Jefferson Lab IEC 61508/61511 Safety PLC Based Safety System

K. Mahoney, H. Robertson

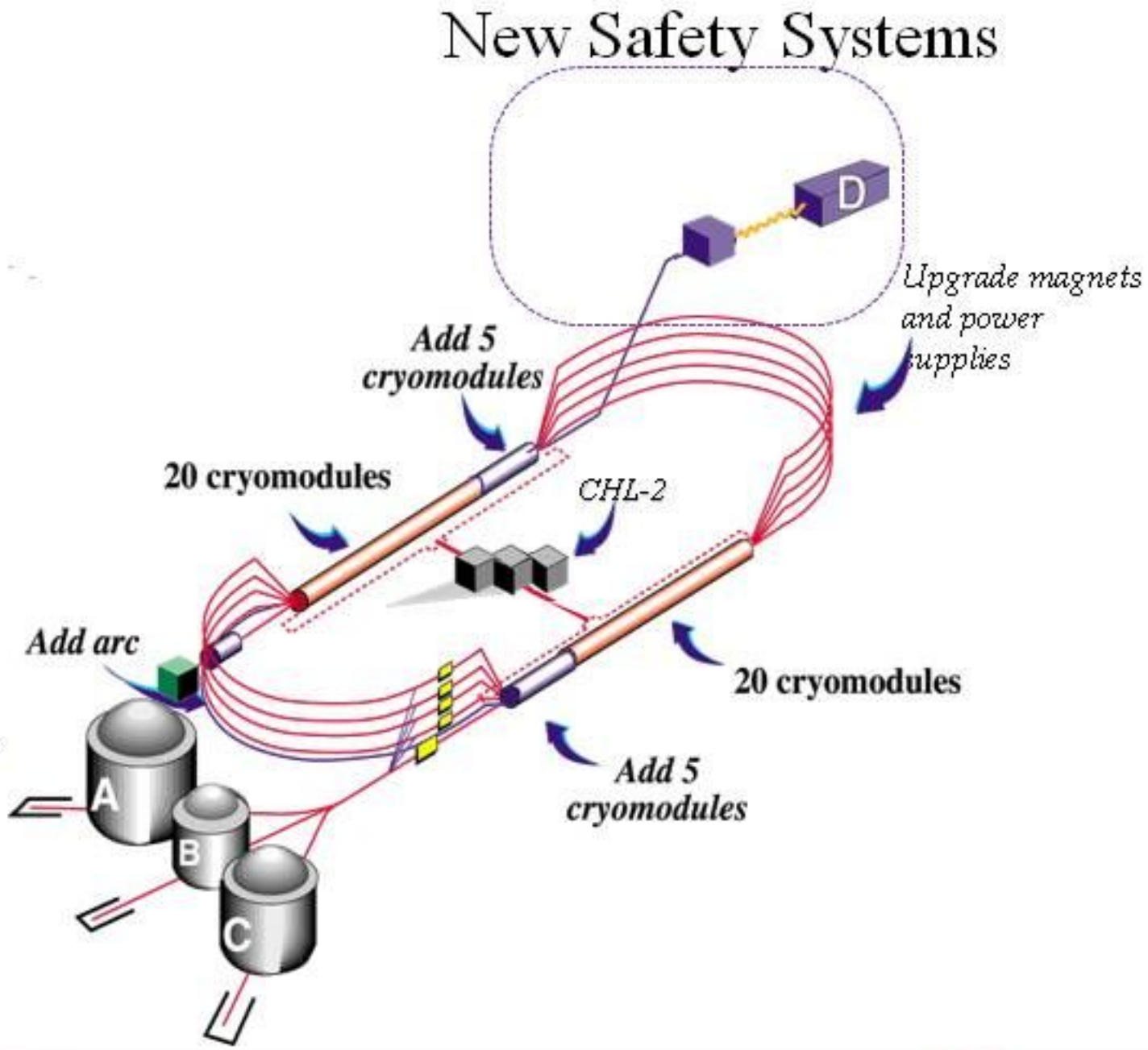
Outline

- CEBAF 12 GeV Upgrade Project
- IEC Standards and SILs
- CEBAF 12 GeV Project Compliance
- Safety PLC Selection and Test
- Hardware Design
- Software Design
- Other Considerations
- High Availability Architectures

CEBAF 12GeV Upgrade

- 10 new RF Interfaces
  - PSS based on existing design
- New Arc Magnet String – Arc 10 (West Arc)
  - PSS based on existing design

- **Tagger/Hall D**
  - **New facility – split in to two buildings**
  - **PSS based on Safety PLCs**
  - **Same shielding/critical devices as existing BSY/Endstation design**
  - **Added protection functions for electron beam transport**



