2015 ICALEPCS melbourne • australia

# Safety Integrity Level (SIL) Verification for SLAC Radiation Safety Systems

Feng Tao

ICALEPCS 2015

Oct. 20, 2015

# Outline

- What is SIL Verification
- SLAC Radiation Safety Systems
- Application of Safety Standards
- SIL Verification for Personnel Protection System (PPS)
- SIL Verification for Beam Containment System (BCS)

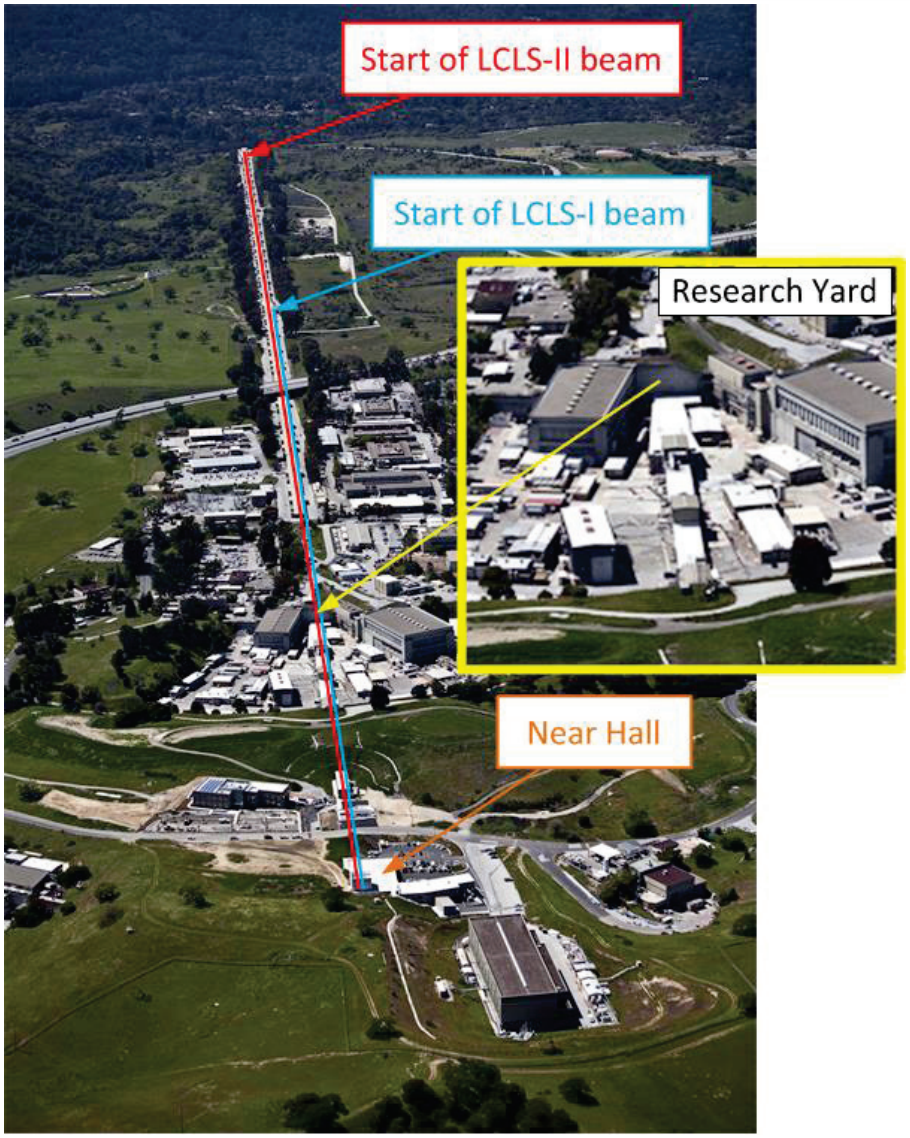
# SLAC Accelerator National Laboratory

Host of user facilities:

- LCLS-I
- FACET
- Several other small test facilities

In design and building:

- LCLS-II
- FACET-II



# What is Safety Integrity Level verification?

SLAC

- SIL is the basis for a risk-based design approach
- It quantifies the reliability performance of each safety function
- Performance Level (PL), used in machinery safety application, has a direct mapping to SIL and PFH
- SIL verification is a critical task required by functional safety standards

Demand Mode

| SIL | PFD | RRF |
|---|---|---|
| 4 | 0.0001 ~ 0.00001 | 10000 ~ 100000 |
| 3 | 0.001 ~ 0.0001 | 1000 ~ 10000 |
| 2 | 0.01 ~ 0.001 | 100 ~ 1000 |
| 1 | 0.1 ~ 0.01 | 10 ~ 100 |

