mechanisms and position sensor for area entrances to protect the people from entering the radiation area during operation.
- Shut off the machine when a predefined accumulated dose values detected in occupied area by radiation monitors. Combined neutron-gamma radiation trolleys (by Thermo Fisher) are distributed in the occupied critical zones. Three digital signals are continuously provided by each trolley to PSS, monitoring the status of radiation level and error signals. PSS will react accordingly to each of these signals [4].
- Provide a set of emergency stops distributed in the radiation area, control room and next to doors in the service area which can be used by personnel to shut off the machine on emergency case.

ISBN 978-3-95450-189-2

LOGIC

The safety PLC monitors a set of conditions connected to its input modules and as result of the programmed logic safety PLC will send the permissions to allow the operation of the interlocked system as Microtron, Booster RF, Storage Ring RF, Injection from booster to Storage Ring and beam shutters, each system has some conditions to be verified, if one or more conditions lost, the PLC will disable the related system.

The Personal Safety System logic has been programmed to work in a three states, the first one is open state which is the mode prior to area search procedure, the interlocked area is free to access, the doors are unlocked, and the beam is not permitted. The second is interlocked; the mode after doing the area search procedure, no people inside the radiation area, no access is allowed to radiation area, doors are closed and locked and beam permits is active. The third state is restricted access; a controlled access to the booster tunnel and storage ring tunnel for a limited number of personnel is available by using a special personal keys located at the PSS panel next to tunnel door (key position is detected by PSS PLC), the beam permit is disabled during the restricted access. This mode ends if all personal keys are returned to their locations on PSS cabinet and the finish button pressed from the control room. The restricted access function is implemented only for the Accelerators PSS in order to make short interventions in the restricted areas without needing a new search patrol [5].

CONTROL ROOM

The control room PSS cabinet contains an HMI display, Fig. 4 shows the main GUI for storage ring PSS, the operator can monitor the PSS status, interlocks state, alarms history and the required conditions for each procedure.

CIP SAFETY PROTOCOL

The communication between PSS PLCs and remote IO modules is carried out through Ethernet CIP safety protocol, the CIP Safety end-to-end protocol gives responsibility to ensuring safety to the end nodes rather than the bridges, routers, or intermediate nodes. CIP Safety cannot prevent communication errors from occurring, but if an error does occur in the transmission of data or in the intermediate router, the end device detects the failure and takes the appropriate action. CIP Safety is certified to be compliant with the functional safety standard IEC 61508 up to safety integrity level SIL 3 [1].

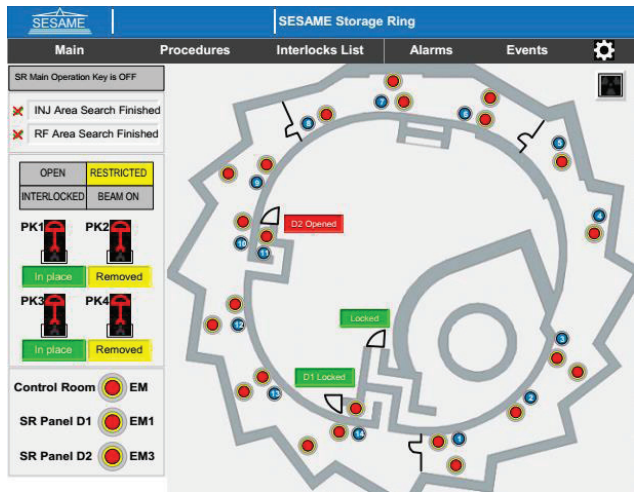

Figure 4: Personal Safety System GUI Main Screen for Storage Ring.

The safety PLC is a de-energize-to-trip system, which means that all of its outputs are set to zero when a fault in communication is detected which disables all the interlocked systems to the safe state [1].

This HMI, only meant for monitoring and diagnostics, reads tags from standard (not-safety) data blocks in the PLCs [5].

ACKNOWLEDGMENT

I would like to thank Dr. Erhard Huttel, Technical Director, the SESAME team, and special thanks to the control team.

REFERENCES

[1] Rockwell Automation, http://ab.rockwellautomation.com

[2] D. M. Macdonald, *Practical Machinery Safety*. IDC Technologies, Cape Town, South Africa: Elsevier, 2004.

[3] International Electrotechnical Commission, "Functional safety of electrical/electronic/programmable electronic safety related systems", IEC 61508, International Electro-technical Commission, Geneva, 2000.

[4] Thermo Fisher, http://www.thermofisher.com

[5] D. Fernández-Carreiras, "Alba, the PLC based protection systems", in *Proc. ICALEPCS'09*, Kobe, Japan, Oct. 2009, paper WEC003, pp. 397-399.

ISBN 978-3-95450-189-2