ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR04

SAFEGUARDING LARGE PARTICLE ACCELERATOR RESEARCH FACILITY- A MULTILAYER DISTRIBUTED CONTROL ARCHITECTURE

Feng Tao*, SLAC National Accelerator Laboratory, Menlo Park, USA

Abstract

Personnel Protection System (PPS) at SLAC is a global safety system responsible for protecting personnel from radiation hazards. The system's functional design shares similar concepts with machinery safeguarding, though the complexity of PPS is much higher due to its wide geographic distribution, large number of devices, and multiple sources of hazards. In this paper, we will first introduce the multilayer distributed control system architecture of SLAC's PPS, which serves three beam programs, e.g., LCLS, LCLS-II and FACET-II, that co-exist in the same 4km linear accelerator infrastructure. Composed of 50+ sets of redundant safety PLCs and 20+ access control PLCs, SLAC's PPS has five layers: beam program, beam switching and permit, zone access control, zone safety control and sensor/shutoff subsystems. With this architecture, safety functions often involve multiple controllers across several layers, make it a challenge on system analysis, verification, and testing. Therefore, in this paper, we will also discuss functional safety related issues for this type of complex systems.

OUTLINE OF THE PAPER

In this paper, the machinery safeguarding concepts and the introduction of SLAC's PPS are given first. Then different layers of SLAC and their functions are explained. For the representative E-Stop function, how each layer of PPS control contributes to the safety integrity is analyzed in Section 3. The impacts on system integrity for such a large distributed system are discussed in Section 4, with proposed solutions. At last, some remarks are given in the conclusion section.

MACHINERY SAFEGUARDING AND SLAC'S PPS

Machinery safety has been a matured and important field for safety-critical control system applications [1]. With the adoption of IEC 61508 [2] and the concept of functional safety, significant progress has been made in various application fields to formalize requirements on typical safety functions and their integrity levels. System designers should follow those standards and use those formalized requirements as a starting point. In machinery sector, there are two functional safety standards, e.g., IEC 62061 [3] and ISO 13849 [4], using different performance metrics Safety Integrity Level (SIL) and performance Level (PL) respectively. In Europe, ISO 13849 has been widely used as a type B1 standard that many type C specific machine safety standards referred to.

SLAC is a large research facility. It has a 2 miles long linear accelerator (Linac), which is being used to generate either high power electron beam, or extremely bright x-ray laser for scientific experiments. For this reason, the whole facility can be treated as a large "machine" producing electron/x-ray. So those best practice from machinery safety can be applied to SLAC's PPS as well.

There are some similarities and differences between conventional machinery safeguarding with SLAC's PPS.

Common practices include:

- Dual redundant circuitry for system reliability
- Operators' search procedure to secure the area
- Personnel trapped key interlock
- Wide usage of machinery safety certified components, from laser scanner, Emergency stop, trapped keys, circuit breaker, to safety PLCs.

On the other hand, as a large research facility, SLAC's PPS is much more complex than a conventional machinery safety system. The complexity comes from four factors:

- Wide geographical distribution
- Large numbers of field devices to monitor/control
- Multiple sources of hazards to interlock
- Interface to many other complex systems.

Those factors combined altogether pose a design challenge for PPS, which must be a distributed global safety system to meet those challenges.

SLAC's 2-mile long Linac was built in 1960s, and it is the longest linear accelerator in the world. Nowadays, this Linac are serving three different beam programs: LCLS completed in 2009, FACET-II completed in 2020, and the superconducting (SC) LCLS-II, which is under construction and will start operation in early 2021.

Figure 1 shows the locations of three beam programs, each taking up one third of Linac for beam acceleration:

- LCLS-II SC beam: Linac West (Sector 00- Sector 09)
- FACET-II: Linac Middle (Sector 10- Sector 20)
- LCLS-I Cu beam: Linac East (Sector 21- Sector 29)

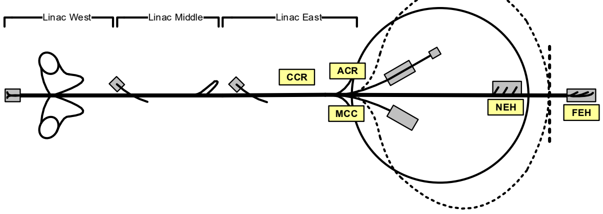

Figure 1: Layout of SLAC's Beam Lines.

