Safegurading Large Particle Accelerator Research Facility - A Multilayer Distributed Control Architecture

Feng Tao

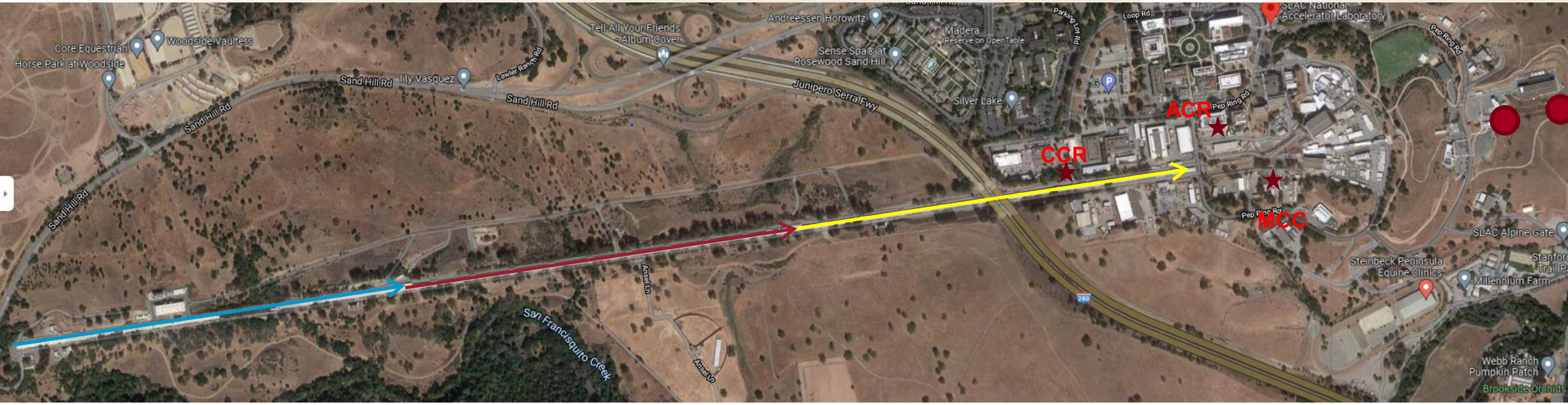
San Francisco, USA

Oct. 20, 2021

Outline

- SLAC's Accelerator and Safety Systems
- Machinery Safety vs. Accelerator Safety
- PPS: Functions and Architecture
- Functional Safety of PPS
- Summary

SLAC National Accelerator Laboratory



3 Beam Programs:

- Linac East: LCLS-I, completed in 2009
- Linac Middle: FACET-II, completed in 2019
- Linac West: LCLS-II, under construction

NEH & FEH

3 Soft X-Ray Hutches

5 Hard X-Ray Hutches

Control Centers:

1st: CCR

2nd: MCC

Current: ACR

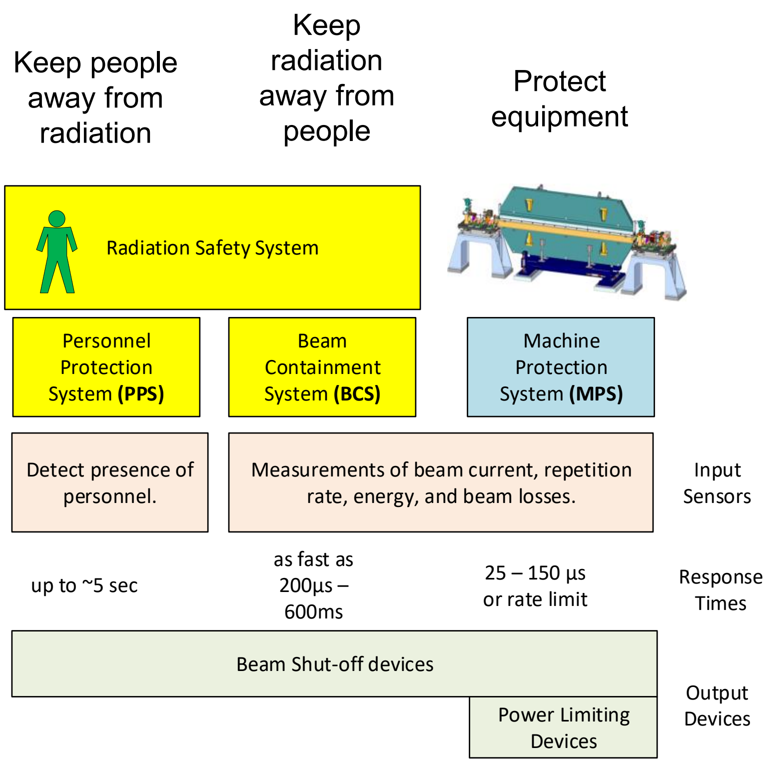
Radiation Safety Systems (RSS) in SLAC

RSS includes:

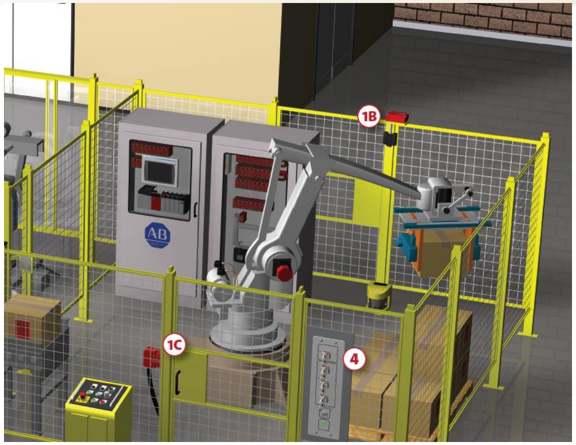
- Personnel Protection System (PPS)
- Beam Containment System (BCS)

- PPS: one of the earliest safety systems
- Hard shutoff actions:
  - Remove power supply to gun/RF
  - Insert beam stoppers
  - Slow response that affects beam stopper design

- BCS: created later to detect beam loss and protect PPS devices
- Shadows many protection functions in MPS, use similar techniques
- Soft shutoff actions:
  - Close injector laser shutter
  - Stop Gun RF acceleration
  - Switch Accelerator RF to standby
  - Fast response, challenge on reliable electronics design



Machine Safety vs. Accelerator PPS



* from Rockwell Automation

Industrial machinery safety:

Keep people away from hazard (moving parts)

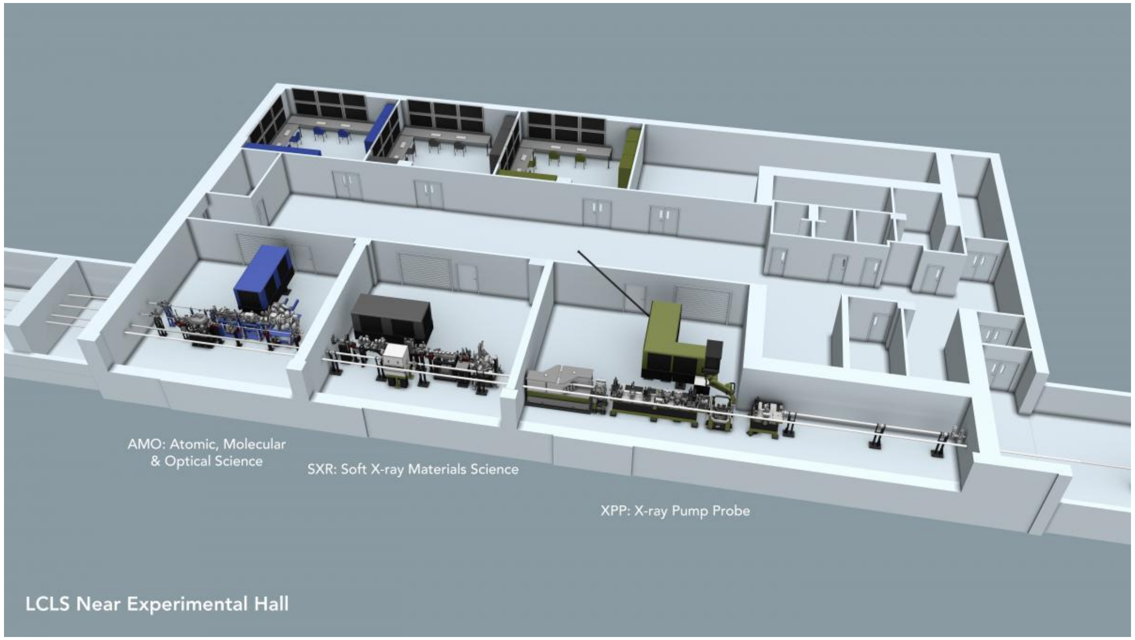
Devices used:

