ICALEPCS2017
Barcelona · Spain, October 8-13 · Palau de Congressos de Catalunya
16th International Conference on Accelerator and Large Experimental Physics Control Systems

Applying Layer of Protection Analysis (LOPA) to Accelerator Safety Systems Design

Feng Tao

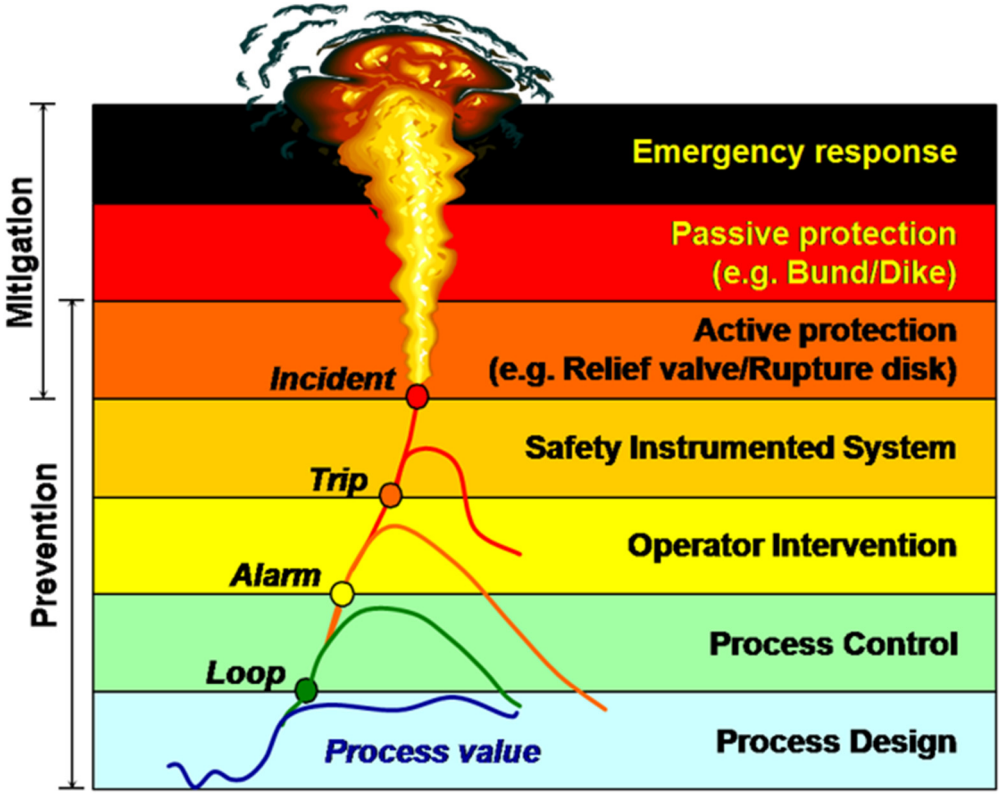
SLAC NATIONAL ACCELERATOR LABORATORY
U.S. DEPARTMENT OF ENERGY | Office of Science
LELAND STANFORD JUNIOR UNIVERSITY 1891

Outline

- LOPA Methodology
- LCLS-II Oxygen Deficiency Monitoring (ODM)
- LCLS Personnel Protection System (PPS)
- LCLS Beam Containment System (BCS)
- Conclusion

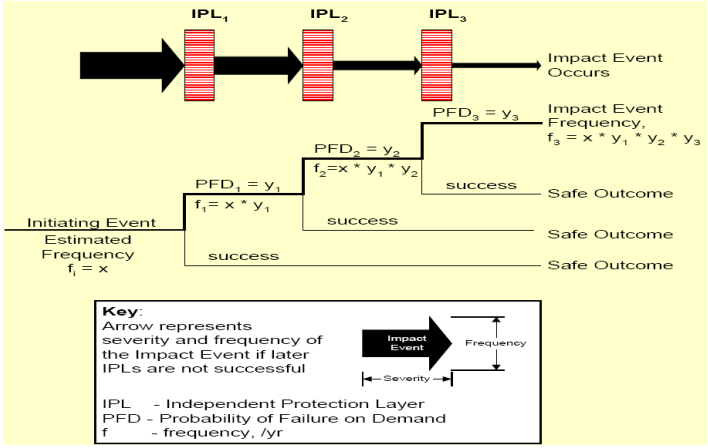
LOPA: Basics

- A semi-quantitative risk assessment method used by process industry for SIL assignment
- Start after risks are identified in the consequence-cause pair
- Carefully evaluate the initiating events, enabling conditions and condition modifiers,



LOPA: Simple Math

- Identify existing protection layers, evaluate if they are Independent Protection Layers (IPL)
  - Core Attributes: independence, functionality, integrity, reliability, auditability, access security, management of change
  - Prevention IPL: lower the frequency of the event
  - Mitigation IPL: lessen the severity of the consequence