* The author currently works for Underwriters Laboratories as a Functional Safety Staff Engineer,
† Feng.Tao@ul.com.

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR04

The FACET-II beam will not pass Sector 20, but LCLS-I Cu beam and LCLS-II SC beam will enter Beam Switch Yard (BSY), where different routes and destinations of the beam are selected. Downstream to BSY is the Beam Transport Hall (BTH) and undulator complex, where electron beam wiggling through undulators to generate soft x-ray or hard x-ray. The x-ray laser travels across FEE-EBD to reach experiment hutches in Near Experiment Hall (NEH) and Far Experiment Hall (FEH).

To cover such a large facility, PPS needs to be distributed to effectively control/monitor field devices. Legacy systems use long haul trunk cables to connect field devices to control racks and control rooms, which is expensive and lack of flexibility. Just cite one example here: -48VDC was used in legacy systems to compensate voltage drop over a long distance. To modernize the system, we have used fiber-optic to create a dedicated ring topology network for all safety systems. Ethernet cables are been used as the infrastructure to minimize copper cable usage and to connect subsystems.

As each beam program has its own gun and acceleration RF devices, at each location, the PPS should be "aware" of not only the local prompt radiation hazards, but also hazards from all sources. Therefore, information exchange between different beam program is unavoidable.

At SLAC, attributes that distinguish PPS from other safety systems are strict configuration control and annual proof testing (bi-annual for some testing facilities onsite). Those are also the reasons that PPS are being trusted and being requested by many other systems (through interface signals) as a reliable means to bring the system into the safe state.

DIFFERENT LAYERS OF PPS

As a complex global safety system, PPS needs to meet the needs from different beam programs. It is a loosely connected system that has multiple layers and multiple installations. As a distributed system, it contains five layers:

- Global Beam Programs
- Beam Switching and Permit System (BSP)
- Zone Access Control
- Zone Safety Interlock Control
- Sensor/Shutoff Subsystems

Each layer includes functions that are important to maintain personnel safety, and they are all part of the hazard mitigation scheme. In this section, we will describe functionality of each layer in details.

Global Beam Program

There are three global PPS systems, corresponding to each beam program, and are conveniently named by their locations: e.g., Linac West Global PPS, Linac Middle Global PPS, and Linac East Global PPS. Each global PPS has separate top level safety controllers, to maintain the separation from other beam programs. This separation is especially important as each program have its own operation and maintenance schedule. Shutoff of one beam program should have no (or minimal) impacts to the operation of other beam programs.

Beam Switching and Permit System (BSP)

In the BSY region, there are a group of 5 sets safety controllers that are responsible for beam switching and stopper permit/control. This system determines if both hard x-ray and soft x-ray beamline configurations are correct, and issues permits for stoppers, magnets, kickers and septum in BSY. A detailed BSY beamline layout with stoppers configuration is shown in Figure 2.

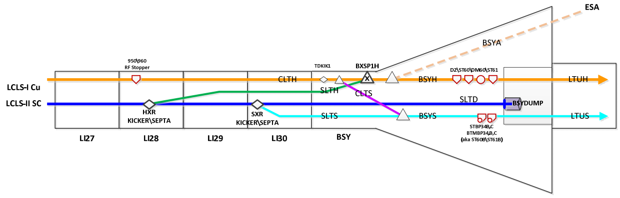

Figure 2: BSY Layout and Beam Stoppers.

As majority of stoppers in BSY cannot hold up to the powerful beam indefinitely, this system needs to work with upper layer control, to shut off beam before damages are made.

Zone Access Control

Each individual PPS zone has an access control system responsible for non-SIL rated protection functions, such as zone search procedure, trapped key release, magnetic door lock, area access control, audio/visual warning etc. Although those functions are not deemed safety critical, they do provide some level of protection, and will be given credit in Layer of Protection Analysis (LOPA) [5]. They are part of the engineering control that reduces risk and lowers the SIL required for safety functions inside safety PLCs.