- Microswitch
- E-stop
- Trapped key
- Locking mechanism
- Laser scanner
- Safety relay/PLC

SLAC's PPS:

Keep people away from radiation hazards (electron/laser beam)

- Search a large area to get it secured
- If other areas are secured, and beam is contained, issue permit for radiation hazards and beam stoppers
- Any security violation or beam lost containment will shutoff beam operation
- Hazards may come from upstream, not necessarily local
- Need to take actions for downstream



Machinery Functional Safety

SLAC

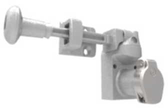
Common Functional Safety Standards Used at SLAC:

- **IEC 61508**, Functional Safety of E/E/PE Systems
- **IEC 62061**, Functional Safety of E/E/PE Systems (for machinery)
- **ISO 13849-1**, Safety-Related Parts of Control Systems (for machinery)
- **IEC 61511**, Functional Safety of E/E/PE Systems (for process industry)

Machinery Safety Certified Products Used Onsite:



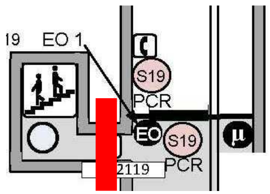


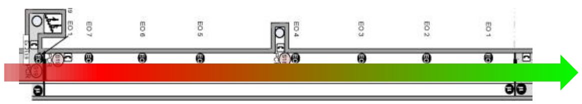




SLAC's PPS Design Process:

- Radiation hazards are high: need 3 independent layers for protection
- Access control functions are given credits for providing one protection layer
- Safety PLC need to provide SIL 2 safety interlocks
- Radiation physicists calculate the radiation does potential, and use effective dose rate for classification
  - Use Level 1/2/3 Category to describe functions required by PPS
  - High risk access point has higher field device redundancy
  - High level of redundancy will result in lower common cause factors

Typical PPS Sequence





1) Control access by restricting permissions.

2) Secure the perimeter from entry and monitor for breach.

3) Search area for occupants and verify clear.

4) Issue warnings and interrupt readiness if area still occupied.

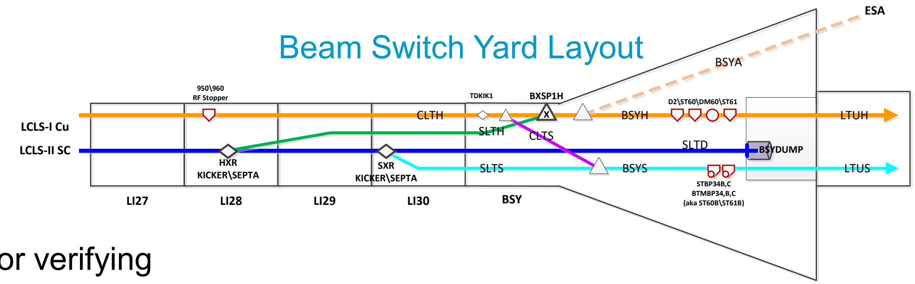
5) Permit prompt radiation/RF sources when safe to do so (Global PPS).

6) Interrupt beam if security violated or radiation detected outside envelope (Global PPS).

