Contemporary Programmable Safety Control Systems and Design Methods

Kelly Mahoney
TJNAF
Newport News, VA

Operated by the Southeastern Universities Research Association for the
U.S. Department Of Energy

Outline

- Historic Models
- Accelerator Safety Environment
- Safety Control Systems Defined
- Risk and Risk Management
- Standards and Design Methods
- System Architectures

Historic Models of Safety Practice

- Use – Fix – Use (Fly-Fix-Fly)
  - Titanic/Britannic
- Over Design
  - Empire State Building
- Reliability Design
  - Pre Apollo 1
- Safety Inclusive Design
  - Post Apollo 1
- System Safety
  - Post Challenger
- ???
  - Post Columbia?

Contemporary Methods

- Part of overall facility risk management program
- Use of standards as guidance
- Adoption of life cycle model
- Incorporated in to a safety program
- Documented hazard analysis
- Quantative Reliability analysis
- Use of programmable logic systems
- Specialty engineering
- Coverage of multiple hazards
- Merger of equipment and personnel safety
- Newer machines need safety systems as part of environmental safety management

Changing Horizon Outside

- US Congress has mandated that U.S. Department of Labor (OSHA) and Nuclear Regulatory Commission (NRC) develop plans to assume responsibility for safety regulation of non-reactor DOE facilities.
- OSHA and NRC have strict regulations requiring use of “accepted good practice” methods.
- Both have authority to assess fines or bring criminal charges.
  - No more mia culpa
- Failure to follow accepted good practice can be considered a “Willful Violation” with fines starting at $77k per citation.

OSHA Guidance

- Safety program conforms to accepted “good practice”
  - Standards
  - Interpretations
  - Regulations
- Personnel are recognized as “competent” in their field
  - Certifications
  - License
  - Specific Training
- Safety programs are well documented
- Safety programs are used

Changing Horizon Within

- New and planned machines push the intensity and energy envelopes to new highs.
- At the same time availability goals are approaching 100%
  - False trips reduce availability
  - High intensity beam loss leads to high radiation areas outside shielding
- Investment in exotic and unique machine elements is required to meet goals.
- Mixing greater investment in equipment with greater risk for damage.
- Hazards considered equipment protection have risk reduction requirements similar to personnel protection systems.

SNS – Multiple Solutions

- Normal Access Controls and Personnel Safety interlocks
  - Industrial PLCs in safety approved configuration
- Normal Equipment Protection
  - Custom Design Modules
- Injection Foil – High Risk equipment protection
  Equipment Protection < Injection Foil < Personnel Safety
  - Industrial PLCs in high reliability configuration
- Target - Liquid Hg
  Personnel Safety < Target Protection
  - Personnel, Environmental, and Equipment consequences

US Lab's Head Start

DOE Labs started move to external standards for design of safety systems.

JLab	1990	UK HSE (now IEC 61511)
RHIC	1995	MIL STD
SNS	2000	ANSI/ISA S84
Fermi	2001	ANSI/ISA S84 (policy change CD0)
SLAC	2002	ANSI/ISA S84 (policy change ESA)

Most DOE Accelerator Labs are now looking at IEC61508/IEC61511

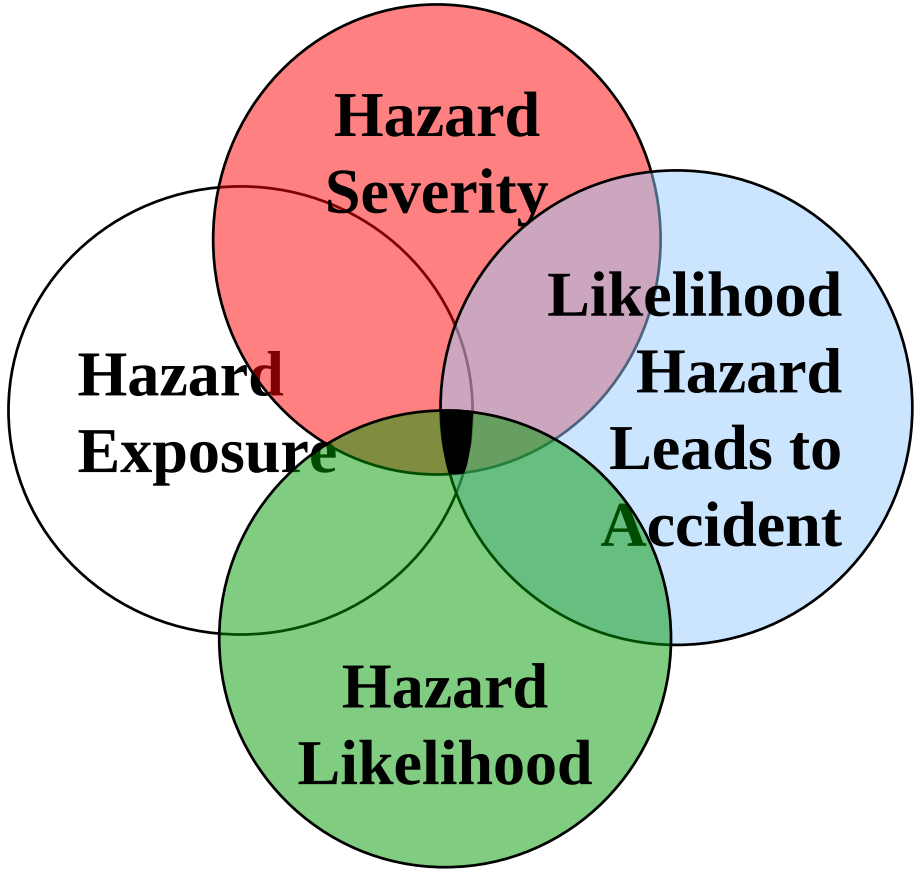
Labs are moving to a risk based safety management approach

EU Labs

- Use IEC61508 for both personnel and equipment protection.
  - LHC IEC 61508
  - Diamond IEC 61508

Risk

Combination of Severity, Likelihood, Impact, and Exposure

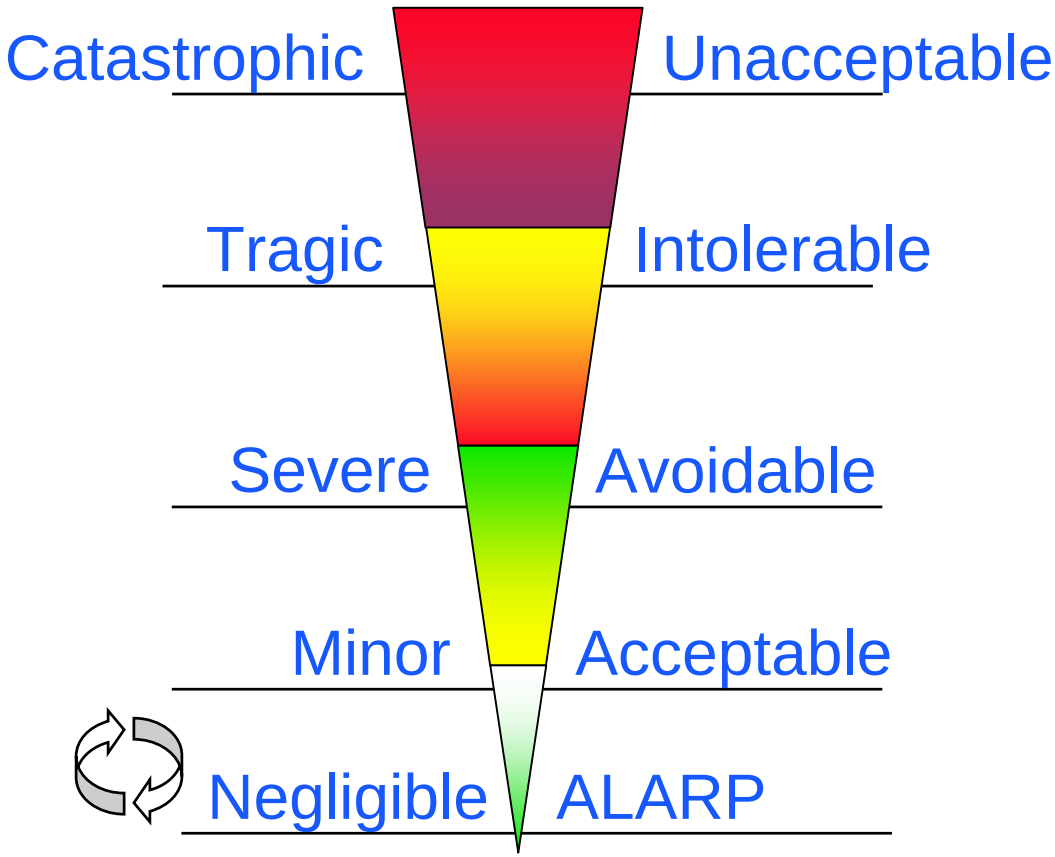


Risk of Incident !