JLab PSS

Functions

- Access Controls
- Beam Containment
- Equipment Interlocks
- ESTOP
- Kickers (Injector Only)
- Alarms/Warning Devices
- Sweep/Controlled Access

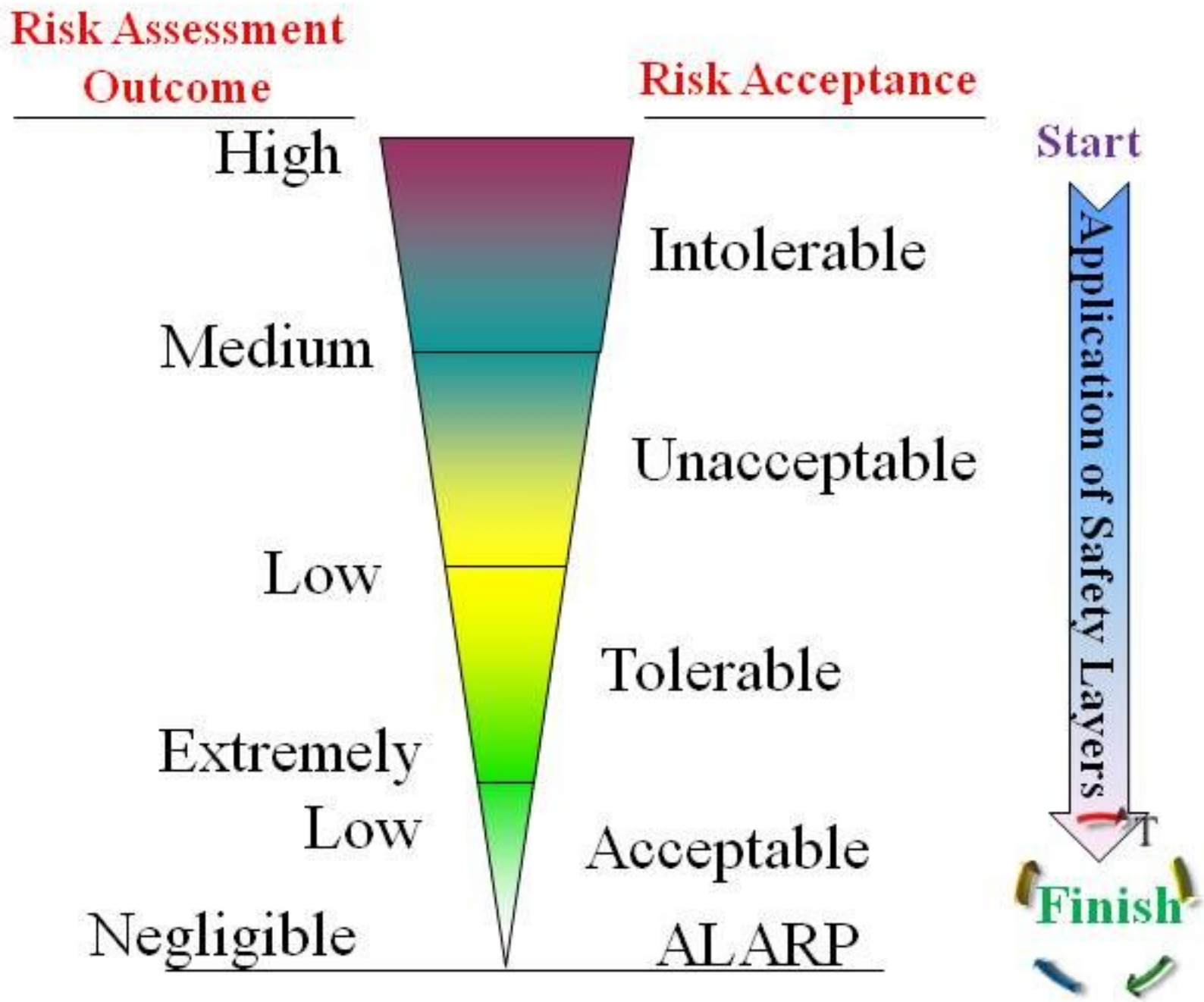
Architecture

- Segmented
- PLC Based
- Fully Redundant
  - 1oo2 or 1oo3 Sensors
  - 1oo2D Logic
  - 1oo2D or 1oo3D Shutdown

* D = Diagnostic Coverage

Objective for Safety Systems

- Reduce risk to acceptable level by application of safety layers
- Work through continuous improvement to further reduce risk to ALARP
- During lifetime of the safety system, the risk will vary between Negligible and Minor.