PPS: Multi-Layer Distributed System

SLAC's PPS is a distributed system, consists of:

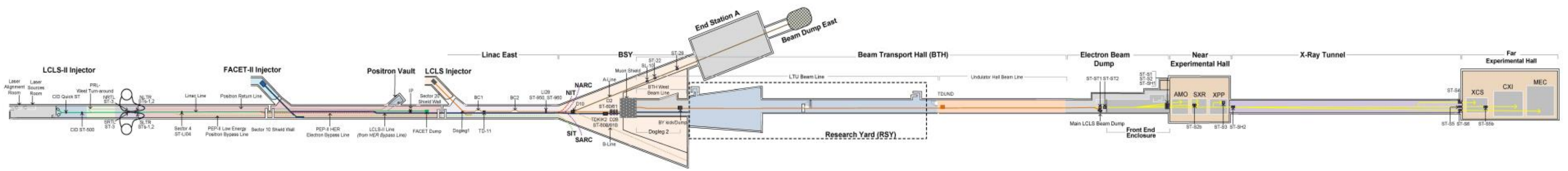
- 15+ access controllers, 100+ safety controllers, footprints are everywhere
- Five Layers of architecture:
  - Beam Program
    - Each beam program has a dedicated global PPS



  - Beam Switching and Permit
    - 5 sets of redundant safety controller responsible for verifying beamline configuration, beam stopper, magnets, kicker/septum controller
    - Re-route the shutoff request to upper layer if additional shutoff needed
  - Access Control
    - Access control functions: zone search procedure, trapped key release, zone access control, audio/visual warning, EPICS communication, communication to lower layer safety controllers, etc.
    - The only layer implemented with non-safety PLC,
  - Zone Safety Control
    - Interlock to area security violation, loss of beam containment, response to other systems' request
  - Sensor/Shutoff Subsystem
    - Modernize electronics, using safety PLC to replace old relay-based chasses
    - Sensor: Burn Through Monitor (BTM), Beam Shutoff Ion Chamber (BSOIC), Residual Dose Monitor (RDM)
    - Shutoff: Stopper Chassis, for beam stopper/magnet/RF power supply control

PPS: Implementation

All safety system PLCs are connected over an isolated dedicated network with ring topology



Beam Program:
- Siemens S7-300 distributed safety PLC (for LM, LE @ CCR)
- Siemens S7-1500 distributed safety PLC (for LW @ Sector 8)
- Hardwired connections to EPICS

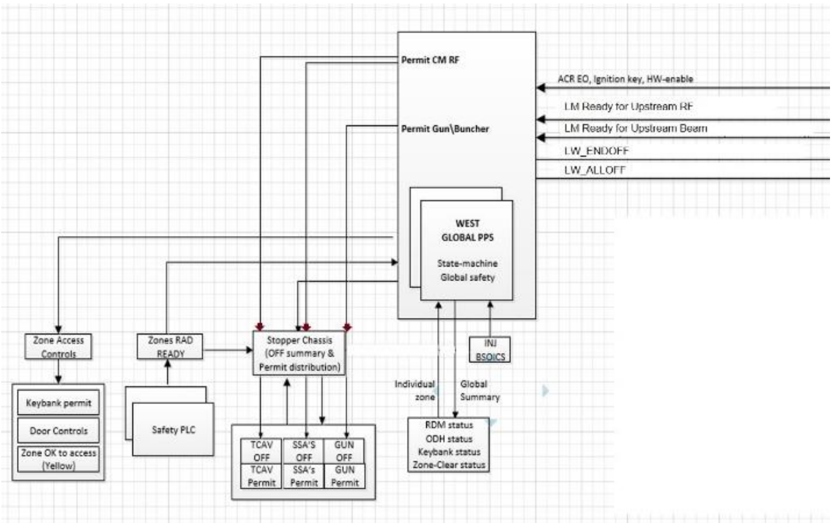
Beam Switching and Permit System (BSP):
- 5 sets of redundant Pilz safety controller @ MCC
- Connected to EPICS through fieldbus module

Access Control
- Mostly are localized system except for S1-S7, BSY
- Allen-Bradley Controllogix 5562, S7-300, S7-1500
- Connected to EPICS through soft IOC