Original Risk: $R = \sum_{i=1}^{n} f_i C_i$

Risk Prevention: $R = \sum_{i=1}^{n} (f_i \prod_{j=1}^{m} PFD_i^j) C_i$

Risk Mitigation: $R = \sum_{i=1}^{n} f_i \{C_i PFD_i + \overline{C}_i (1 - PFD_i)\}$

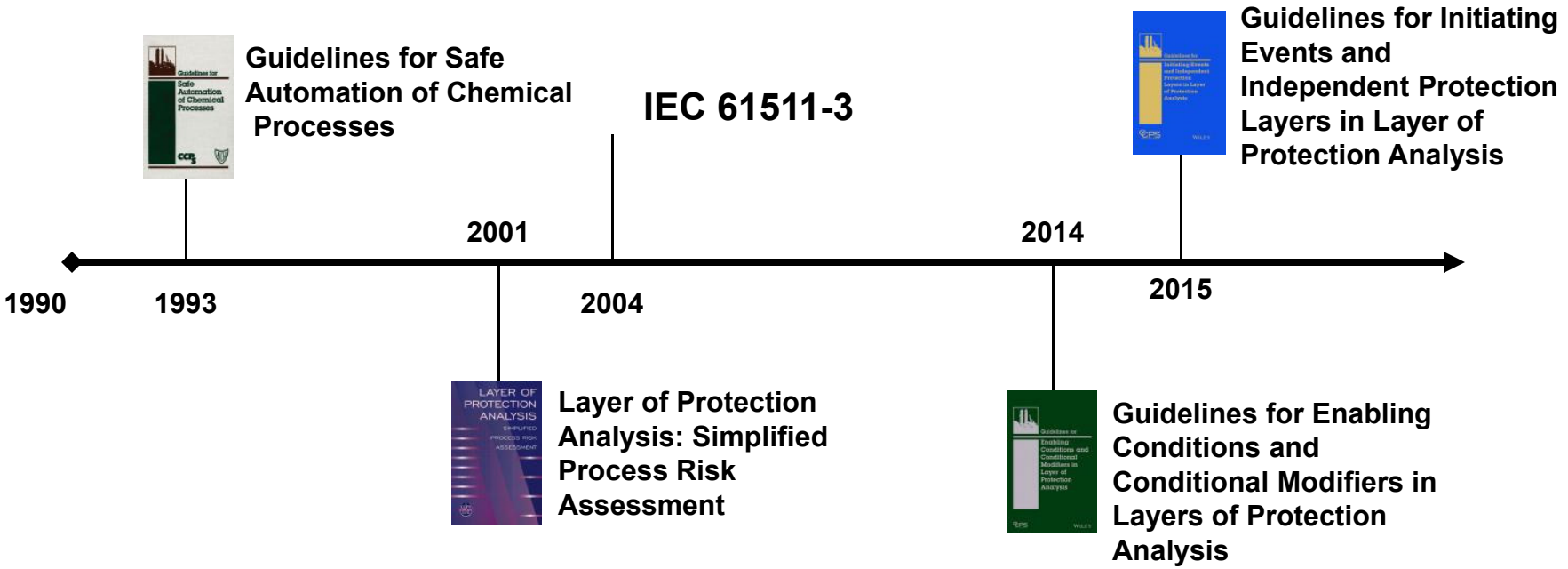
SIL	Average Probability of Failure on Demand	Risk Reduction Factor	Availability (%)
1	10^{-1} to 10^{-2}	10 – 100	90 - 99
2	10^{-2} to 10^{-3}	100 - 1,000	99 - 99.9
3	10^{-3} to 10^{-4}	1,000 – 10,000	99.9 – 99.99

Why LOPA

- Accelerator safety systems are more complex compared to machinery safeguarding
- In addition to safety systems, other risk reduction measures are deployed: alarms, periodic checkout, multiple layers of control and protection
- Radiation Physicists use a “descriptive” approach to mandate requirements for Radiation Safety Systems (PPS and BCS)
- Radiation Safety Systems are required to be: redundant, self-checking, fail-safe, etc.
- If classified as SIL rated, additional work to comply with standard-compliance development procedure
  - FMEDA, structural constraints, SFF, QA

Evolution of LOPA

- From concept to widely adopted



LCLS-II Oxygen Deficiency Monitoring

- LCLS-II will introduce significant cryogenic hazards
- An Oxygen Deficiency Monitoring (ODM) system will be added to the credited safety system list
- Risk Criteria: fatality rate per area