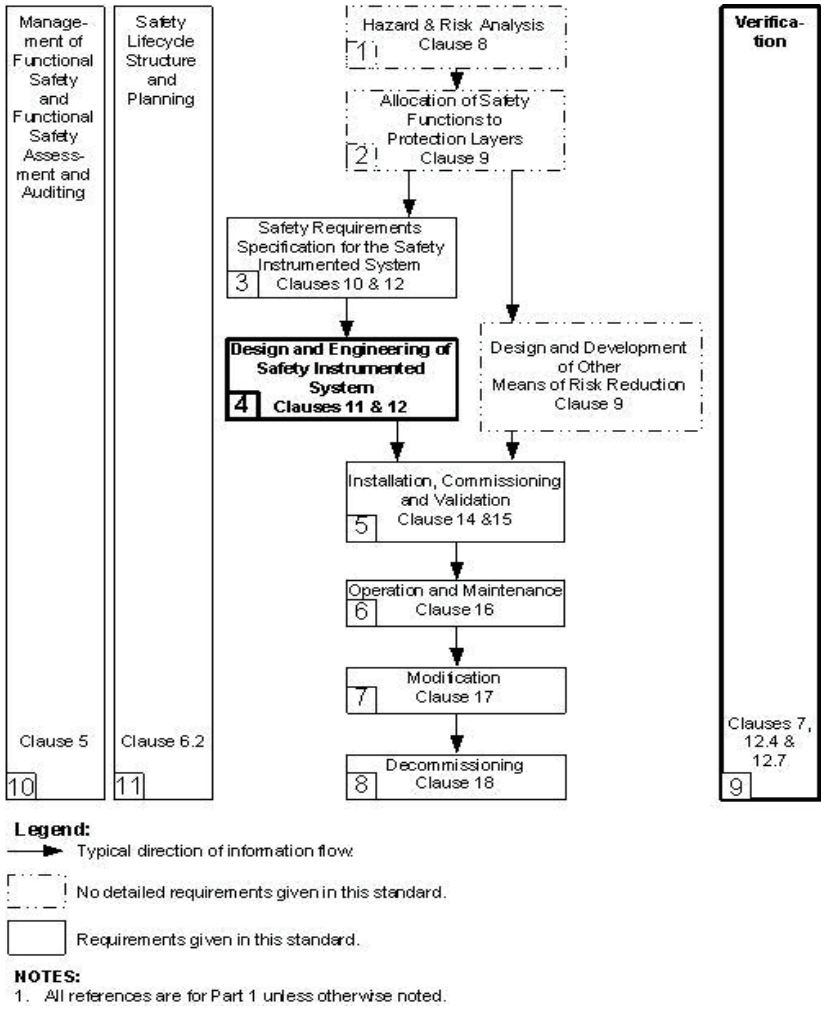
Continuous Mode

| SIL | PFH |
|---|---|
| 4 | $10^{-8} \sim 10^{-9}$ |
| 3 | $10^{-7} \sim 10^{-8}$ |
| 2 | $10^{-6} \sim 10^{-7}$ |
| 1 | $10^{-5} \sim 10^{-6}$ |