Other functions contained in access control are state machine for access states, communication with EPICS, sensors checking and maintenance (such as BTM fill/vent routines). For cybersecurity reason, all safety controllers do not directly connect to EPICS, but use access controllers as the bridge by connecting to those controllers using fieldbus modules. This configuration is to provide an air gap for safety controllers to prevent potential cyber-attacks. Access control PLC is also responsible for driving field devices such as E-Stop LEDs and Emergency-Exit buzzers to make safety control portion compact.

Zone Safety Interlock Control

Zone safety interlock functions are contained in zone safety PLCs. At SLAC, PPS always uses dual redundant architecture, so there are identical Chain A and Chain B safety PLCs for each PPS zone. In *normal* mode, faulted input to Chain A will force both Chain A and Chain B controllers to turn off outputs; while in *test* mode, this cross-interlock between two chains is being turned off to facilitate testing, making it easier to identify faulty components on a single chain.

Sensor and Shutoff Subsystems

Traditionally those subsystems are customized built chasses with a soldered relay assembly inside. They have

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-WEBR04

been modernized by using safety PLCs to lower lifecycle cost and to increase reliability. Typical sensors used by PPS are Burn Through Monitor (BTM), Beam Shutoff Ion Chamber (BSOIC) and Residual Dose Monitor (RDM). Shutoff devices usually are relays or contactors to disconnect power supply to radiation generating devices, or solenoid valves to insert beam stoppers into beamline. Those devices are permitted by PPS logic at upper layer, and they also need to provide reliable status to the upper layer for escalated shutoff or setting access to the accelerator.

Historically, outputs of BTM and BSOIC chasses are connected to a 17mA current loop, worked as a logic “AND” gate to sum up all discrete subsystems’ “OK/Fault” status within a given area. This current loop is called “Secure Loop” as it carries the information on whether a given area is secured to turn on hazards. For status of shutoff devices, similar current loops called “Set Entry” loops were built to sum up radiation generation devices’ OFF status in a given area, to indicate if the area is safe to access.

During upgrade, some current loop chasses have been eliminated by directly wiring individual input of the loop to a safety controller, which functions the same but have more diagnostics and is more reliable.

There are no clearly established guidelines on how to define and divide the boundary of PPS subsystems. It involves many project decisions when the project was planned. Global PPS uses Siemens distributed safety PLC family of products, such as S7-315F and the newer S7-1515F. The same fail-safe CPUs are used in access control PLC systems, but I/O modules in those systems are simply not fail-safe. Allen-Bradley ControlLogix is also being used in access control PLC in some PPS zones. Those two layers of PPS use large-size PLCs suitable for distributed applications. On the other hand, zone safety and sensor/shutoff subsystems are usually compact and use Pilz PNOZMulti safety PLCs.

Functional Block Diagram of Linac West PPS

For better understanding of different layers of PPS, a functional block diagram of the Linac West is given in Figure 3:

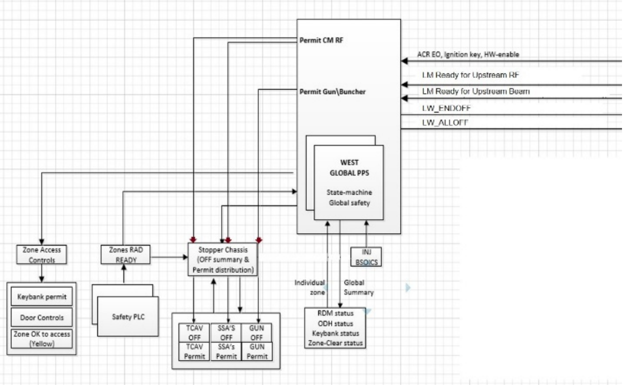

Figure 3: Linac West Functional Block Diagram.

Linac West is under construction for the LCLS-II project. The 10 sectors of Linac have been divided into three PPS zones: Inj-S00 for the injector, S01-S07 is the superconducting RF section, and S08-S10 will host normal conducting RF, as part of the LCLS-II-HE (High Energy) project scope, to boost electron beam energy from 4GeV to 8GeV. Each PPS zone has one dedicated access control PLC and two zone safety PLCs (Chain A/B), with the exception for S01-S07 zone. To effectively control such a large area over 700 meters, both access control and zone safety control use distributed architecture to make the field wiring manageable. To be specific, the zone access control using S7-1515F controller with 2 remote I/O drops, so that each I/O drop covers no more than 3 sectors. Zone safety control uses “SafeLink” communication modules to connect one “master” Pilz safety PLC with two “slave” PLCs, although the communication protocol itself is “peer-to-peer”.