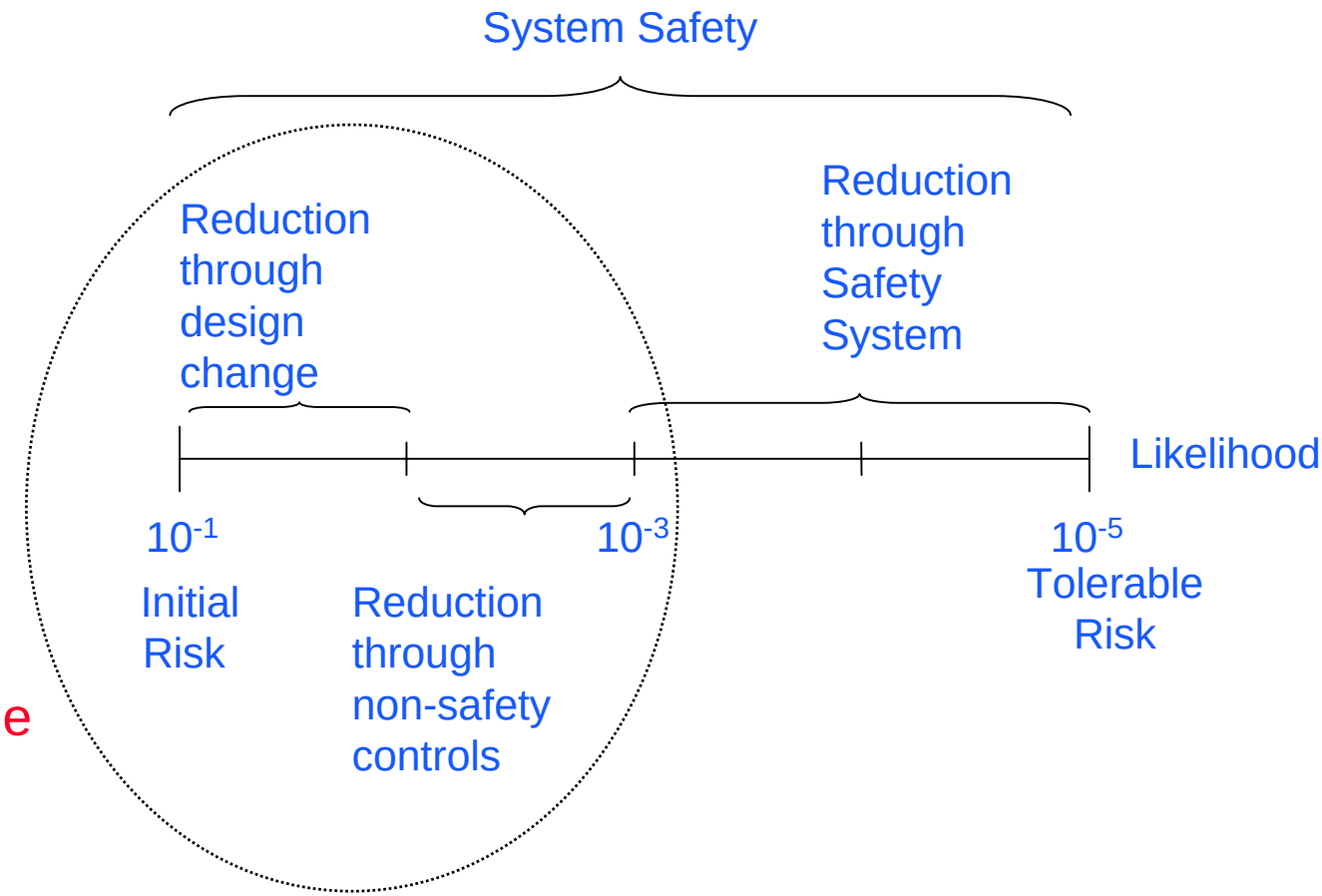
Objective

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

Potential incidents over the lifetime of a facility

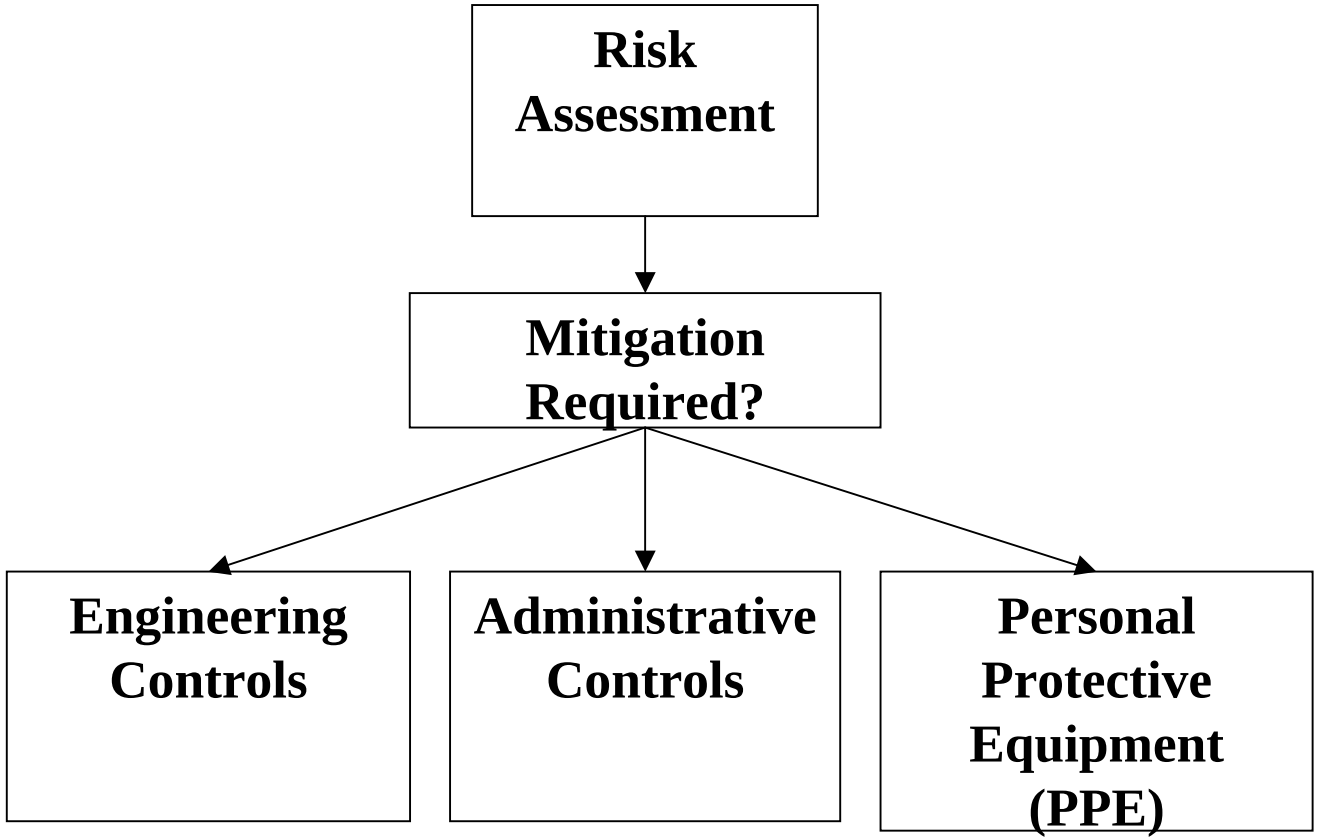


Risk Reduction

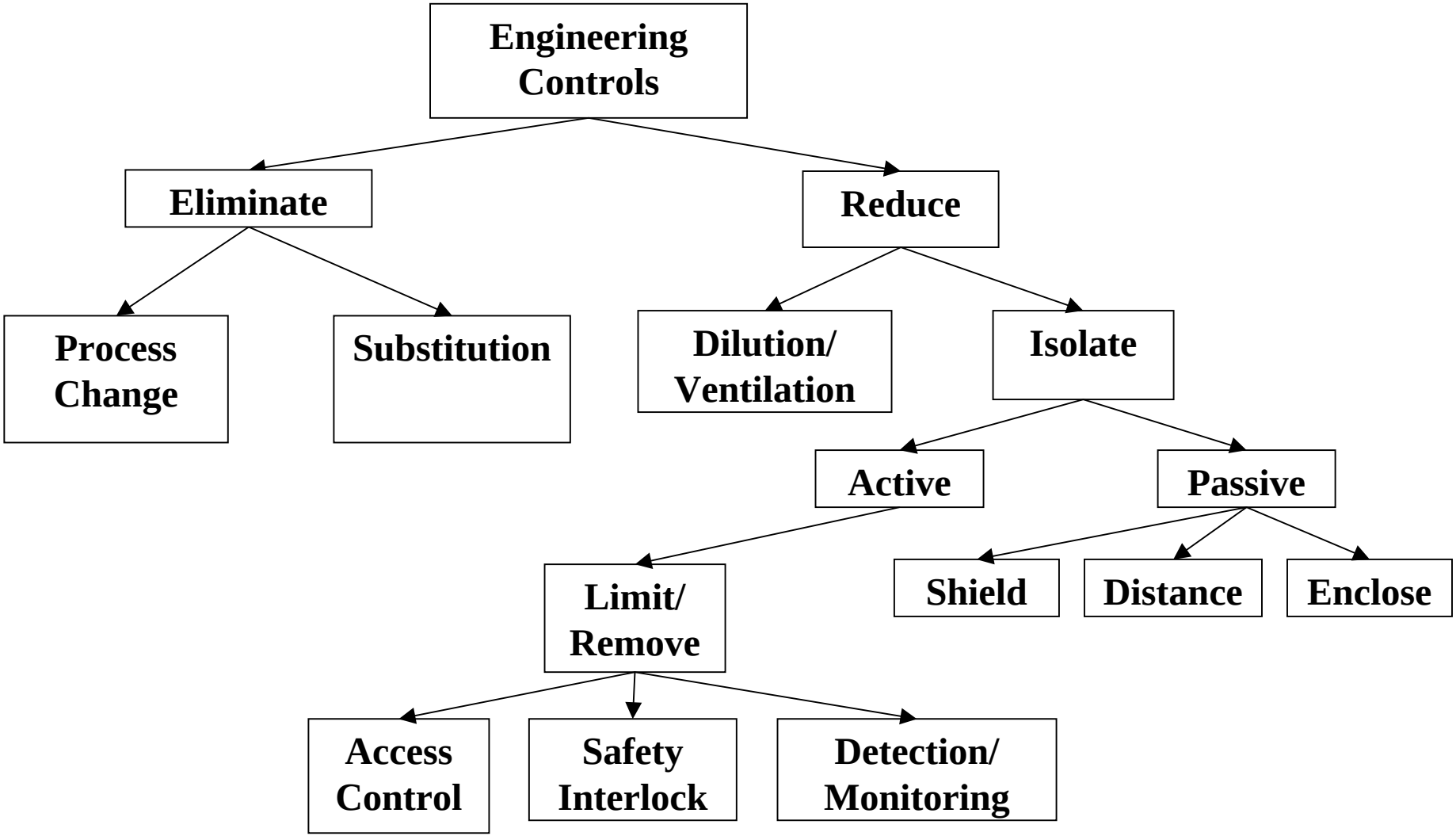


This is the part that is hard to manage over the lifetime of the facility