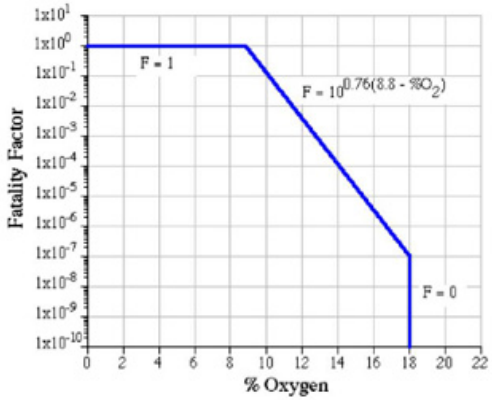
$$\emptyset = \sum_{i=1}^{n} P_i F_i$$

where

$\emptyset$ = the ODH fatality rate (per hour)

P_i = the expected rate of the i type of event (per hour)

F_i = the fatality factor for the i type of event



Using results from FMEA to get the list of event, frequency and consequence

- SLAC's tolerable risk threshold: fatality rate 1x 10^{-7} /hour

LCLS-II ODM Risk

- Unmitigated risk is high

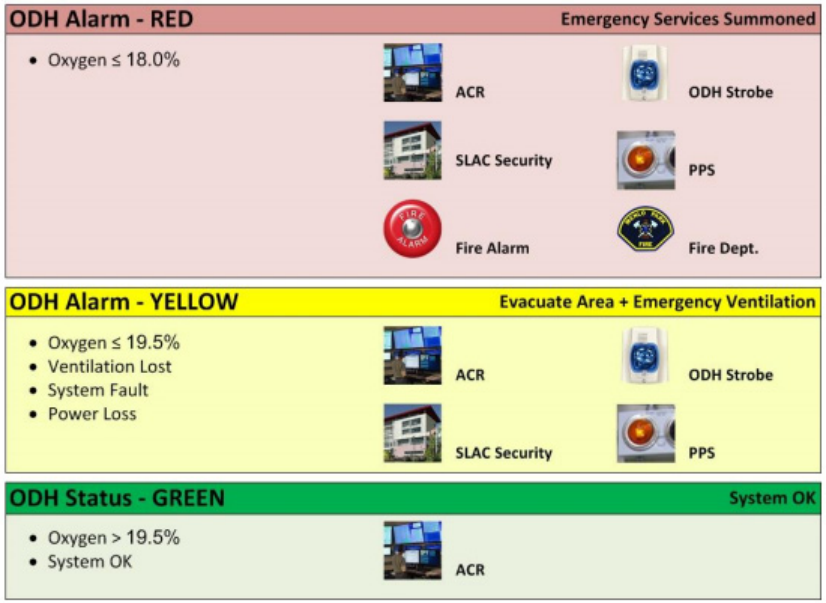
	A	B	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR
1	Preliminary ODH Analysis for Linac Tunnel with LCLS-II SRF Linac - w/9000 CFM of Forced Fresh Air	Comments	Total Q Ventilation Rate (scfm)	Total q Ventilation Rate (scfs)	He flow thru orfice (lbs/sec)	He flow thru orfice (ft^3/s)	He spill rate (SCFM)	He spill rate (SCFS)	Control Volume (ft^3)	Oxygen Conc. ($\%O_2$) wtih t=0	Oxygen Conc. ($\%O_2$) wtih t=1	Oxygen Conc. ($\%O_2$) wtih t=10	Oxygen Conc. ($\%O_2$) wtih t=20	Oxygen Conc. ($\%O_2$) wtih t=30	Oxygen Conc. ($\%O_2$) wtih t=40	Oxygen Conc. ($\%O_2$) wtih t=50	Oxygen Conc. ($\%O_2$) wtih t=60	Oxygen Conc. ($\%O_2$) wtih t=120	Oxygen Conc. ($\%O_2$) as $t \rightarrow \infty$	F_i (fatalities/ failure)	P_i (failures/hr)	ODH Rate (fatality/hr) $=F_i*P_i*\#$
2	CM Cavity (Pressure Vessel)	Rupture	-	-	1.63E+02	21.583	818,945	13,649.09	32,472	21.0	13.8	0.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.00E+00	5.00E-09	1.48E-06
3	Very Large Earthquake	Many Ruptures	n/a	n/a	n/a	n/a	n/a	n/a	330,000	21.0								0.1	0.1	1.00E+00	7.61E-07	7.61E-07
4	Weld Leak CM Helium Circuit (G) - 2-phase pipe	Rupture	-	-	2.68E+01	3.555	134,881	2,248.01	32,472	21.0	19.6	10.5	5.3	2.6	1.3	0.7	0.3	0.0	0.0	1.00E+00	9.23E-11	8.20E-08
5	Valve Leak CM Cool-Down and Liquid Level Control Valves	Rupture	-	-	2.21E+01	2.170	111,362	1,856.03	32,472	21.0	19.8	11.9	6.7	3.8	2.1	1.2	0.7	0.0	0.0	1.00E+00	5.00E-10	3.70E-08
6	Weld Leak Transfer Line, End & Feed Cap Circuit (B) - 2K Return	Large leak	-	-	7.96E+00	1.056	40,085	668.09	32,472	21.0	20.6	17.1	13.9	11.3	9.2	7.5	6.1	1.8	0.0	1.00E+00	1.38E-10	3.03E-08
7	Weld Leak CM Helium Circuit (G) - 2-phase pipe	Large leak	-	-	8.22E+00	1.092	41,421	690.36	32,472	21.0	20.6	17.0	13.7	11.1	9.0	7.3	5.9	1.6	0.0	1.00E+00	2.77E-11	2.46E-08
8	Weld Leak CM Helium Circuit (H) - warm up / cool dn	Rupture	-	-	1.35E+01	1.431	68,208	1,136.80	32,472	21.0	20.3	14.8	10.4	7.3	5.2	3.6	2.6	0.3	0.0	1.00E+00	6.56E-12	1.75E-08
9	Weld Leak CM Helium Circuit (B) - 2K Return	Large leak	-	-	8.83E+00	0.953	44,451	740.85	32,472	21.0	20.5	16.7	13.3	10.6	8.4	6.7	5.3	1.4	0.0	1.00E+00	1.38E-10	1.53E-08