The West Global PLC is another distributed safety system at the top level to connect other distributed systems at lower levels. It will provide permits to devices that can generate radiation hazards when following conditions are met:

- Zone safety controllers in all 3 PPS zones indicate the entire Linac West is searched and secured
- Interface signal from Linac Middle indicates the downstream area (from Sector 10 down to BTH) is “READY” (searched and secured)
- Beam containment subsystems (BTM, BSOIC, RDM (Residual Dose Monitor)) indicate beam are contained and those subsystems are working properly.
- Interface signals from other safety systems such as ODH (Oxygen Deficiency Hazard), BCS (Beam Containment System) indicate no need for PPS to shut off the accelerator for them.

Linac West Global PPS issues permit signals to stopper control PLCs, which enable operators to turn on circuit breakers that provide power to 280 Solid State Amplifiers (SSAs) and traditional modulators (for LCLS-II-HE). Those SSAs are grouped into 20 facilities Interface Switches (IS) panels, using SIL rated 600A circuit breakers to shut off power supply to a group of SSAs reliably.

SAFETY INTEGRITY ANALYSIS

In a safety system design, the SIL or PL of a safety function is determined by risk assessment. For a standard machinery safety function, inputs, logic solver and final elements are all local devices. But this is not the case for large accelerator safety functions, making the analysis very tricky. In this section, we will use “Emergency Stop” function at different locations to demonstrate how different layers of PPS control work coordinately and affect the integrity of the overall function. Here the E-Stop function is chosen as the example because it is the most common safety function that required to achieve SIL 2 or PLd integrity performance by many safety standards.

Photon Experiment Area

For photon experiment hutches in NEH and FEH, PPS is relatively simple, and its settings are almost identical to those of standard machinery safety. Each experiment hutch is an isolated room with dedicated stopper for that beamline. In this system, safety inputs such as E-Stop, microswitches installed on the perimeter boundary, are interlocked to the beam stopper using safety PLCs. The overall system is dual-redundant as well, with diagnostic test pulses applied to PLC's inputs whenever possible.

The E-Stop function in this area is affected by three PPS layers. The bottom layer is the hutch safety controller, which handles safety interlock logic; and the layer above is the access control PLC, which provides additional protection layers related to personnel safety. This helps to reduce the SIL required for those safety functions in the zone safety controllers [5]. For example, the perimeter door magnetic lock function will reduce the probability of challenging door microswitch interlock from outside of the hutch. The audio/visual warning function, which alerts people to leave the area also reduces the need of people left behind pressing E-Stop to initiate emergency shutdown.

In addition to those controllers, there is a diagnostic function implemented by upstream *PPS beam switching and permit system (BSP)*, which will insert the upstream beam stoppers in case the photon beam stopper fails to move in for any reason. This is achieved via a 17mA current loop named "LCLS Secure Loop", which passes through each photon beam stopper chassis in NEH. If any beam stopper has no permit and is not in "IN" position, relay logic inside the chassis will break the current loop. The current loop receiver will repeat the status and feed into BSP controllers to insert upstream stopper(s) in BSY. This function shall be treated as a diagnostic function applied to the output subsystem, photon stopper in this case, to provide a secondary shutoff path in case of the primary path failure. The safety function's reliability block diagram (RBD) is shown in Figure 4. As the overall system is dual-redundant, each block does contain symmetric components on two parallel paths.

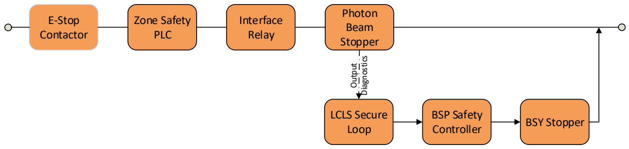

Figure 4: RBD for E-Stop Function.