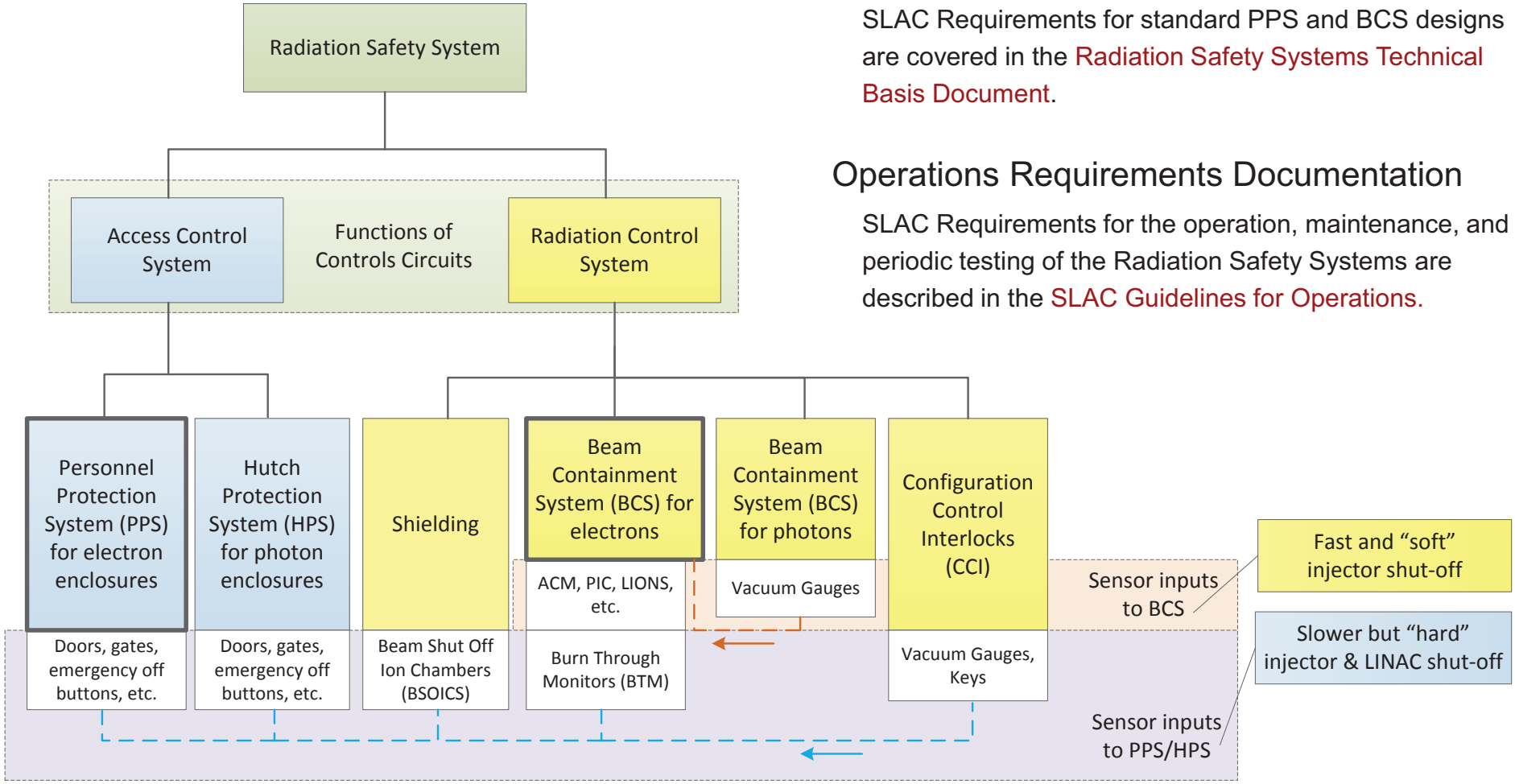
PFD: Probability of Failure on Demand
PFH: Probability of Failure per Hour
RRF: Risk Reduction Factor

# What is SIL verification?

- SIL is the basis for a risk-based design approach
- It quantifies the reliability performance of each safety function
- Performance Level (PL), used in machinery safety application, has a direct mapping to SIL and PFH
- SIL verification is a critical task required by functional safety standards