10	Weld Leak Transfer Line, End & Feed Cap Circuit (B) - 2K Return	Rupture	-	-	2.80E+02	37.110	1,408,075	23,467.92	32,472	21.0	10.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.00E+00	4.13E-11	9.09E-09
11	Weld Leak CM Helium Circuit (A) - 2.3 K Liquid Supply	Rupture	-	-	2.69E+01	2.840	135,362	2,256.03	32,472	21.0	19.6	10.5	5.2	2.6	1.3	0.7	0.3	0.0	0.0	1.00E+00	1.19E-11	5.71E-09
12	Weld Leak CM Helium Circuit (B) - 2K Return	Rupture	-	-	2.80E+02	37.110	1,408,075	23,467.92	32,472	21.0	10.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.00E+00	4.13E-11	4.59E-09
13	Weld Leak Transfer Line, End & Feed CapCircuit (C) - 5K TI Supply	Rupture	-	-	2.69E+01	2.840	135,362	2,256.03	32,472	21.0	19.6	10.5	5.2	2.6	1.3	0.7	0.3	0.0	0.0	1.00E+00	1.19E-11	2.61E-09
14	Weld Leak Transfer Line, End & Feed CapCircuit (D) - 5K TI Return	Rupture	-	-	2.60E+01	2.932	131,075	2,184.58	32,472	21.0	19.6	10.7	5.5	2.8	1.4	0.7	0.4	0.0	0.0	1.00E+00	1.19E-11	2.61E-09
15	Weld Leak Transfer Line, End & Feed CapCircuit (E) - 40K TI Supply	Rupture	-	-	5.93E+00	5.939	29,868	497.80	32,472	21.0	20.7	18.0	15.5	13.3	11.4	9.8	8.4	3.3	0.0	1.00E+00	1.19E-11	2.61E-09
16	Weld Leak Transfer Line, End & Feed CapCircuit (F) 40K TI Return	Rupture	-	-	4.72E+00	7.403	23,782	396.37	32,472	21.0	20.7	18.6	16.5	14.6	12.9	11.4	10.1	4.9	0.0	1.00E+00	1.19E-11	2.61E-09
17	Weld Leak Transfer Line, End & Feed CapCircuit (A) - 2.3 K Supply	Rupture	-	-	1.64E+01	1.732	82,570	1,376.17	32,472	21.0	20.1	13.7	9.0	5.9	3.9	2.5	1.7	0.1	0.0	1.00E+00	9.27E-12	2.04E-09
18	Weld Leak CM Helium Circuit (C) - 5K Supply	Rupture	-	-	2.69E+01	2.840	135,362	2,256.03	32,472	21.0	19.6	10.5	5.2	2.6	1.3	0.7	0.3	0.0	0.0	1.00E+00	1.19E-11	1.32E-09
19	Weld Leak CM Helium Circuit (D) - 5K Return	Rupture	-	-	2.60E+01	2.932	131,075	2,184.58	32,472	21.0	19.6	10.7	5.5	2.8	1.4	0.7	0.4	0.0	0.0	1.00E+00	1.19E-11	1.32E-09
20	Weld Leak CM Helium Circuit (E) - 40K Supply	Rupture	-	-	5.93E+00	5.939	29,868	497.80	32,472	21.0	20.7	18.0	15.5	13.3	11.4	9.8	8.4	3.3	0.0	1.00E+00	1.19E-11	1.32E-09
21	EC/FC Pneumatic Valve	Rupture	-	-	2.21E+01	2.170	111,362	1,856.03	32,472	21.0	19.8	11.9	6.7	3.8	2.1	1.2	0.7	0.0	0.0	1.00E+00	5.00E-10	1.00E-09
22	Valve Leak CM Cool-Down and Liquid Level Control Valves	Leak	-	-	9.44E-01	0.093	4,755	79.25	32,472	21.0	20.9	20.5	20.0	19.5	19.0	18.6	18.1	15.7	0.0	1.00E+00	1.00E-08	7.40E-07
23	EC/FC Pneumatic Valve	Leak	-	-	9.44E-01	0.093	4,755	79.25	32,472	21.0	20.9	20.5	20.0	19.5	19.0	18.6	18.1	15.7	0.0	1.00E+00	1.00E-08	2.00E-08
24	Weld Leak CM Helium Circuit (F) - 40K Return	Rupture	-	-	9.58E-01	1.503	4,827	80.45	32,472	21.0	20.9	20.5	20.0	19.5	19.0	18.6	18.1	15.6	0.0	1.00E+00	8.05E-12	8.94E-10