In a previous paper by the author [6], the similar case has been studied, and the PFD value was calculated. Readers can compare the difference between two diagrams. In Figure 4, due to the presence of the additional diagnostic shutoff path, the safety function has a higher safety integrity. It is noticed that add-on diagnostics is a common strategy used in system design to improve system integrity. Such as using a Watch Dog Timer (WDT) as a secondary shutoff path, which can effectively upgrade the implementation from Category 1 to Category 2 for a machinery safety function [4]. But as on the primary shutoff path, dual redundancy should already provide sufficient reliability from electronics perspective; adding a secondary path may only be justified if the stopper has a substantial percentage of non-electrical failures from its failure mode analysis.

PPS in BTH and FEE-EBD

These sections are upstream to photon experiment area but downstream to BSY. There are no dedicated beam stoppers, so if any input to the zone safety controller faulted, the controller will de-energize its output to directly break the "LCLS Secure Loop". As stated before, this will cause the BSP to remove the BSY beam stopper permit, causing the stopper automatically move in. Therefore, in this case, zone PPS safety controller and BSP safety controller combined to be the logic solver during the safety integrity verification. The reliability block diagram in this case is shown in Figure 5 below:

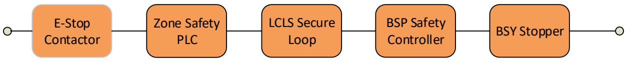

Figure 5: RBD for E-Stop Function at FEE-EBD and BTH.

In the figure above, the logic solver portion includes two or more safety PLCs (zone safety and BSP safety), LCLS Secure loop transmitter/receiver. Each Pilz safety PLC will add up about 150ms into the function's response time, so if the shutoff action needs to propagate further upstream to the Linac area and involves multiple subsystems, the overall response time should be verified against requirements.

Comparing Figure 4 and Figure 5, for the same E-Stop function, due to the different system configuration, the reliability performance differs, and the E-Stop function in photon area is more reliable.

PPS in Linac and BSY

The upstream LCLS-II SC beam has a bypass beamline all the way from Sector 10 to Sector 29 and have almost the same destination as LCLS-I beam. Therefore, once it is turned on, its radiation effects will affect downstream all the way to BTH. FACET-II does not have bypass line, but its radiation is dangerous to people in the LCLS-I Linac accelerator tunnel as well.

The impacts of such a layout are two folders:

- The safety functions triggered in a downstream area also include turning off upstream radiation sources.
- To turn on radiation generating devices in the upstream, all downstream areas need to provide enable signals to indicate it is safe to do so.

In both cases, the block diagram of the safety function will become more complex than usual, as more devices are showing up on the shutoff path, makes it even harder to meet the reliability requirements.

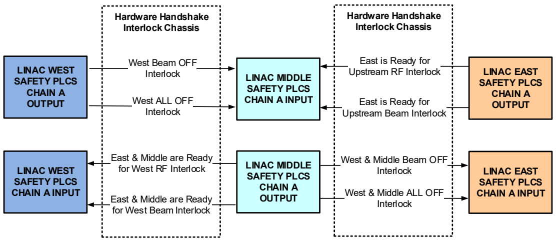
Hardware Handshake Interlock Chassis
Hardware Handshake Interlock Chassis
LINAC WEST SAFETY PLCS CHAIN A OUTPUT
West Beam OFF Interlock
West ALL OFF Interlock
LINAC MIDDLE SAFETY PLCS CHAIN A INPUT
East is Ready for Upstream RF Interlock
East is Ready for Upstream Beam Interlock
LINAC EAST SAFETY PLCS CHAIN A OUTPUT
LINAC WEST SAFETY PLCS CHAIN A INPUT
East & Middle are Ready for West RF Interlock
East & Middle are Ready for West Beam Interlock
LINAC MIDDLE SAFETY PLCS CHAIN A OUTPUT
West & Middle Beam OFF Interlock
West & Middle ALL OFF Interlock
LINAC EAST SAFETY PLCS CHAIN A INPUT

Figure 6: Interface Signals between Beam Programs.