# SLAC Radiation Safety Systems (RSS): PPS and BCS



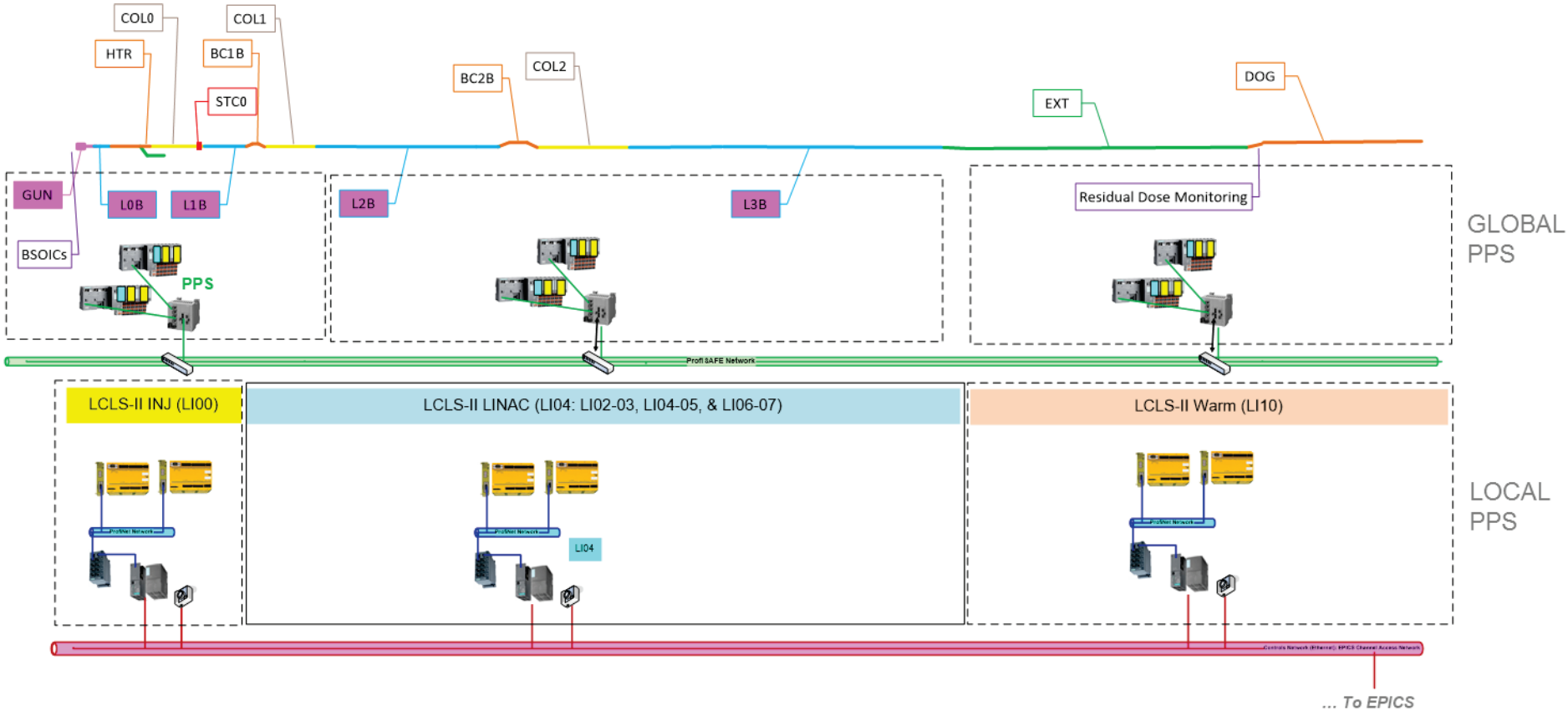

## Design Requirements Documentation

SLAC Requirements for standard PPS and BCS designs are covered in the Radiation Safety Systems Technical Basis Document.

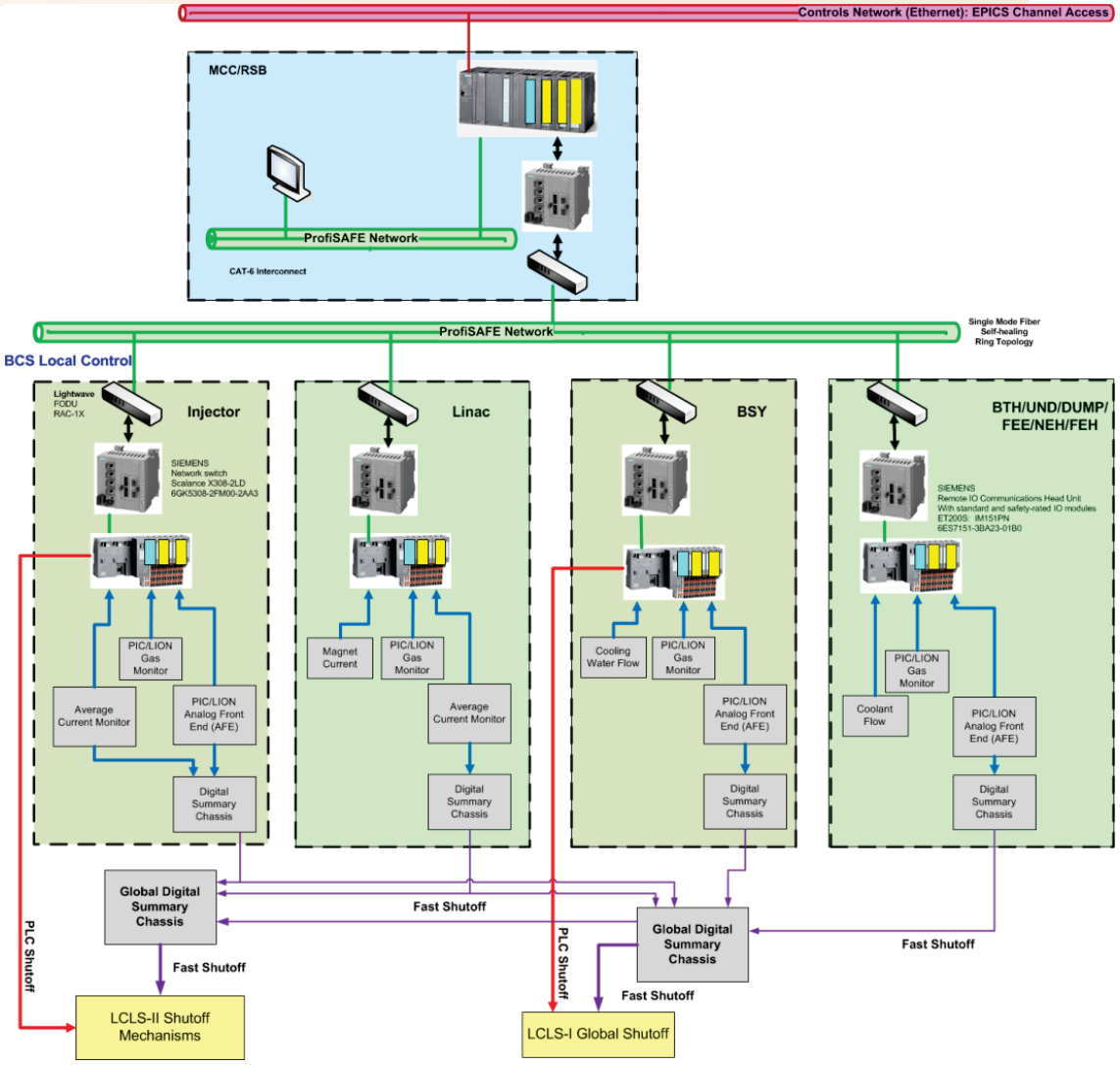
## Operations Requirements Documentation

SLAC Requirements for the operation, maintenance, and periodic testing of the Radiation Safety Systems are described in the SLAC Guidelines for Operations.