Zone Safety Control
- Redundant Pilz safety PLC
- Connected to Access Control PLC through fieldbus module

Sensor/Shutoff Subsystem
- Pilz safety PLC
- Connected to Access Control PLC through fieldbus module

Linac West (LCLS-II) Global PPS Functional Diagram

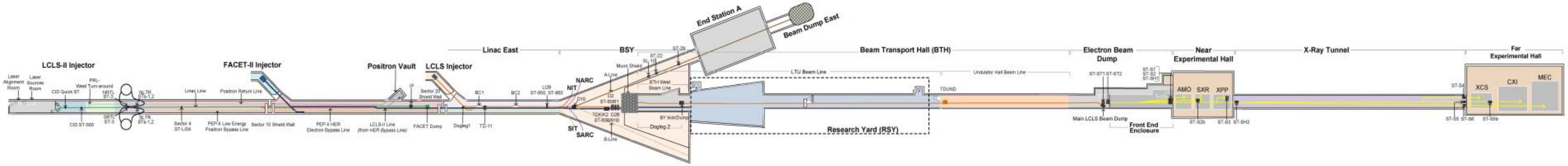


Challenges on PPS Functional Safety

Compared to industrial machinery safety, SLAC's PPS:

- Large geographic distribution
- Multiple sources of hazards
- Modularity increases number of subsystems
- Complex subsystem interconnections on safety functions
- One safety function may cross multiple subsystems
- Safety integrity is affected

- Examine the E-stop function at different locations of accelerator
- E-stop function needs to be SIL 2 or PL d by many safety standards!

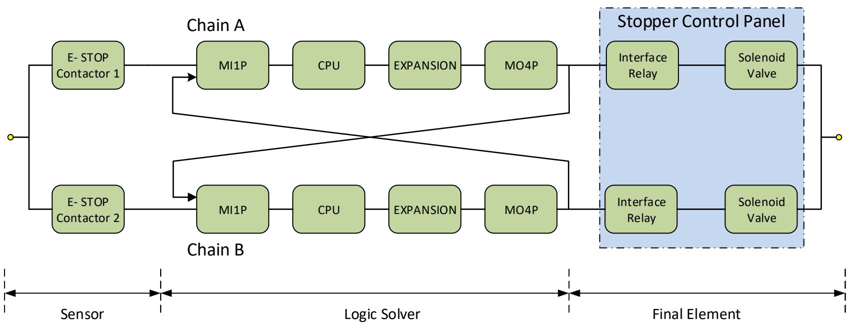


E-Stop Function: Reliability Block Diagrams

SLAC

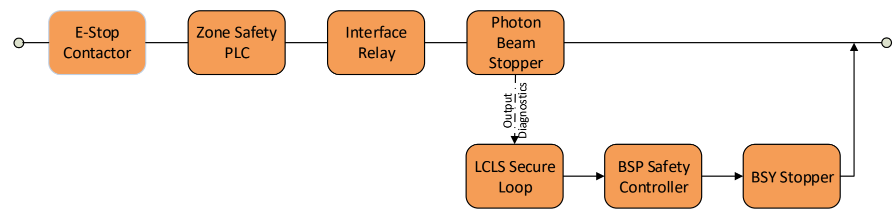
E-Stop in NEH/FEH:

- Dual Redundant configuration
- Equivalent to Cat. 4, highest from ISO13849
- Easily meet SIL 2 or PLd



E-Stop in NEH: (with shutoff escalation)

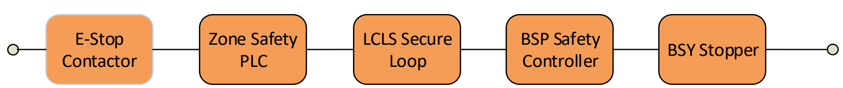
- Upstream stopper will insert
- Additional diagnostics with another shutoff path on standby



In FEH: (with shutoff escalation)