IEC Standards

Process Management Standards

ISO/IEC 15288 Systems Engineering

ISO/IEC 12207 Software Lifecycle

Safety System Standards

IEC 61508 Parts 1-3 Functional Safety for Programmable Systems

Umbrella Standard

Sector Specific Standards

IEC 61511 Safety For the Process Industries

IEC 62061 Safety For the Machine Industries

IEC 62304 Safety For the Medical Industries

IEC 61513 Safety For the Nuclear Power Industries

Safety Integrity Levels

- **Safety Integrity**
  - Probability that a system will perform a given safety function over specified time period.
  - Safety availability

- **Safety Integrity Level (SIL)**
  - Classification system for safety functions
  - Applies only to specific function
  - Based on safety unavailability PFD_{avg} or $\lambda_D(t)$
  - Integer number between 1 and 4
    - SIL1 = lowest. $PFD_{avg} = 10^{-1}$ to 10^{-2}
    - SIL4 = highest. $PFD_{avg} = 10^{-4}$ to 10^{-5}

      Note: for high demand mode ($\lambda_D(t)$) multiply by 10^{-4}
  - Performance Specification

Critical Decision Points in SIL Design

- Systems Engineering Process/Project Management Process
- Hazard Identification and Risk Assessment Process
  - Events
  - Consequences
  - Exposure
  - Likelihood
- Allocation of Safety Functions
  - Demand Mode or Continuous Demand
  - SIL
- Safety Timing
- Operational Considerations
  - Machine Availability
  - Certification (Test) Interval
- Test Criteria
- Architecture/Redundancy
- V&V

IEC61511 Compliance

12GeV PSS Project Status

	IEC 61511 Clause # - Subject
✓	5 – Management of Functional Safety
✓	6 – Safety Lifecycle
✓	7 – Verification
✓	8 – Hazard and Risk Assessment
✓	9 – Allocation of Safety Functions
✓	10 – SIS Requirements Specification
✓	11 – SIS Design and Engineering
P	12 – Application Software
P	13 – Acceptance Testing
P	14 – SIS Installation and Commissioning
P	15 – SIS Validation
✓	16 – SIS Operation and Maintenance
✓	17 – Modification
✓	18 – Decommissioning
✓	19 – Information and Documentation

Refer to lifecycle model and IEC61511 for specific requirements

61511 Clause 8 – Hazard and Risk Assessment

- Risk assessment performed as part of Facility Safety Assessment Documentation (SAD) process
- Identifies initiating events
- SAD process designed to produce necessary inputs to PSS requirements
  - Traceable link between SAD and PSS
  - Identifies credited controls vs. defense in depth
- Continuous process
- Developed new method of Software Risk Assessment (ICALEPCS 2011?)

Risk Assessment

Safety Assessment - Hazard Analysis Table

Abbreviations: WBD – Whole Body Dose, EL – Extremely Low, L – Low, M–Medium.

								Unmitigated			Mitigated		
ID	Bounding	Hazard Type	Event Description	Potential Initiators	Basis/ Assumptions	Results	Location	Consequence	Probability	Consequence	CC: Credited Control DD: Defense in Depth	Probability	Consequence
1a	Y (CEBAF Only)	Prompt Ionizing Radiation	**High power beam (900kW) enters occupied area and strikes thick target ($X >> X_0$) with authorized personnel present in beam enclosure**	Magnet supply failure Control System Failure MCC Operator Error	No warning Worst-case exposure to workers Condition not sustainable for > 0.1 second, after that beam burn through and impossible to transport	Multiple worker exposure to very high radiation fields, WBD >> 500 rem (lethal dose within seconds at close distance)	CEBAF Tunnels and Halls	Worker deaths No off-site consequence	M	M	CC: PSS – Critical Devices, Access Controls, Sweep procedures, Interlocks	EL	M