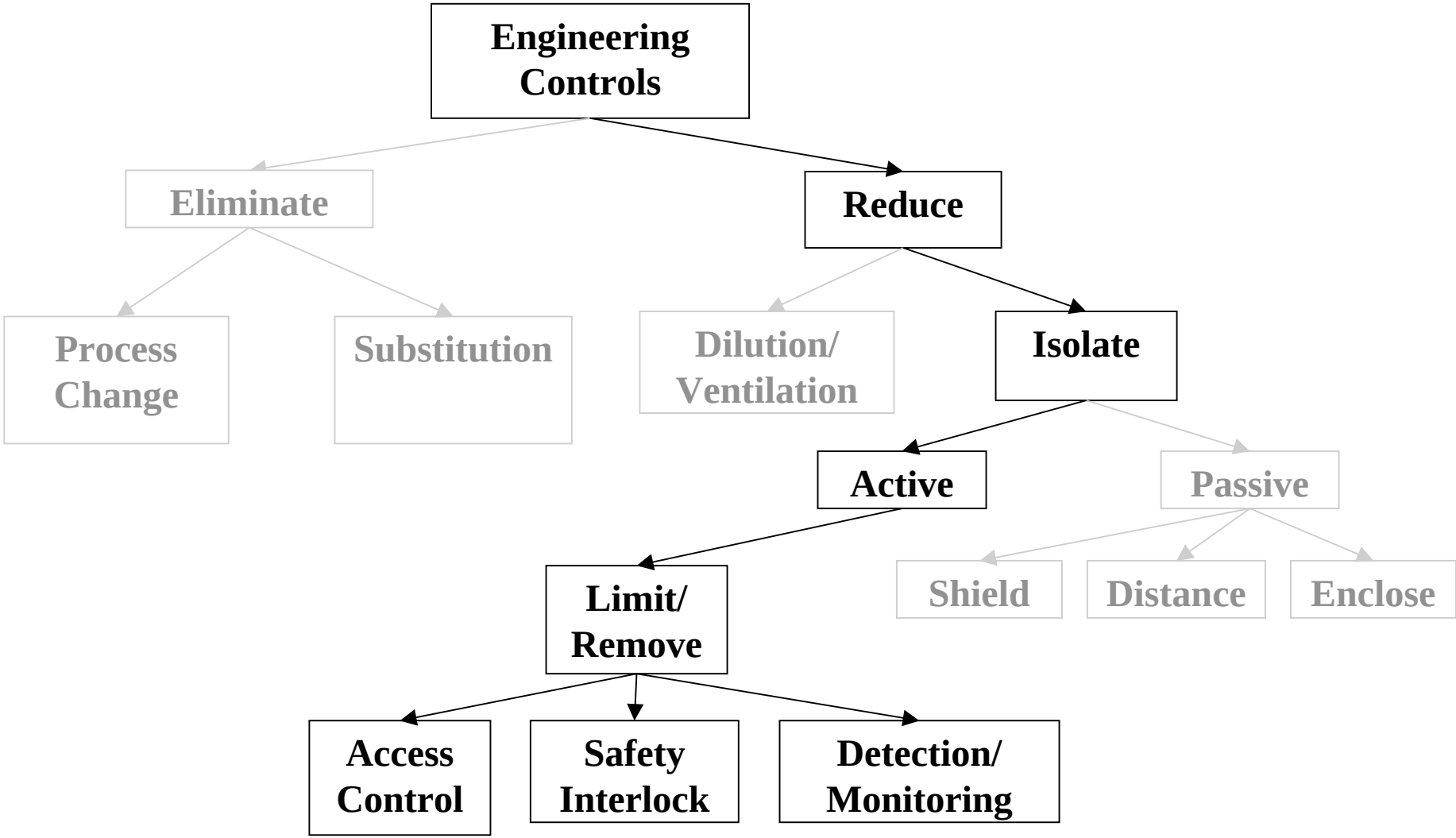
Basic Hazard Controls



Engineering Controls



Engineering Controls



Safety Systems

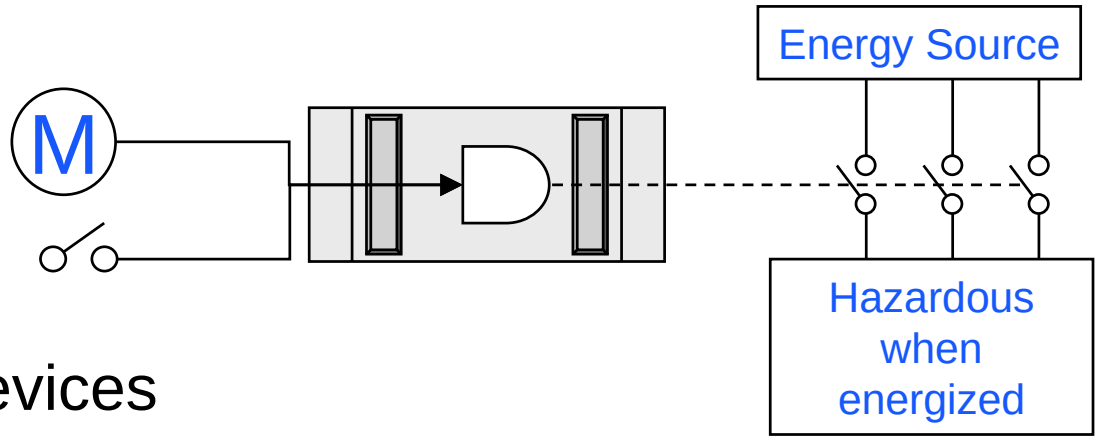
A Safety System is an engineered system that reduces the risk of harm to people, equipment, or the environment that may arise from the operation of a process or equipment.