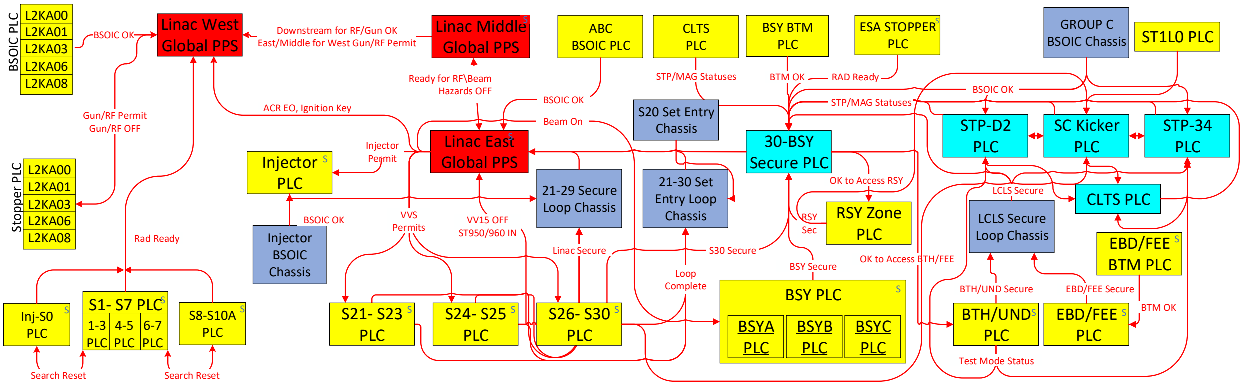

Figure 7: Signal Interfaces among PPS Safety Controllers and Safety Critical Electronics.

Figure 6 shows the interface signals among three global PPS systems. It should be noted that a beam program may have different modes to turn on beam, or RF or both. The hazard level is different for each operation mode.

As there are over 50 sets of safety controllers and safety critical electronic chasses across SLAC. There is a need to identify how those safety-critical signals flow through those subsystems for a better understanding. For SLAC's PPS at electron areas, a completed signal interface diagram is shown in Figure 7, where a letter "S" on the top-right corner of the PLC indicates it has a supervisory (access control) PLC.

This diagram is useful when to determine the safety shutoff action sequence, e.g., how the safety interlock broadcasts from one controller to another.

This diagram is also vital in interface control and test planning. For such a large system, PPS's annual site acceptance tests (SAT) need to be carried out by area and in multiple stages. Every interface signal in the diagram needs to be verified seamlessly on both ends to ensure the overall system functionality is intact.

Reading from Figure 7, we can identify the most challenging scenario for PPS safety interlock, e.g., E-Stop activation in BSY region. In this area, zone safety control also adopts the "master-slave" configuration. So if any E-Stop button wired to a "slave" safety controller is pressed, the shutoff actions will take the following sequence:

1. BSY zone safety "slave" PLC
2. BSY zone safety "master" PLC
3. 30-BSY Secure PLC
4. Linac East Global PPS
5. Linac Middle Global PPS
6. Linac West Global PPS
7. 5 Stopper PLCs (L2KA00/01/03/06/08)

For this scenario, there are 11 safety PLCs shown up in the reliability block diagram. Since all those PLCs are serially connected on the RBD, each PLC's PFH (Probability of Failure per Hour) value will add up to the PFH of the overall function.

If more than one beam program is running, then there are more controllers get involved in the shutoff action. For example, assume that both LCLS-I and LCLS-II beams are running and need to be shut off, then Linac East Global PLC also needs to remove permits sent to four zone safety controllers:

- Injector PLC (at Sector 20)
- S21- S23 PLC
- S24- S25 PLC
- S26- S30 PLC

In this extreme case, there are 15 safety controllers in total must function correctly to shut off all radiation hazards.

The following table from ISO 13849 [4] (Table 11) shows the relationship between number of subsystems, lowest PL and the overall system PL. Though the calculation is based on the average reliability value of each PL, but the message is clear: reliability lowers when more subsystems are connected in a simplex configuration.

Table 1: Calculation of PL for Series Alignment of SRP/CS

PL_{low}	N_{low}	➡	PL
a	>3	➡	None, not allowed
	≤3		a
b	>2	➡	a
	≤2		b
c	>2	➡	b
	≤2		c
d	>3	➡	c
	≤3		d
e	>3	➡	d
	≤3		e

Due to the large number of subsystems involved, in our case, it would be a challenge, if not impossible, for the E-Stop function to achieve SIL 2 integrity level!