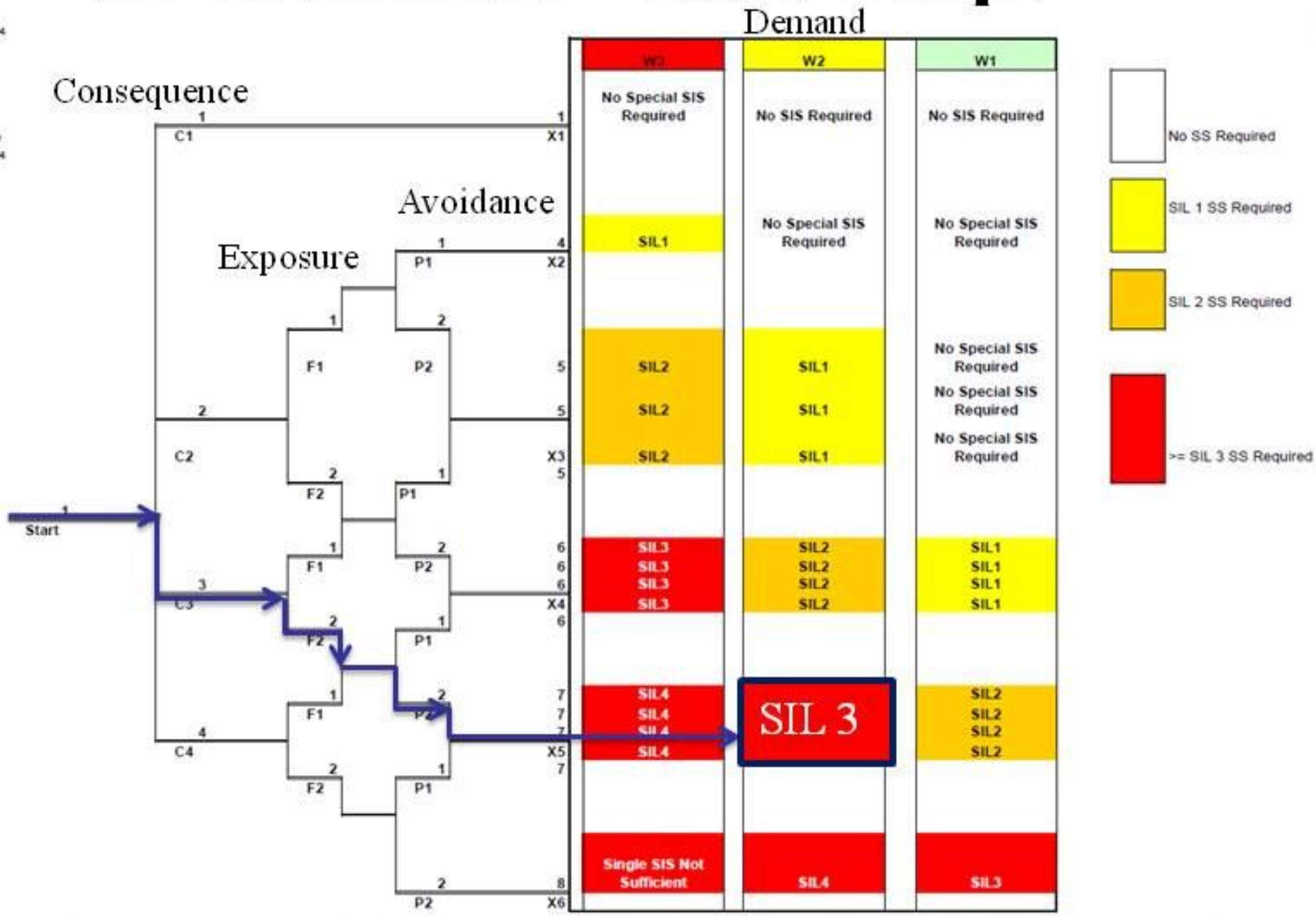
Safety Requirements Specification

Function ID	Safety Function	Required SIL
SF1	Prevent beam transport from exclusion to occupied areas	3
SF1.1	The PSS shall prevent beam transport to occupied areas by use of designated critical devices.	
SF1.2	For the purposes of verification, SF1 shall be considered a continuous demand safety function.	

SIL Selection – Risk Graph

Risk Graph
Today's Date 6/22/2004

Project	12geV
Evaluator	K. Mahoney
Date	6/22/2004
Hazard	
Constraint 1	
Constraint 2	



Consequence		
C1	Minor Injury	1
C2	Serious Injury	2
C3	Death	3
C4	Multiuple Deaths	4