General Attributes of a Safety System:

- Autonomous – acts on it's own to achieve a safe state
- Requires kinetic energy external to the process (although fails-safe)
- Sensor $\Rightarrow$ Logic $\Rightarrow$ Final Control Element

Elements of a Safety Control System

- Sensors
- Decision Logic
- Final Elements/Devices



SIL

- A classification of the risk reduction needed or provided by a safety system
  - Expressed in numbers tied to Probability of Failure to Danger (PFDavg, PFD)

- NOT a rating that can be applied outside the context of a specific safety system implementation
  - e.g. there is no such thing as a “SIL3 PLC.”

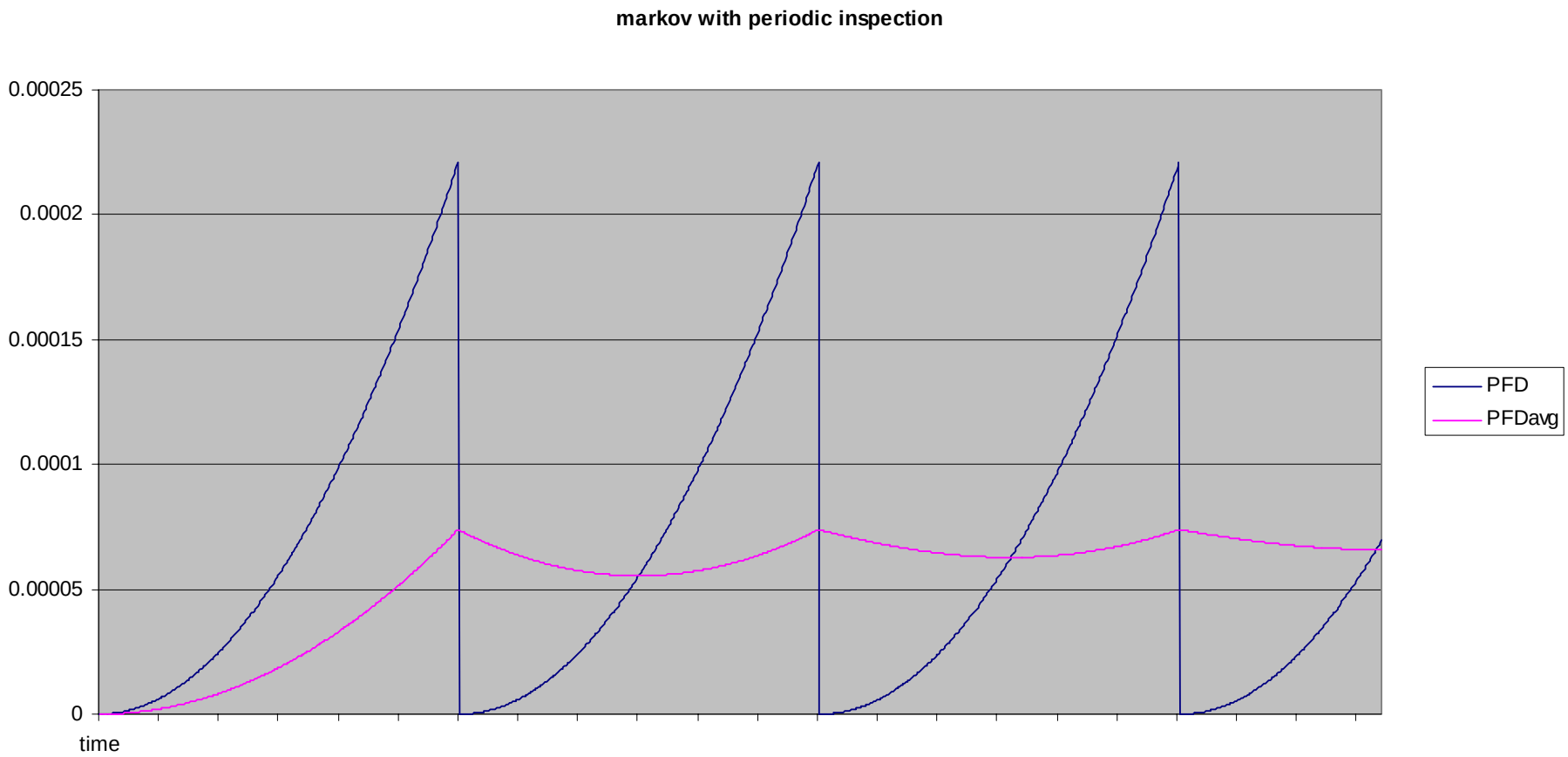
Safety Integrity Level – SIL

ICALEPCS 2003

DEMAND MODE OF OPERATION		
Safety Integrity Level (SIL)	**Average Probability of Failure on Demand**	**Risk Reduction**
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to ≤ 100,000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤ 10,000
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤ 1000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤ 100

CONTINUOUS MODE OF OPERATION	
Safety Integrity Level (SIL)	**Frequency of Dangerous Failures Per Hour**
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

PFD average vs. PFD



Example PFD and PFD avg. of 1002 shutdown system

Accelerator Safety Control Systems - ICALEPCS 2003

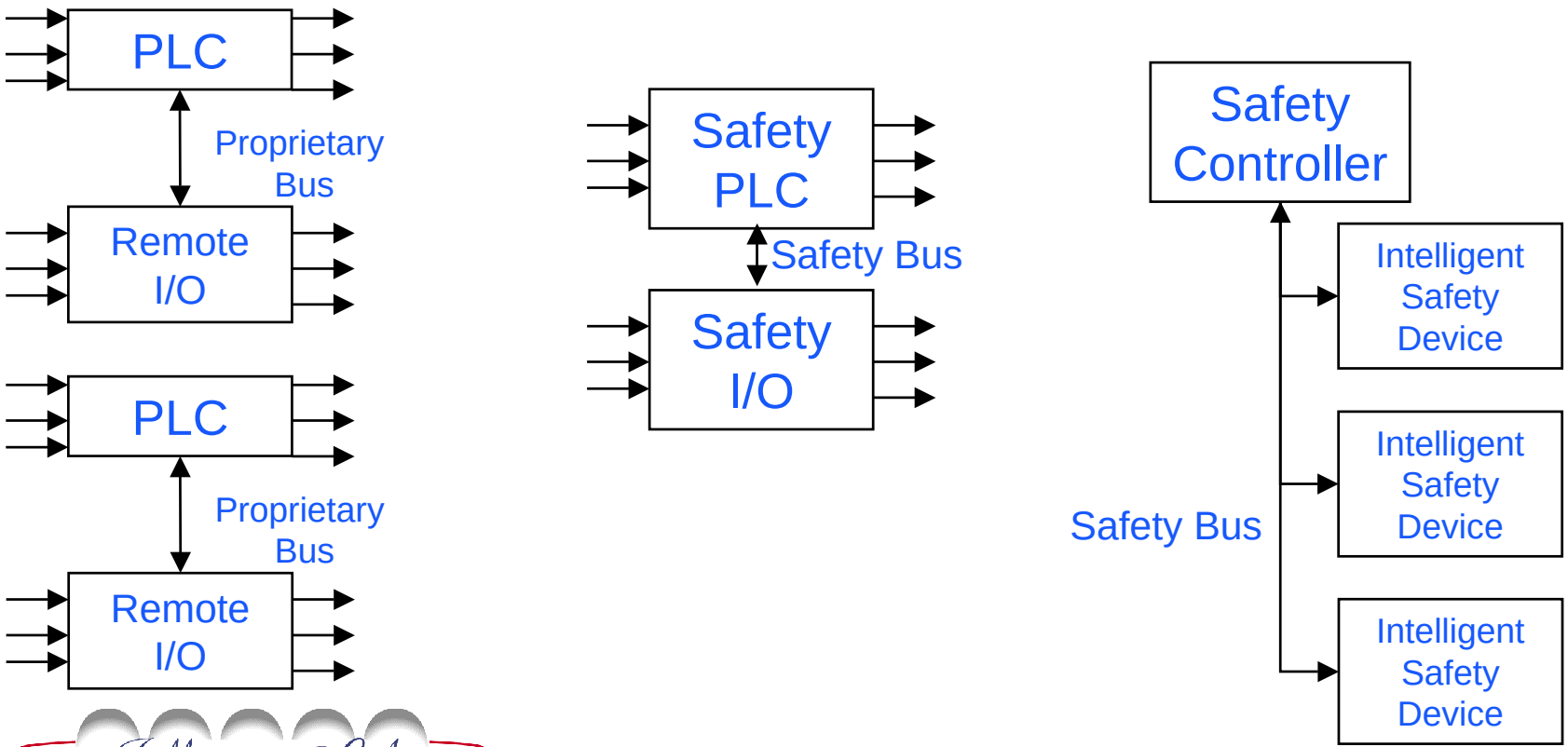
- Prompt Ionizing Radiation
- Residual Ionizing Radiation
- Equipment Protection
- Oxygen Deficiency
- Fire/Explosive (Hazardous Classified) Areas
- Laser Radiation
- Other Non-Ionizing EM Radiation
- Open Machinery
- Exposed Electrical Equipment
- Chemical Processes
- Biological Research Facilities