# SLAC LCLS-II PPS



# SLAC LCLS-II BCS



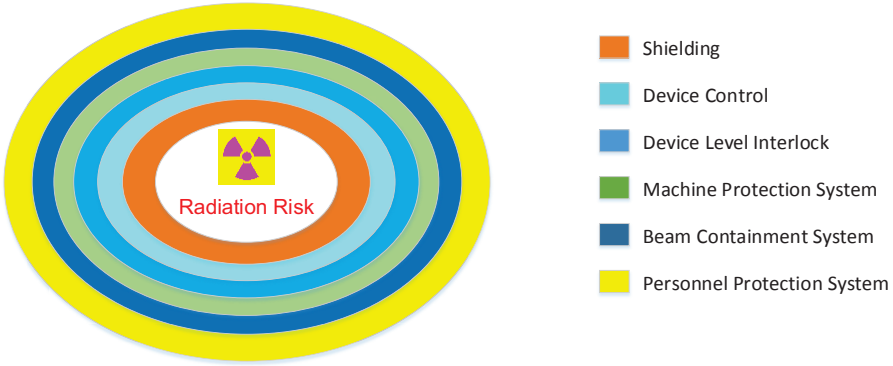
# Safety Standards

- Applying functional safety standards:
  - IEC 61508
    - IEC 61511/ ISA 84: Process
    - IEC 62061: machinery
  - ISO 13849: machinery

- If there is no sector specific IEC standard, use IEC 61508
- ISO/TR 23849: guidance on selecting machinery standard IEC 62061 and ISO 13849, these two standards will eventually merge into ISO/IEC 17305

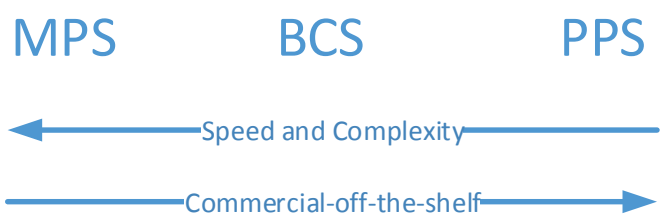
# Mode of Operation

- Three operation modes defined for safety functions:
  - Low demand
  - High demand
  - Continuous
- Protection Layers for Radiation Risks



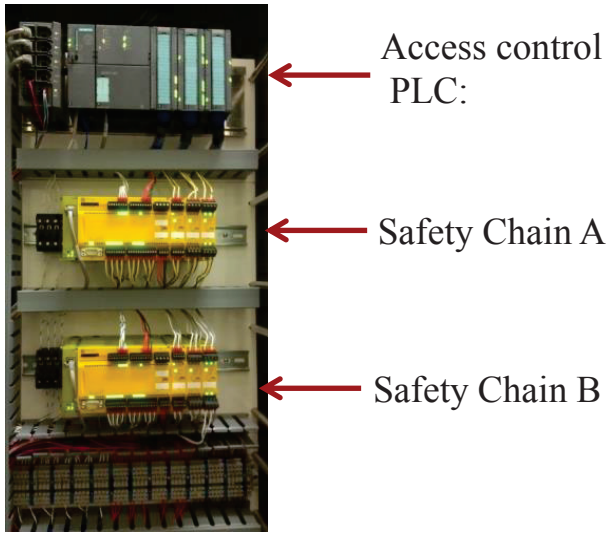

- Protection layers in front of RSS will lower the activating frequency of safety functions
  - PPS and BCS safety functions are operating in “demand” mode

# SIL Verification: Difference of PPS and BCS




- PPS uses ~95% of commercial-off-the-shelf devices, increase this ratio for modularity, lower life-cycle cost and faster deployment
- BCS has to rely on customized electronics to meet response time requirements, COTS products will be used wherever possible.
- The higher the level of customization = a complex reliability assessment
  - Reliability assessment of detailed device/assembly
  - For complex electronics, Obtaining SIL Capability information is very difficult
  - Designing out systematic failures is difficult , need consensus
  - Maintain a proper balance between quality control and cost