25	CM Cavity (Pressure Vessel)	Leak	-	-	8.83E-02	0.010	445	7.41	32,472	21.0	21.0	21.0	20.9	20.9	20.8	20.8	20.7	20.4	0.0	1.00E+00	8.00E-08	2.37E-05
26	Weld Leak CM Helium Circuit (A) - 2.3 K Liquid Supply	small leak	-	-	2.62E-01	0.026	1,319	21.99	32,472	21.0	21.0	20.9	20.7	20.6	20.4	20.3	20.2	19.4	0.0	1.00E+00	3.96E-10	1.90E-07
27	Weld Leak CM Helium Circuit (B) - 2K Return	Small Leak	-	-	8.83E-02	0.010	445	7.41	32,472	21.0	21.0	21.0	20.9	20.9	20.8	20.8	20.7	20.4	0.0	1.00E+00	1.38E-09	1.53E-07
28	Weld Leak CM Helium Circuit (C) - 5K Supply	small leak	-	-	2.52E-01	0.027	1,271	21.18	32,472	21.0	21.0	20.9	20.7	20.6	20.5	20.3	20.2	19.4	0.0	1.00E+00	3.96E-10	4.39E-08
29	Weld Leak CM Helium Circuit (D) - 5K Return	small leak	-	-	2.44E-01	0.028	1,231	20.51	32,472	21.0	21.0	20.9	20.7	20.6	20.5	20.3	20.2	19.5	0.0	1.00E+00	3.96E-10	4.39E-08
30	Weld Leak CM Helium Circuit (E) - 40K Supply	small leak	-	-	5.96E-02	0.060	300	5.00	32,472	21.0	21.0	21.0	20.9	20.9	20.9	20.8	20.8	20.6	0.1	1.00E+00	3.96E-10	4.39E-08
31	Weld Leak CM Helium Circuit (F) - 40K Return	small leak	-	-	4.75E-02	0.074	239	3.99	32,472	21.0	21.0	21.0	20.9	20.9	20.9	20.9	20.8	20.7	0.1	1.00E+00	2.68E-10	2.98E-08
32	Weld Leak CM Helium Circuit (G) - 2-phase pipe	small leak	-	-	2.52E-01	0.027	1,271	21.18	32,472	21.0	21.0	20.9	20.7	20.6	20.5	20.3	20.2	19.4	0.0	1.00E+00	2.77E-11	2.46E-08
33	Weld Leak CM Helium Circuit (H) - warm up / cool dn	Leak	-	-	2.62E-01	0.026	1,319	21.98	32,472	21.0	21.0	20.9	20.7	20.6	20.4	20.3	20.2	19.4	0.0	1.00E+00	4.71E-10	1.26E-06
34	Weld Leak Transfer Line, End & Feed CapCircuit (A) - 2.3 K Supply	Leak	-	-	2.52E-01	0.027	1,271	21.18	32,472	21.0	21.0	20.9	20.7	20.6	20.5	20.3	20.2	19.4	0.0	1.00E+00	3.09E-10	6.80E-08
35	Weld Leak Transfer Line, End & Feed Cap Circuit (B) - 2K Return	small leak	-	-	7.96E-02	0.011	401	6.68	32,472	21.0	21.0	21.0	20.9	20.9	20.8	20.8	20.7	20.5	0.1	1.00E+00	1.38E-09	3.03E-07
36	Weld Leak Transfer Line, End & Feed CapCircuit (C) - 5K TI Supply	small leak	-	-	2.52E-01	0.027	1,271	21.18	32,472	21.0	21.0	20.9	20.7	20.6	20.5	20.3	20.2	19.4	0.0	1.00E+00	3.96E-10	8.70E-08
37	Weld Leak Transfer Line, End & Feed CapCircuit (D) - 5K TI Return	small leak	-	-	2.44E-01	0.028	1,231	20.51	32,472	21.0	21.0	20.9	20.7	20.6	20.5	20.3	20.2	19.5	0.0	1.00E+00	3.96E-10	8.70E-08
38	Weld Leak Transfer Line, End & Feed CapCircuit (E) - 40K TI Supply	small leak	-	-	5.96E-02	0.060	300	5.00	32,472	21.0	21.0	21.0	20.9	20.9	20.9	20.8	20.8	20.6	0.1	1.00E+00	3.96E-10	8.70E-08
39	Weld Leak Transfer Line, End & Feed CapCircuit (F) 40K TI Return	small leak	-	-	4.75E-02	0.074	239	3.99	32,472	21.0	21.0	21.0	20.9	20.9	20.9	20.9	20.8	20.7	0.1	1.00E+00	3.96E-10	8.70E-08
40																				ΣΦ- w/ NO ventilation		2.94E-05