JLab Safety Systems

- JLab is using high reliability design principles in several areas. Systems are designed to a level that is appropriate to the hazards and risk.
  - Test Facility
  - CEBAF Accelerator
  - Explosive gas monitoring
  - FEL
  - Laser Labs
  - Chemical Processing Rooms
  - RF Test Stands
  - Cryomodule Test Facility
  - Cavity Test Area

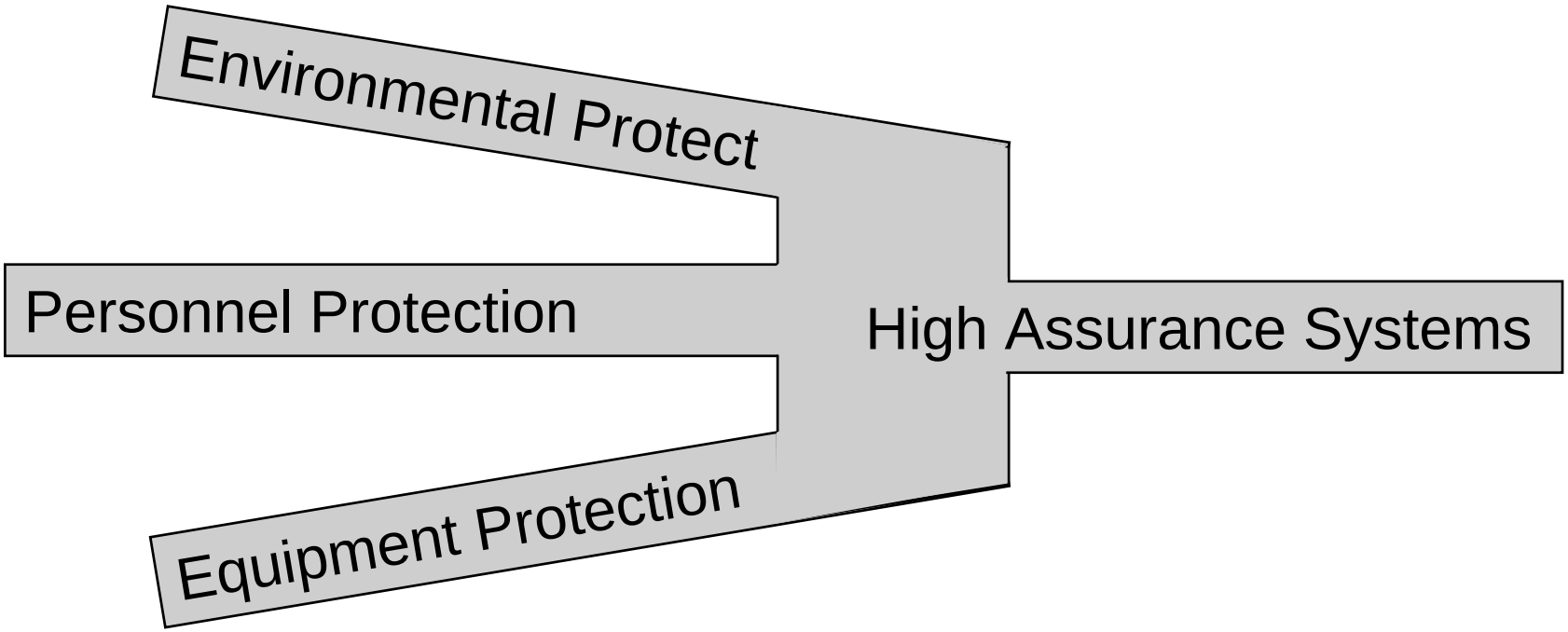
Safety Systems

Accelerator Custom Design	Process Safety Design	Machine Safety Design



Operated by the Southeastern Universities Research Association for the U.S. Department Of Energy

Merging Design Practices



High reliability engineering design practices are required in several areas.

Expertise is being pooled to address common equipment/needs.