Frequency and Exposure Time		
F1	Rare to Frequent	1
F2	Frequent to Continuous	2

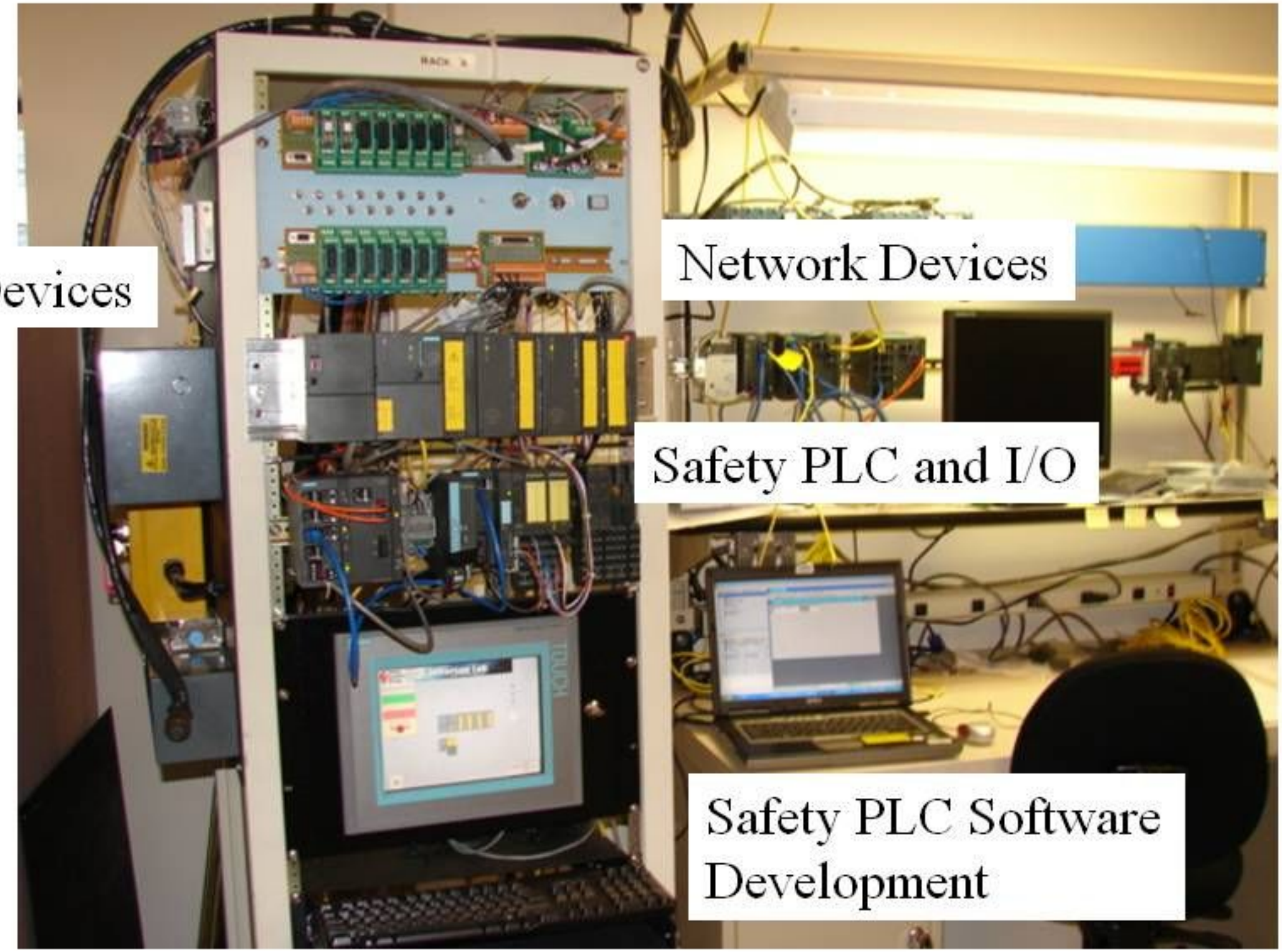
Possibility of Avoidance		
P1	Avoidnace Possible	1
P2	Avoidnace not likely, almost impossible	2

Probability of outcome		
W1	Very Slight probability	1
W2	Slight Probability, few occurances	2
W3	High Probability	3