-Improve the system

-Add instrumented functions to reduce the risk

ODM Alarm & Control

- Instrumented Alarms

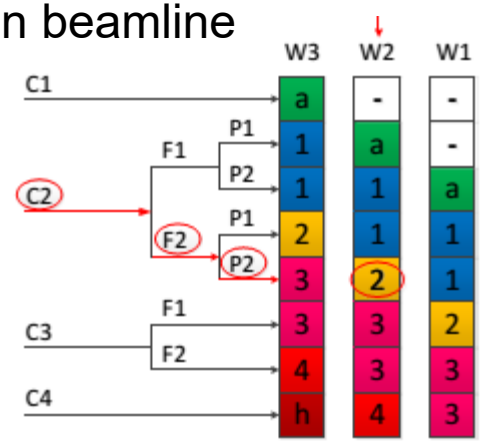


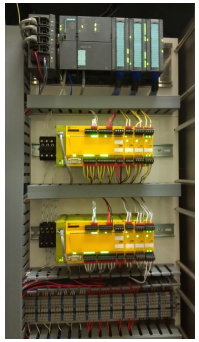
- Instrumented control function (SIL 1 rated)
  - Turn on 9000 ft^3/min active ventilation, tunnel air exchange before setting access
  - Turn on emergency ventilation
- ODM will mitigate part of the risks by about a factor of 10

Experimental Area (photon) PPS

- Hutch Protection System (HPS)

- Risk is relatively low compared to electron beamline





HPS controller system

Risk Parameter		Classification
Consequence (C)	C1	Light injury to persons
	C2	Serious permanent injury to one or more persons; death of one person
	C3	Death of several persons
	C4	Catastrophic effect, very many people killed
Frequency of presence in the hazardous zone multiplied with the exposure time (F)	F1	Rare to more frequent exposure in the hazardous zone
	F2	Frequent to permanent exposure in the hazardous zone
Possibility of avoiding the consequences of the hazardous event (P)	P1	Possible under certain conditions
	P2	Almost impossible
Probability of the unwanted occurrence (W)	W1	A very slight probability that the unwanted occurrences occur and only a few unwanted occurrences are likely
	W2	A slight probability that the unwanted occurrences occur and few unwanted occurrences are likely
	W3	A relatively high probability that the unwanted occurrences occur and frequent unwanted occurrences are likely