Applicable Standards

SAFETY SYSTEM STANDARDS

Custom Design

IEC 61508

System Integrators

ANSI/ISA S84

IEC 61511

Simple Access Control/Interlocks

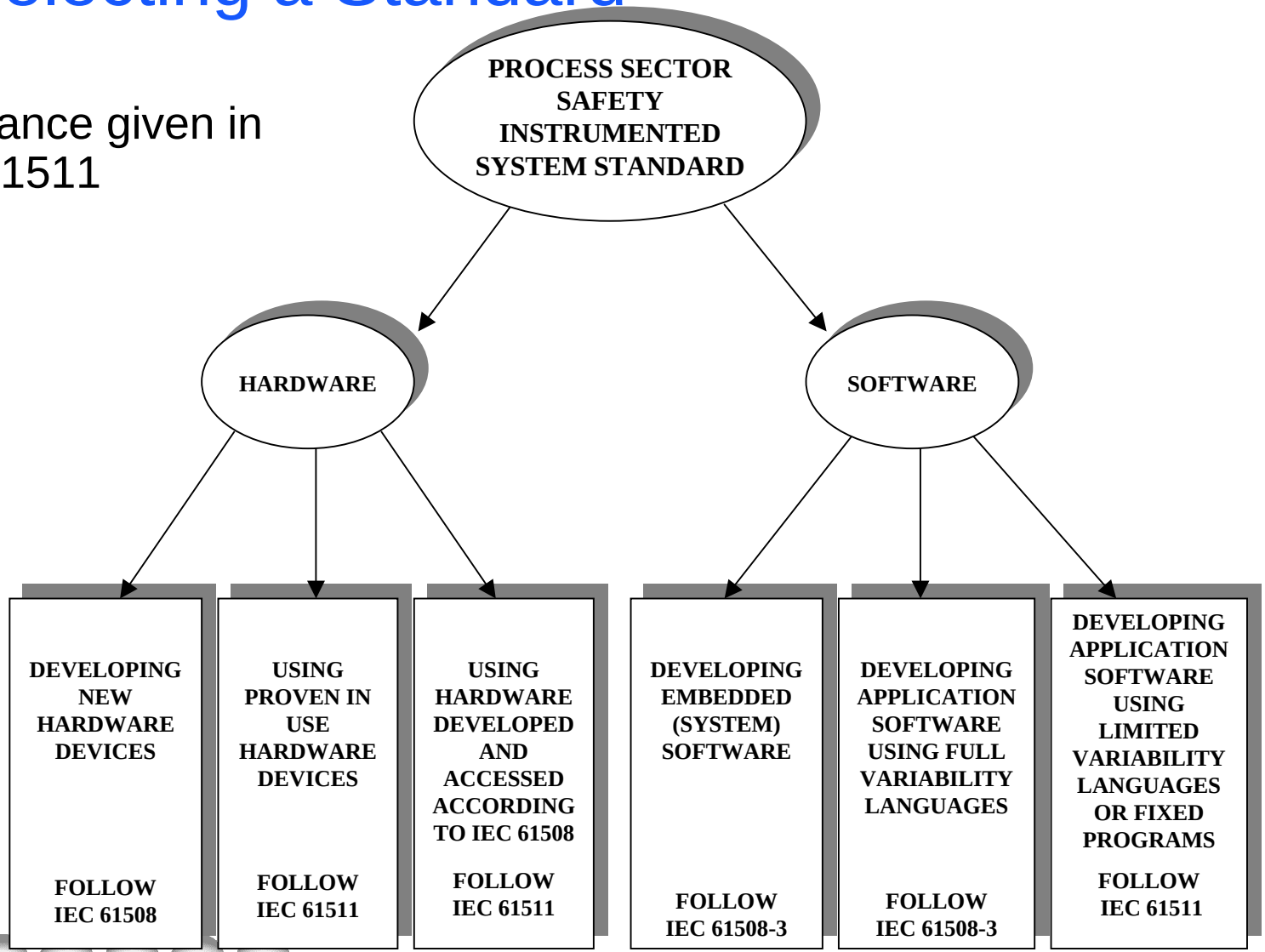
EN954-1

IEC d62061

ANSI B11.xx

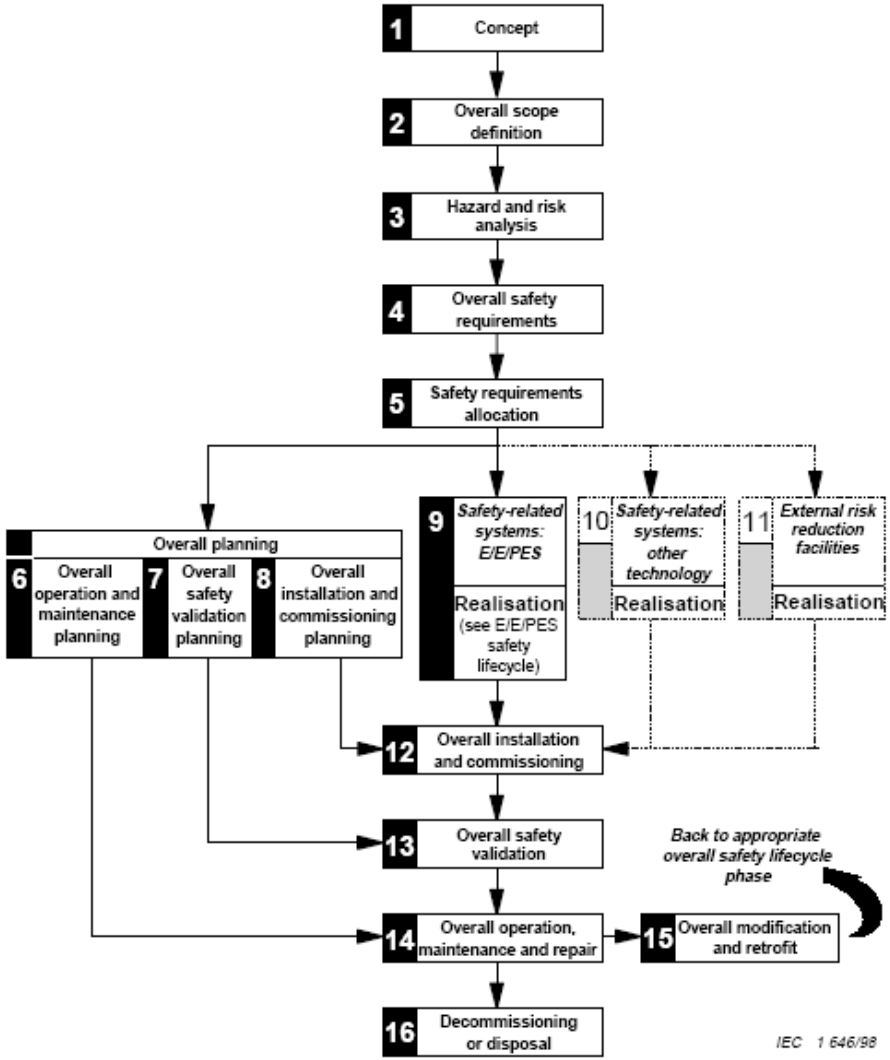
Selecting a Standard

Guidance given in IEC61511



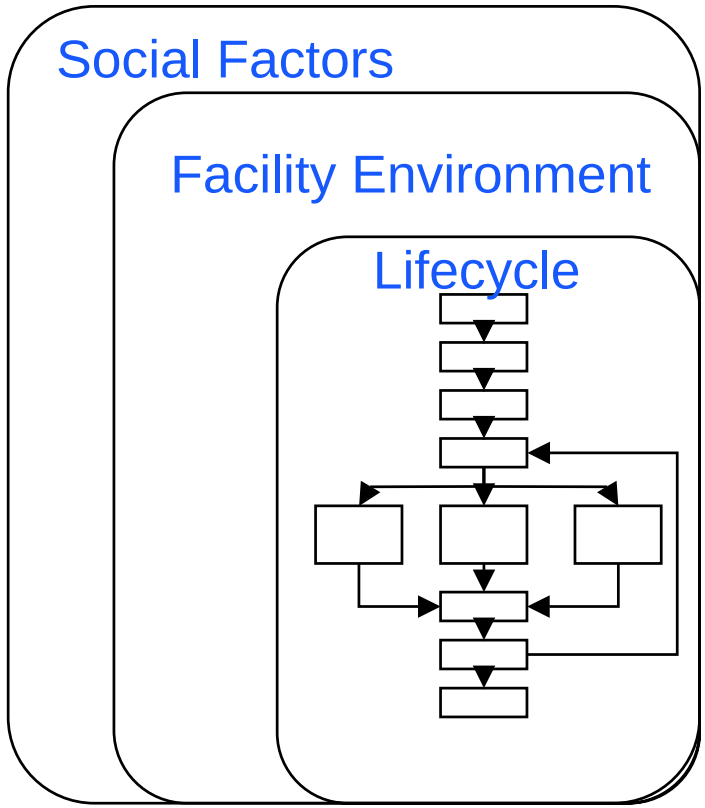
IEC61508 Lifecycle

- Manages lifecycle from concept to decommissioning



Expanding the Envelope

- Current standards address lifecycle items that directly affect safety system.
- Only address other contributions to overall risk reduction at the outset of the project. Not part of the feedback loop of the lifecycle.



JLab Requirements Docs

- JLab SSG Requirements Documents Include:
  - Intent Specification
    - Non-technical description of why the system is needed, important aspects of the system, generalized priorities.
    - Aimed at non-system technical experts, e.g. programmers
  - Assumptions at the time the system is implemented
    - Environmental assumptions
    - Regulatory assumptions
    - Configuration Assumptions
    - Operational assumptions
    - Training assumptions
    - Things that used to start with the word “Obviously”
  - Discussion
    - Non-technical description of the system, operational aspects, constraints.

JLab Requirements Docs –Cont'd

ICALEPCS 2003

- General Requirements
  - Quasi technical description of system and subsystems
- Specific Requirements
  - Verifiable description of device or subsystem behavior.
  - The "shalls", "shoulds", "mays" live in this part
- Quality Assurance
  - Test Requirements
  - Documentation Requirements
  - Process requirements (e.g. deign reviews)

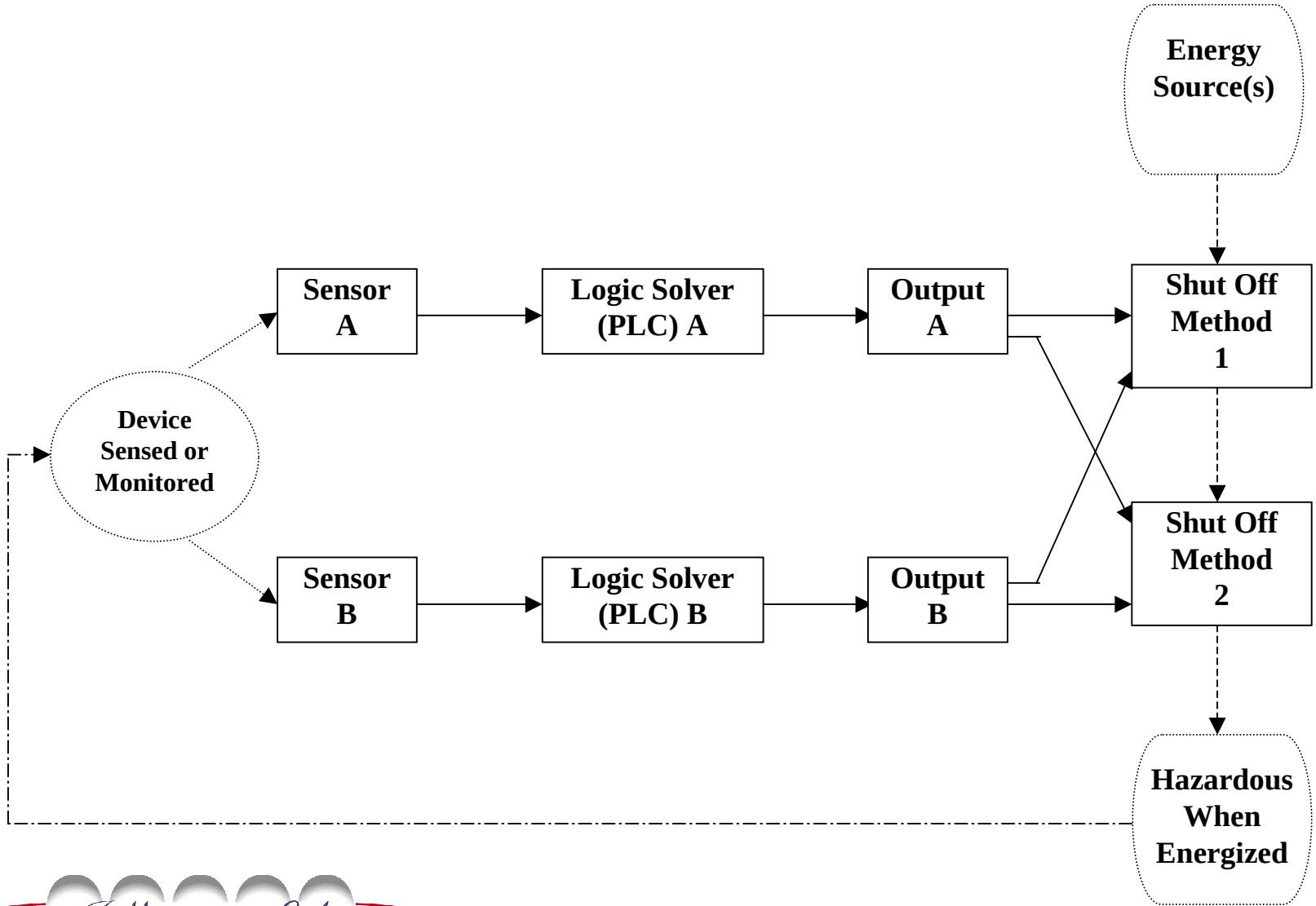
Programming Languages

- Fixed Programming Language (FPL)
  - Embedded Code, ASIC, FPGA,…
  - Only operating parameters may be changed
  - Example: Smart Sensor