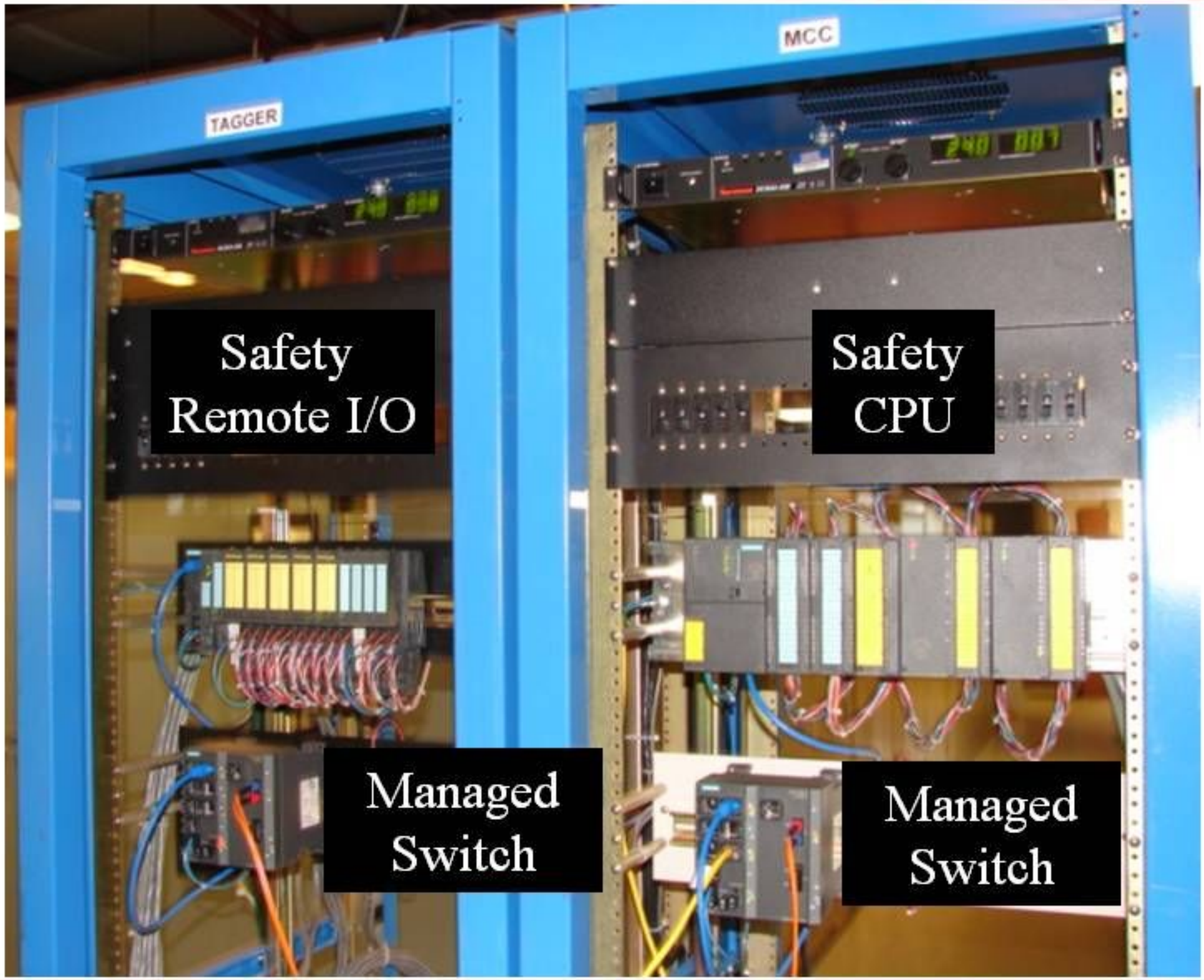
12 GeV CEBAF Safety Functions

Function ID	Safety Function	Required SIL
SF1	Prevent beam transport from exclusion to occupied areas	3
SF2	Shut off interlocked devices when physical barriers between personnel and hazards are unsecured.	2
SF3	Shut off interlocked devices upon activation of an ESTOP	2
SF4	Shut off interlocked devices in support of administrative access to a secure beam enclosure.	2
SF5	Support search and secure operations prior to facility operations.	2
SF6	Inhibit operation of radiation generating devices when a high radiation dose rate associated with the device is detected in an occupied area	1
SF7	Deter unauthorized entry to exclusion areas	1
SF8	Provide visual indications of unsecured safe, secure safe, and unsafe radiological enclosure status.	1
SF9	Provide audible warnings of pending unsafe status of a beam enclosure	1
SF10	Activate audible and visual alarms when the indicated oxygen level in monitored areas drops below 19.5% by volume.	1