HPS LOPA

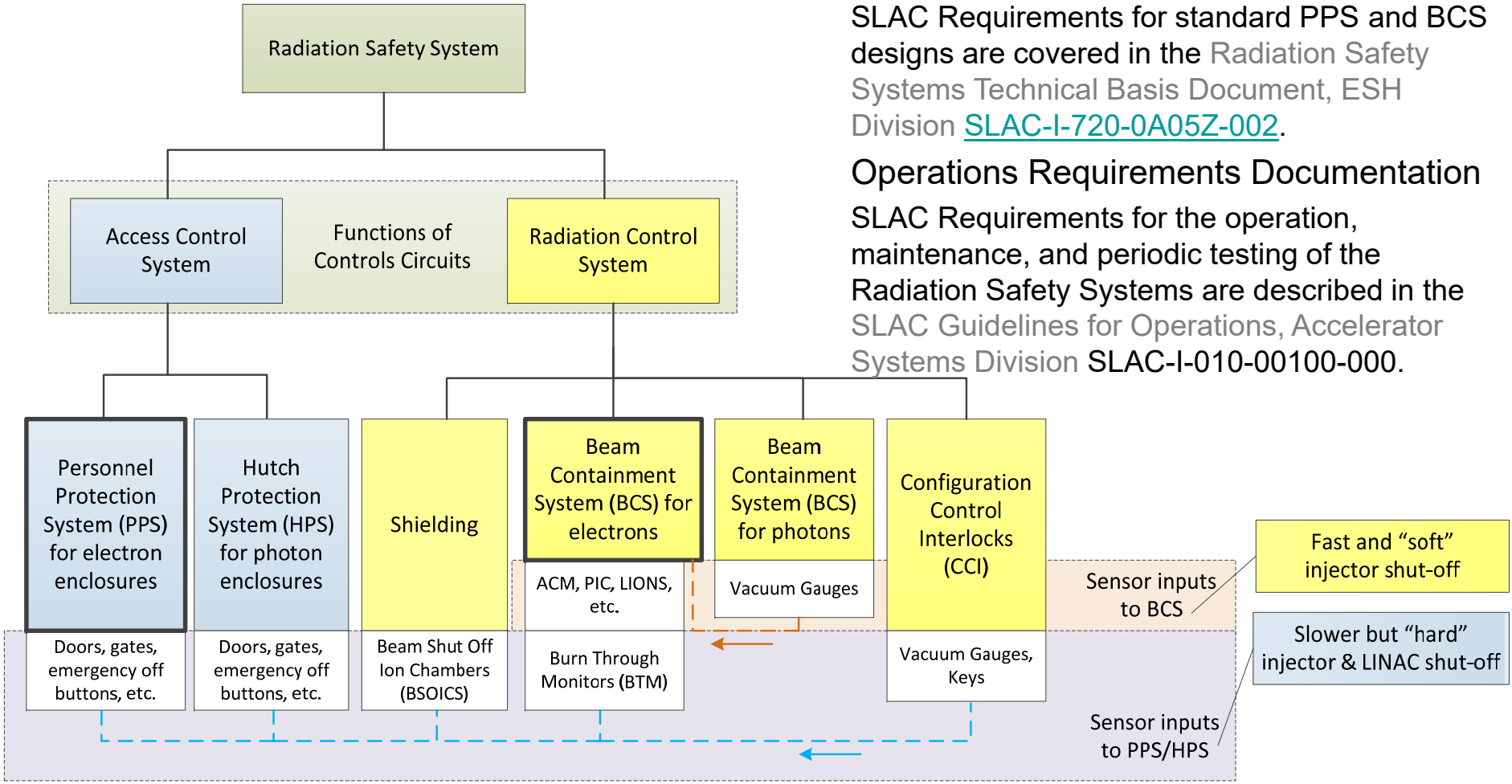
- List all potential scenarios as well as protection layers for each case

Case	Radiation Safety Risk	C	F	P	W	IPL	Safeguards	Creditable IPL	SIL Requirement
1	people trapped inside the hutch during beam operation	2	2	2	2	2	1. Training	No, given credit to reduce W factor	
							2. Search Preset and Search Reset	Yes	
							3. Audio/Visual Warning	3 and 4 combined as one safety function	SIL 1 *
							4. E- Stop function	3 and 4 combined as one safety function	SIL 1 *
							5. Emergency Exit mechanism	No, mechanical means, depend on 3 , will have no SIL rating since it is not an I&C function	
2	people entering the hutch during operation through the sliding door	2	2	2	2	2	1. Training	No, given credit to reduce W factor	
							2. Visual Warning (Y/M light)	No, given credit to reduce W factor	
							3. Key release function	Yes	
							4. Key bank complete switches	Yes	4 or 5 need to be designed as a SIL 1 function
							5. Sliding door switches	Yes	4 or 5 need to be designed as a SIL 1 function
3	people entering the hutch mistakenly via emergency entry mechanism	2	2	2	2	2	1. Training	No, given credit to reduce W factor	
							2. Visual Warning (Y/M light)	No, given credit to reduce W factor	
							3. Sliding door switches	Yes	SIL 2 for sliding door interlock
4	people enter the hutch through rollup equipment door	2	2	2	2	2	1. Training	No, given credit to reduce W factor	
							2. Lock of the rollup door to ground	Yes	
							3. Rollup door magnetic switches	Yes	SIL 1

Case 1, 2, 4: Already have 2 IPLs

Case 3: One SIL2 function; or take additional efforts to credit another IPL

Application to SLAC RSS



- Design Requirements Documentation

  SLAC Requirements for standard PPS and BCS designs are covered in the Radiation Safety Systems Technical Basis Document, ESH Division SLAC-I-720-0A05Z-002.