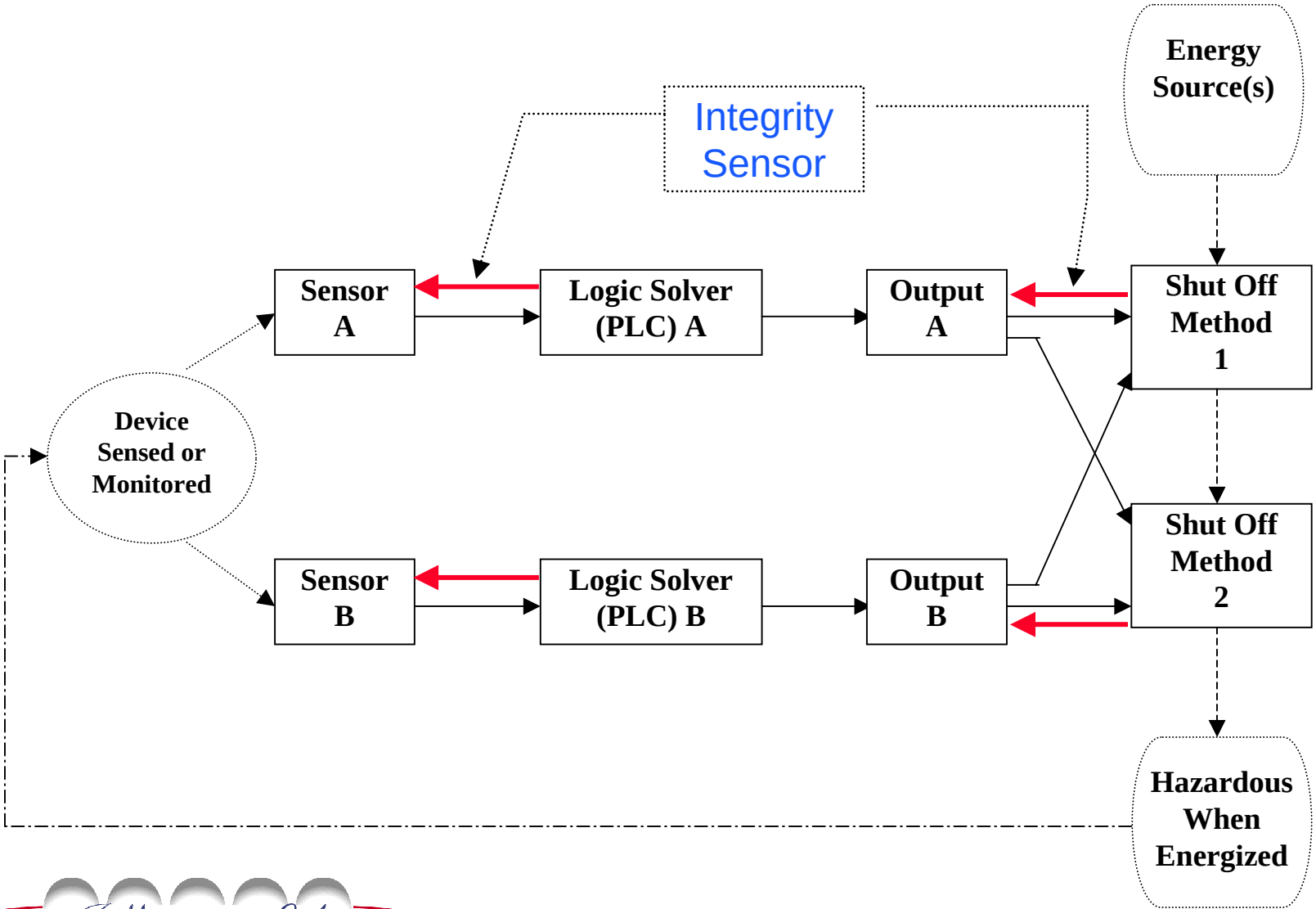
- Limited Variability Language (LVL)
  - Most PLC development languages (IEC61131-3)
  - Programs run in restricted memory space. Restricted by hardware, e.g. disable write line on user memory.
  - Program with functional modules
  - Example: PLC

- Full Variability Language (FVL)
  - General Purpose Languages, C, C++, JAVA, ADA,…
  - Allowed to write any value to any memory space
  - Includes modules implemented in a “wrapper” or similar software security feature.