Solutions for Meeting Integrity Requirements

There are several possible solutions to improve PPS's integrity:

- Add shielding to the boundary between Sector 9 and Sector 10 to eliminate the need to shut off upstream radiation source, thus simplifying the safety function.
- Re-define the shutoff function, make a clear distinction between interlock to gun and RF. Shutting off gun is more effective than shutting off RF, as RF alone only generates dark current, which is less dangerous than the accelerated beam.
- Simplify system architecture, reduce number of the PLC that re-routes the shutoff command. Safety relays and hardwiring may improve the safety integrity than safety PLCs.
- Add additional shutoff path.

For each option, there are some corresponding concerns as well:

- Adding additional shielding is expensive for the project, though this is the safest approach, and is consistent with the "inherently safe" principle.
- Before re-define the function, detailed study needs to be performed to narrow down the scope of shutoff, reduce the number of safety controllers on the shutoff path.
- Replacing PLCs with relays and cables is a reversal of the trend for more functional integration, modularity, and configurability. This will make the system less flexible and difficult to upgrade later.
- A good candidate for the shutoff path is to use Beam Containment System (BCS), which is another global safety system at SLAC [6]. This system is an independent system using different mechanisms to shut off the beam. Currently it is only being requested by PPS for a fast shutoff when BSY beam stoppers are in motion, so as to avoid the damage caused by beam hitting sides of stoppers. Using BCS as the secondary shutoff path needs additional work to connect two systems, but as there is no common cause factor between primary/secondary shutoff, the PPS's safety integrity can definitely meet the SIL 2 or PLd performance requirement.

Reviewing all options above, the best solution is to use BCS as the secondary shutoff path. The tie-in point from PPS to BCS should be close to the BSY, to maximize the performance.

CONCLUSION

SLAC's PPS employs a complex multilayer distributed architecture to protect personnel from prompt radiation hazards. This architecture is far more complex than the standard ones from ISO 13849 and IEC 62061 standards. In this architecture, there are more modular control systems deployed at different levels to meet the operation needs. However, this complexity inevitably lowers the overall system's integrity, which need to be considered and verified during the system implementation. For a successful safety system design, both functional requirements and integrity requirements must be met.

ACKNOWLEDGEMENTS

I would like to thank my colleagues in the Safety System Department: Enzo Carrone, James Murphy and Keith Belt. I deeply appreciate their supports during my ten years of adventure at SLAC! Accelerator Safety Officer Paul Miller and Michael Stanek, accelerator physicist John Schmerge and Jerry Yocky provided valuable information during discussions and design reviews.

REFERENCES

[1] D. Macdonald, "Practical Machinery Safety", Burlington, MA, USA: Newnes, 2004.

[2] IEC 61508, "Functional Safety of Electrical /Electronic /Programmable Electronic Safety-related Systems", 2nd Ed, IEC, 2010.

[3] IEC 62061, "Safety of Machinery- Functional Safety of Safety-related Electrical, Electronic and Programmable Electronic Control Systems", IEC, 2005.

[4] ISO 13849, "Safety of Machinery – Safety-related Parts of Control Systems", ISO, 2006.

[5] F. Tao, J. Murphy, "Applying Layer of Protection Analysis (LOPA) to Accelerator Safety Systems Design," in *Proc. 16th Int. Conf. on Accelerator and Large Experimental Physics Control Systems (ICALEPCS'17)*, Barcelona, Spain, Oct. 2017, paper THCPA03, pp. 1217-1220, doi:10.18429/JACoW-ICALEPCS2017-THCPA03

[6] F. Tao, E. Carrone, J. Murphy, and K. Turner "Safety Integrity Level (SIL) Verification for SLAC Radiation Safety Systems," in *Proc. 15th Int. Conf. on Accelerator and Large Experimental Physics Control Systems (ICALEPCS'15)*, Melbourne, Australia, Oct. 2015, paper TUC3O07, pp. 561-564, doi:10.18429/JACoW-ICALEPCS2015-TUC3O07