- Another photon stopper in XRT will insert

E-Stop in BTH

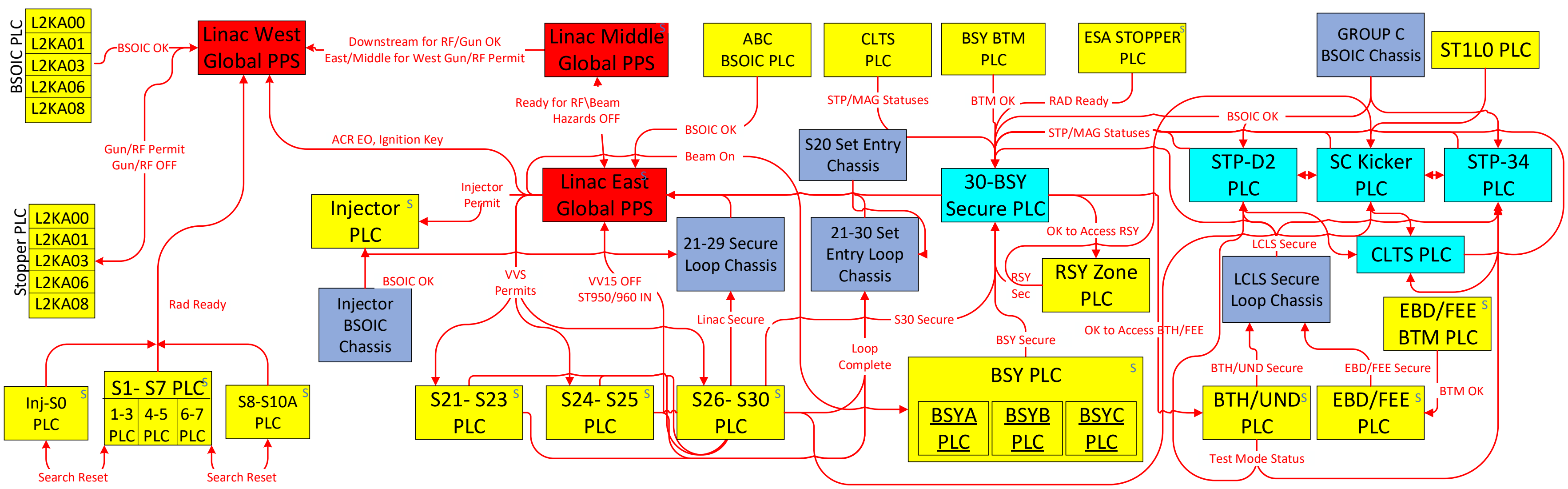


E-Stop in BSY:

- To shut off LCLS-I beam:
  - ➢ 8 safety PLCs in shutoff path
- To shut off LCLS-II beam:
  - ➢ 11 safety PLCs in shutoff path
- To shut off both LCLS-I/II beam:
  - ➢ 15 safety PLCs in shutoff path

Accelerator PPS Signal Flowchart

SLAC



How we use this diagram

- Identify critical PPS interface for configuration control
- Make sure interface signals been checked “end-to-end” during annual SAT
- Estimate the PPS response time at each location
- Determine the PPS shutoff sequence of event at each location

System Architecture and Function's Integrity

PPS

- Individual PLC adopts one of the best architecture (Cat. 4)
- But too many PLCs are on the single shutoff path
- ***May not*** be able to meet SIL 2

BCS

- has a flat architecture
- Single distributed PLC for the entire LCLS-II beamline
- Code's change control is an issue

Potential solutions for PPS

- Re-define the safety function
- Add more shielding
- Architecture change, make it as flat as BCS
- Add an additional shutoff path
  - BCS is a good candidate
  - Has almost no common cause with BCS
  - Need to tie in at BSY, close to E-Stop inputs

ISO 13849-1:
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

Summary

- Compared machinery safety with PPS
- Discussed PPS's function
- Described the multi-layer distributed architecture
  - Independent, Modular, Scalable, Configuration control
  - SF crosses multiple layers & controllers
- E-Stop example on functional safety challenge
- Potential solutions to improve integrity