Safety PLC Evaluation

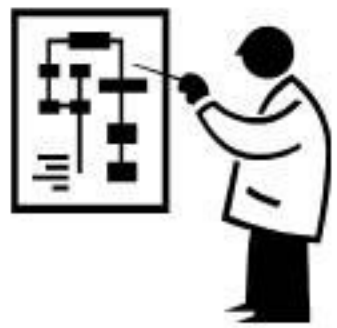


12GeV PSS Pre-Production Mockup

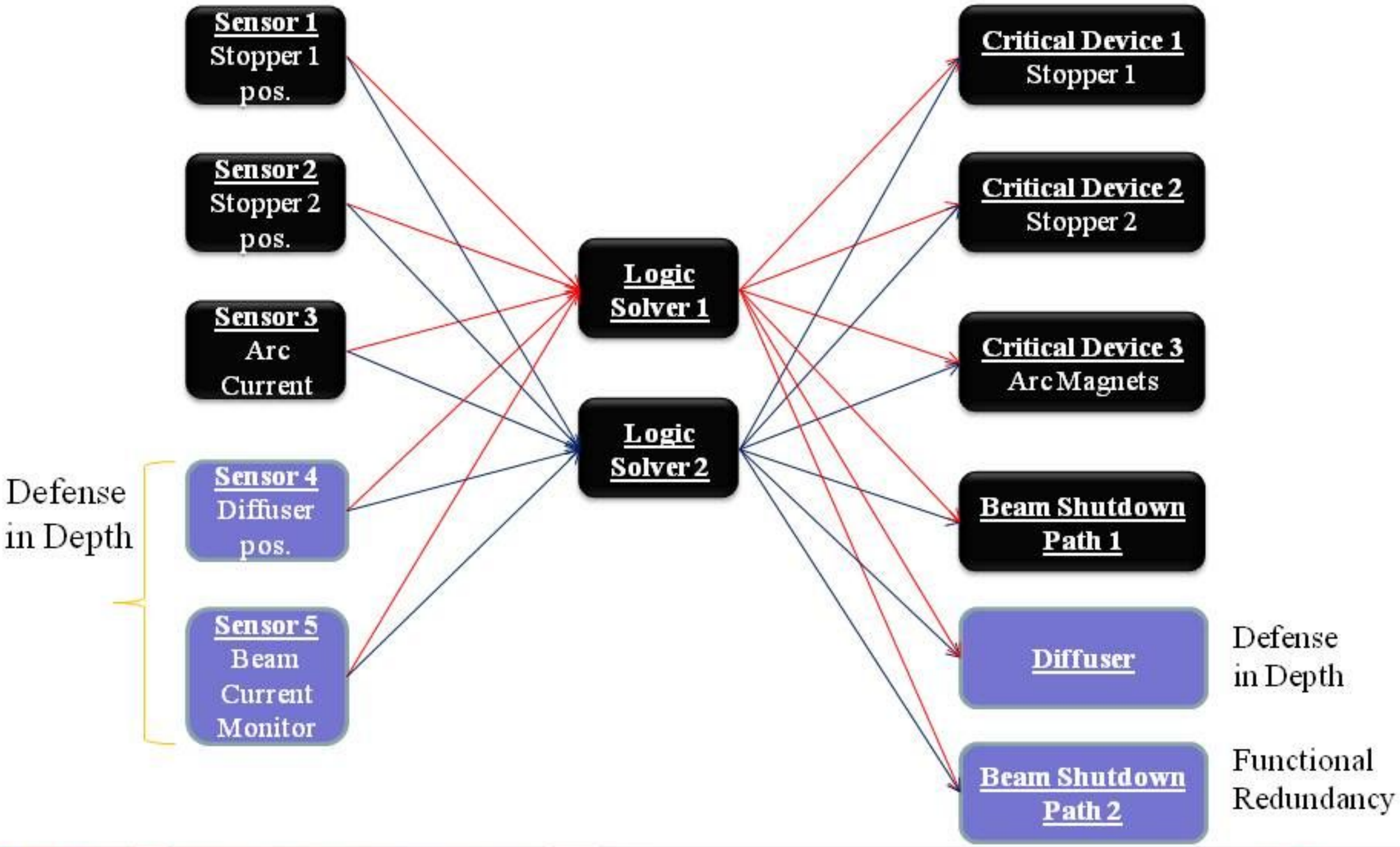


61511 Clause 11 – SIS Design and Engineering

- Design based on SIL 3 rated PLCs
- Fully redundant
- Incorporates human factors, operability, testing,…
- Incorporates manual shutdown (ESTOP)
- Highly Distributed
- Extensive fault detection coverage
  - Meets 61511 Fault Tolerance requirements
    - Logic Solver 1oo2 - SIL 3 SFF > 90% FT of 1 (0 required)
    - Field devices
      - SIL 3 FT of 2 (1oo3)
      - SIL 2 FT of 1 (1oo2)



Typical SIL 3 Architecture



61511 Clause 12 – Application Software

- Lifecycle based
- Spec based on modified logic specification
- Methods and tools based on NASA, DOD, IEC12207 processes
- Limited variability languages
- Integration testing using test stand
  - Limited simulation capability
- SSG Engineers have manufacturer's SW training
- Two programmer implementation
- Functional redundancy where possible
- IEC61508 and other safety style rules
  - Deterministic
  - No dynamic variables
  - No recursive loops
  - No Subroutines (in user program)
  - … See IEC61508-3 and Leveson "System Safety and Computers"

Other Considerations

- Cyber Security
  - Obtained pre-production copy of NIST 800-53
    - Edited into check list
  - Working to NIST 199/200 security for federal computer systems