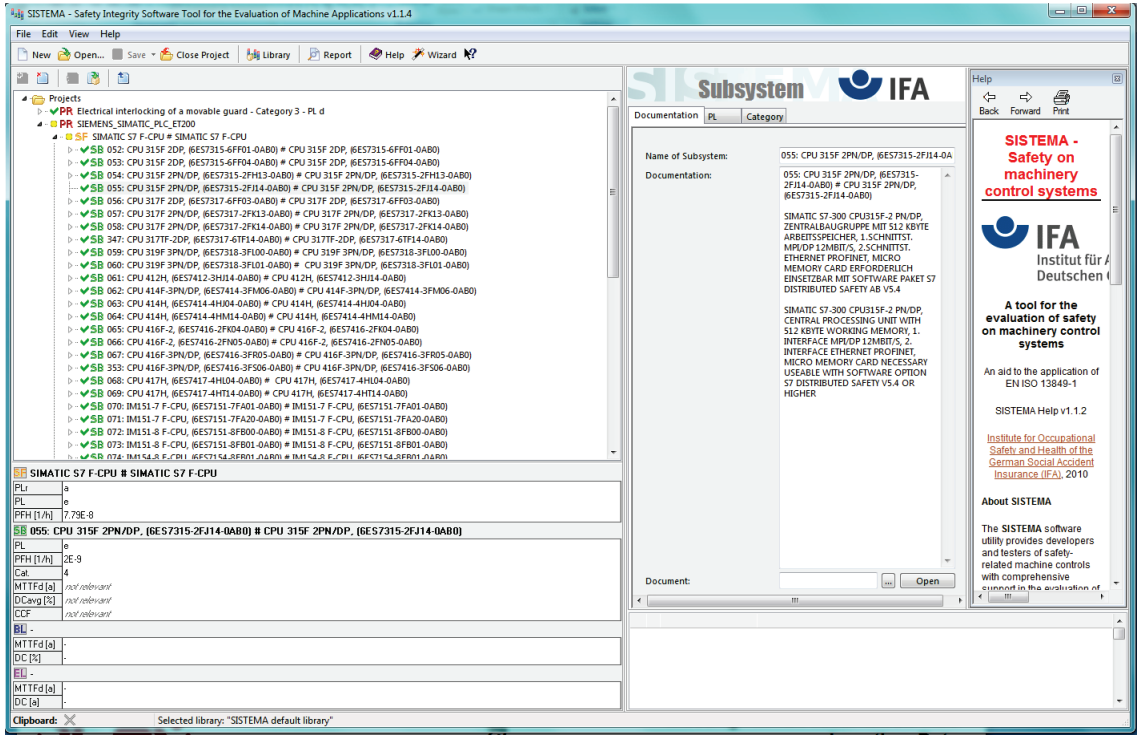
# PPS SIL Verification




- SIL verification is for each safety function, not for system as a whole
  - Access control contains non-safety critical functions, but will reduce the challenge to safety functions
  - Access Control may act as a protection layer for ODM
  - PPS Safety functions reside in safety PLCs
- Usually any PLC control/interlock with configuration control can be regarded as one protection layer (SIL 1)

# Commercial Tools and Software

- Machinery - free software：SISTEMA
- Process industry - commercial software available for *standard* configurations
- For non-standard configuration, be cautious!



# PFD Calculation

- Structural constraints should be satisfied first !
- PFD of a SIF is the sum of all factors contributing to failure:

$$PFD_{SIF}=PFD_{Sensor}+PFD_{PLC}+PFD_{Final\ Element}+PFD_{Supporing\ System}$$

- Power supply reliability is difficult to evaluate:
  - Follow the fail-safe design principle and eliminate the power dependency
  - Power line monitoring and an alarm can be another option
  - UPS can be a solution -used by PPS
  - IEEE Std 493 provides the method and data, is the default method used in America
  - Different loads have different reliabilities, depends on the distribution design
  - SLAC's single source of big blackout:

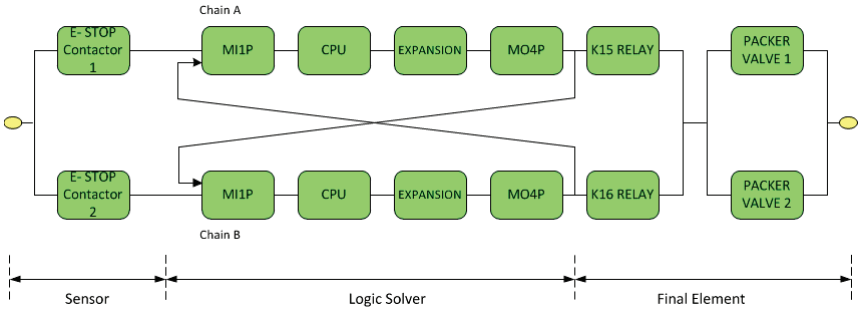
# PFD Calculation

SLAC

- Does not need to be precise, but needs to be conservative
- IEC 61508 only requires for 2 effective digits
- Should never yield optimistic results
- IEC 61508 lacks of details on how equations are derived, new publications fixed this issue:
  - ISA/TR84.02 written and was approved early 2015
  - ISO/TR 12489 published in 2013
  - Reliability of Safety-critical Systems, 2014