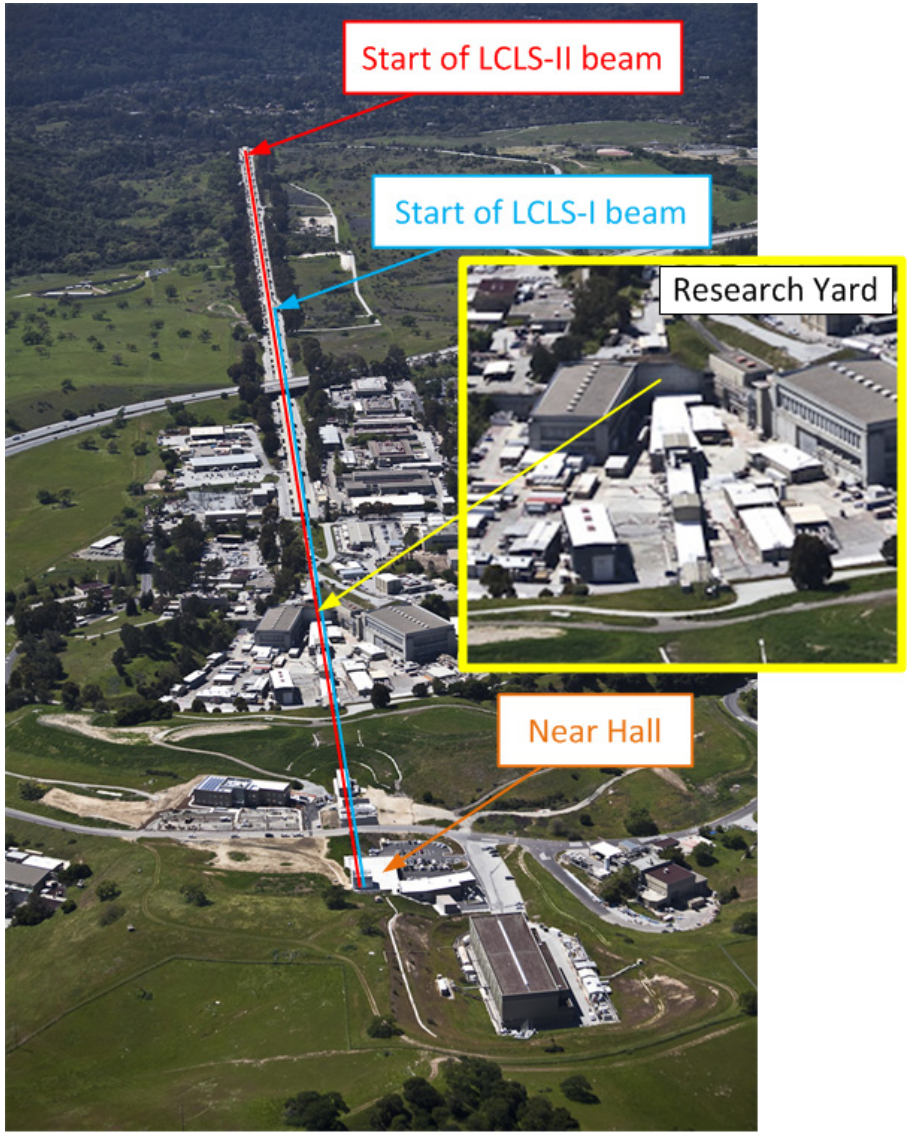
- Operations Requirements Documentation

  SLAC Requirements for the operation, maintenance, and periodic testing of the Radiation Safety Systems are described in the SLAC Guidelines for Operations, Accelerator Systems Division SLAC-I-010-00100-000.

Electron PPS

Safe access with beam parked

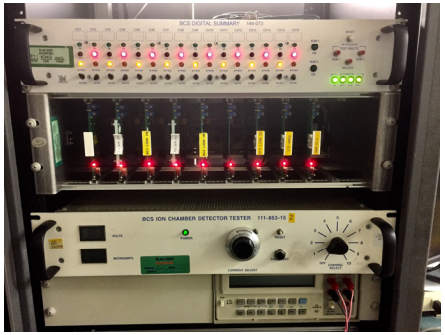
- Operators park the beam on the Beam Switch Yard (BSY) stopper set, to allow personnel downstream access
- Protection layers
  - 3-stopper set (5kW x1, 500W x2)
  - BCS beam power interlock
    - Beam energy interlock (bend magnet current)
    - Average Current Monitor
  - 6 Protection Ion Chambers (PICs) installed, interlocked to BCS
  - 1 Burn Through Monitor (2 pressure switches) interlock to PPS



SLAC NATIONAL ACCELERATOR LABORATORY

Beam Transport Hall (BTH) Beam Loss

- The BTH is above the ground and the shielding is insufficient
- Protection Layers:
- Protection Collimators
  - PICs installed on Protection Collimators
  - PPS interlocked to BTMs at the back of collimators
  - BCS interlocked to Long Ion Chambers (LION)
  - PPS interlocked to Beam Shutoff Ion Chambers (BSIOC)
- There are 4 PLs for the hazards, but they are not all independent: PIC and LION sensors are connected to the same signal processing chassis
  - Need to find more IPLs
  - Or the PIC/LION chassis should be SIL2 capable



Summary

- LOPA methodology explained
- Used three SLAC safety systems to illustrate methodology
- One IPL is equivalent to one SIL 1 function, but may simplify the hardware development efforts
- The LOPA worksheet is a good reference for decision making.

Another Perspective