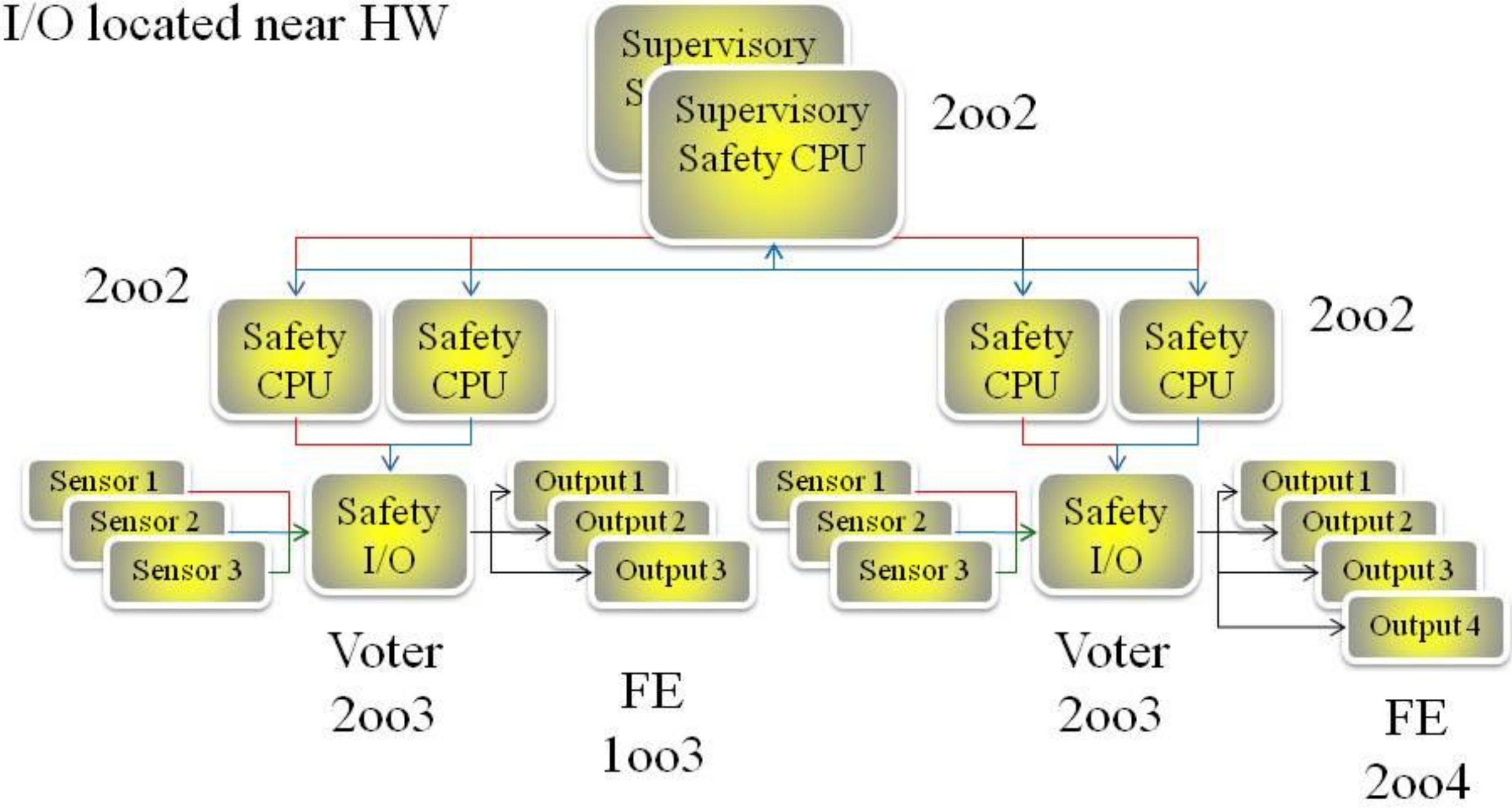
- Newly developed software assurance program
  - Risk based graded approach
  - Working towards CMMI implementation
  - Modeled on NASA program and ISO/IEC 12207

High Availability Architectures

High degree of fault tolerance

On-line test and repair

I/O located near HW



Conclusion

- JLab 12 GeV PSS design based on IEC 61511 standard
  - Addresses full lifecycle of system
  - Safety Functions assigned an SIL
  - Design Verified

- Major Requirements tied to Safety Assessments

- System Engineering process facilitates context for incorporation of all aspects of system design

- Quantification of Safety Functions supports exploration of unconventional architectures