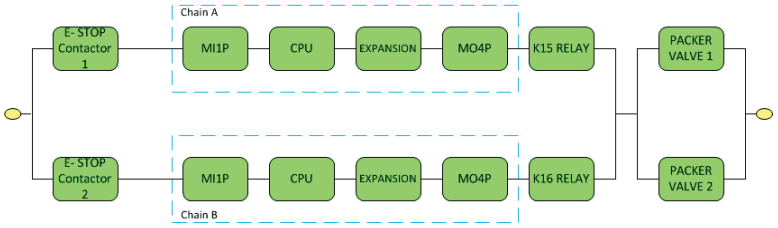
# PPS Example – E-Stop Function

- Photon interlock to beam stopper (2 stoppers)

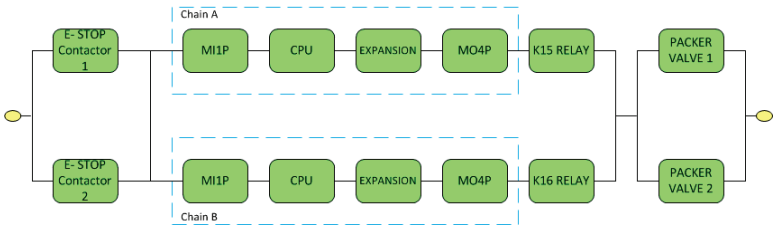



- Non-standard configuration
- Using the “cut set” method to find the bounds of PFD:

Lower Bound




Upper Bound



# PFD Calculation – Cont.

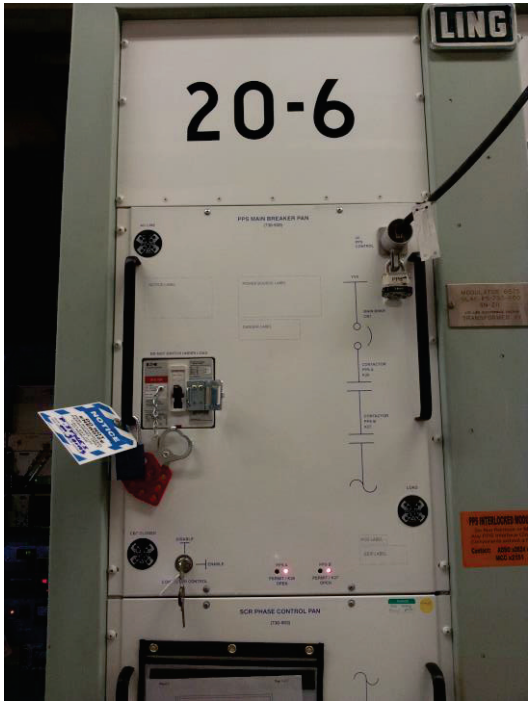
- For system with redundant channels, common cause failure will dominant the overall system failure
  - Reduce the common cause factor β is critical
  - Sector specific standards provide score tables for β value determination
  - They are good information sources on how to achieve a better design
- While redundancy >2, additional credit should be given:

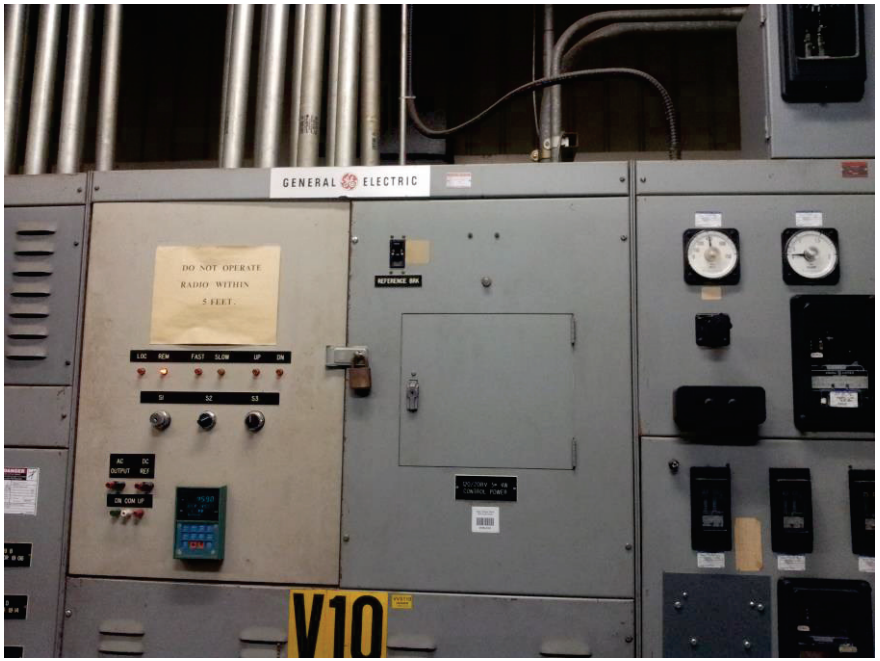
$$\beta(MooN) = \beta C_{MooN}$$

| M\N | N=2 | N=3 | N=4 |
|---|---|---|---|
| M = 1 | C1oo2= 1 | C1oo3=0.5 | C1oo4=0.3 |
| M = 2 | | C2oo3=2.0 | C2oo4=1.1 |
| M = 3 | | | C3oo4=2.9 |

# Accelerator Specific Final Elements

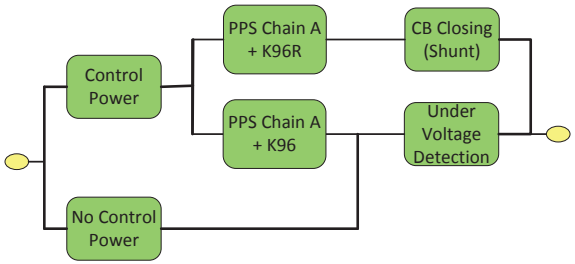
- Modulator and Variable Voltage Substation (VVS)
- Review schematics to establish reliability model of that device



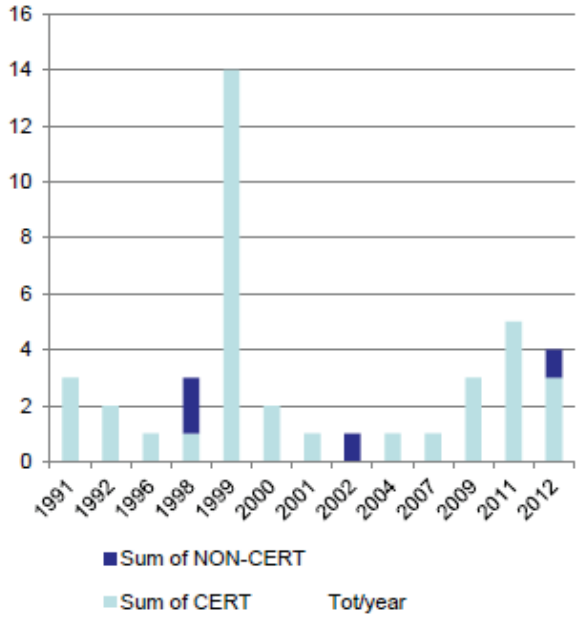



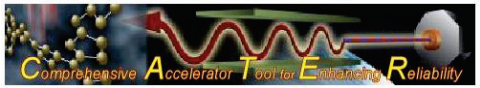
# Additional Reliability Analysis

VVS circuit breaker assembly RBD:




Site-specific reliability data is retrieved from operational data




- Device installation, maintenance and repair history information can be obtained
- Use total operational time and number of failures to get the device failure rate data, 90% confidence is required
- Combined with previous RBD, the PFD of the PPS interlock to VVS can be calculated
- Provided colleagues feedback on how to improve their design, and standardize the interface

# SIL Verification for BCS

- Customized electronics should be designed for reliability as well as functions:
  - Structural Constraints

Type A:

| SFF | Hardware Fault Tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| <60% | SIL 1 | SIL 2 | SIL 3 |
| 60%-90% | SIL 2 | SIL 3 | SIL 4 |
| 90% - 99% | SIL 3 | SIL 4 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |

Type B:

| SFF | Hardware Fault Tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| <60% | N/A | SIL 1 | SIL 2 |
| 60%-90% | SIL 1 | SIL 2 | SIL 3 |
| 90% - 99% | SIL 2 | SIL 3 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |

  - IEC 61508 requires design quality assurance (minimum requirements)
  - Standard  requires a conservative estimate with 70% single-sided confidence when using component failure rates

# BCS Hardware - Design for Reliability

SLAC

- Carefully define the boundary between safety/non-safety critical parts of circuits
- Limit the complexity of the safety-critical parts of circuits
- Reduce the number of combinations of failure modes, and FMEA
- Reliability calculation for circuit boards:
  - IEC 62380
  - Telcordia SR-332
  - RiAC 217plus
- Integrated Circuits can be treated as a blackbox
- Vendor provided tools and utility software will expedite designs
- CATER database is useful in justifying “proven-in-use” of complex ICs

# Summary



- SIL verification for PPS is relatively easy, just be conservative
- Large components should be decomposed to analyze the reliability
- Design for reliability is critical for BCS
- BCS reliability analysis is done at the circuit board component level
- Site specific operational data is important to retrieve failure rates and justify “proven-in-use”