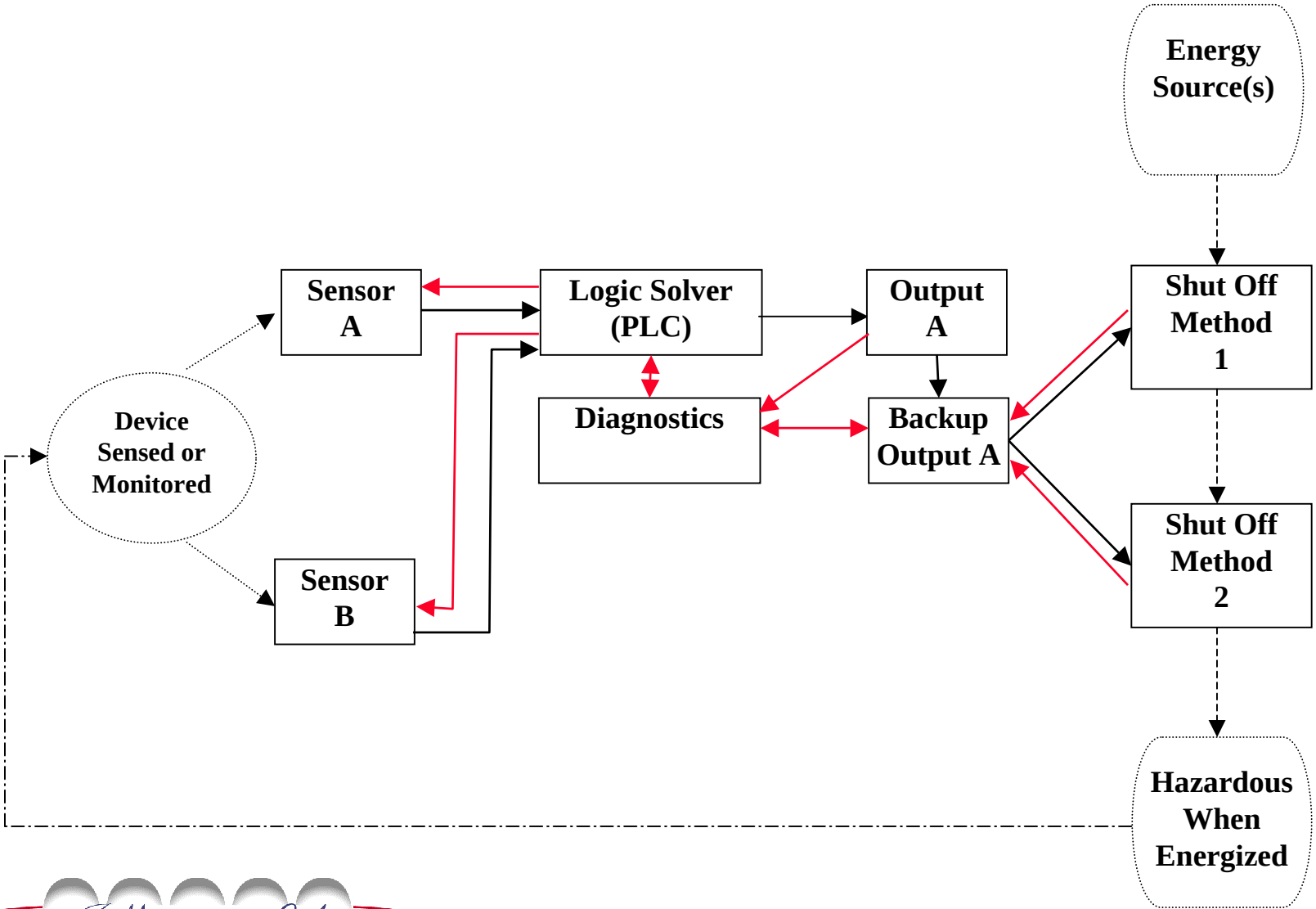
Traditional Architecture



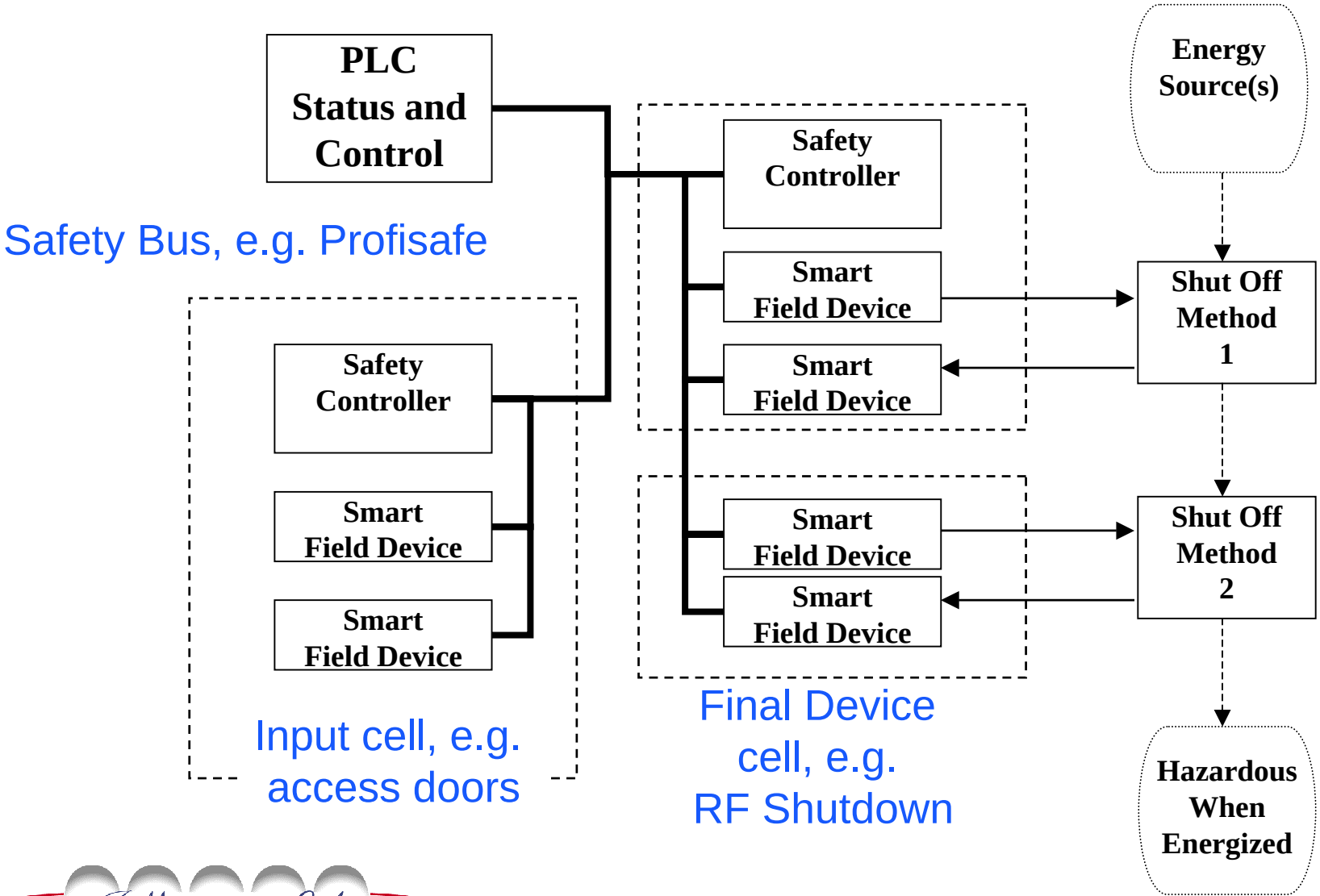
Modified Traditional Architecture



Safety PLC


Energy Source(s)
Sensor A
Logic Solver (PLC)
Output A
Shut Off Method 1
Device Sensed or Monitored
Diagnostics
Backup Output A
Sensor B
Shut Off Method 2
Hazardous When Energized

Distributed Safety Cells

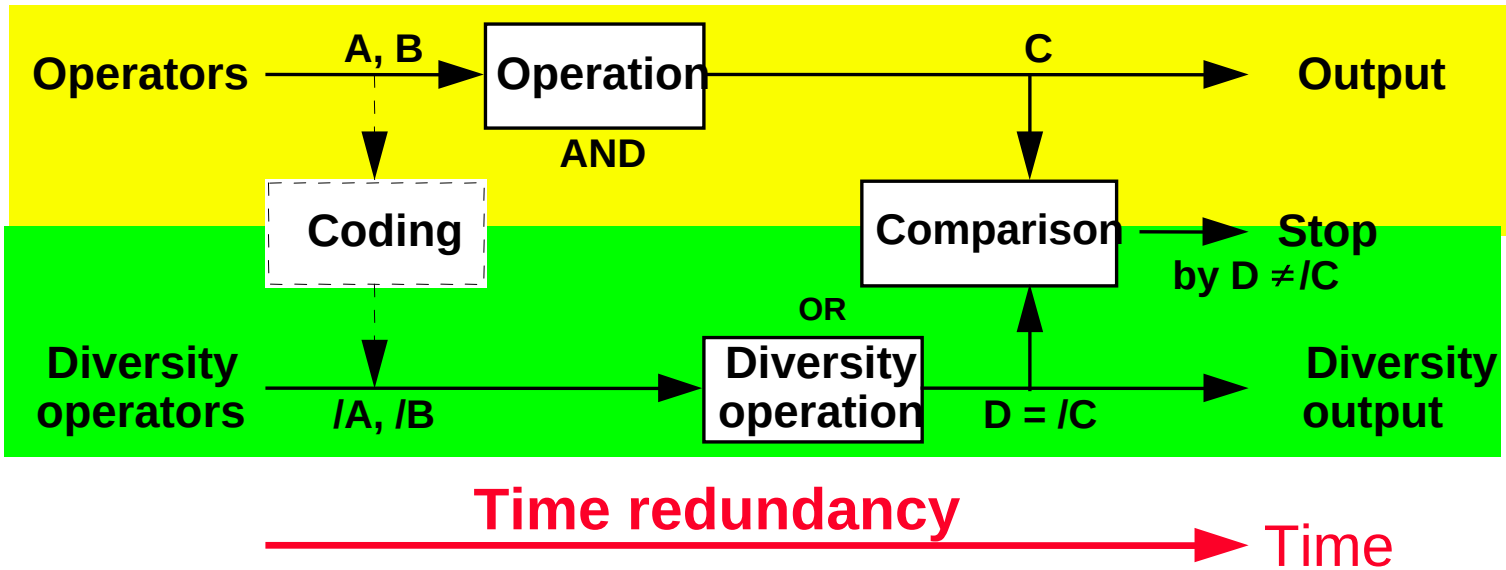


PLC Types

	Industrial PLC	Process Safety PLC	Machine Safety PLC
Program Space	Common Memory Space	Protected Safety Memory Space	Protected Safety Memory Space
Program elements	User defined	Certified/Tested Function Library	Manufacturer Tested Safety Function Library
I/O	Monitored line available	Monitored Line	Monitored Line Available
Fail-Safe Backup	N/A	Internal relay or solid state switch	N/A
Available Single PLC SIL Ratings	1-2	3	3

Safety PLC Program Execution

Time redundancy / diversity
instead of structural redundancy



Courtesy of Siemens GmbH Arwit Lehmann

Operated by the Southeastern Universities Research Association for the U.S. Department Of Energy

Safety VME?

- Real Time Kernel Development SW approved for some critical safety applications
  - VxWorks ® AE
  - QNX® Neutrino® RTOS
  - Integrity® RTOS
  - ThreadX®

Eternal Questions

- Separation of safety and non safety functions
- Can one division of a redundant system be taken off line while the accelerator has one system remains on line for protection?
- What level of testing is required when a component is repaired or replaced?
- What level of testing is required when software is modified?
- What level of testing is required when the (supposedly) same version program is reloaded on a PLC?

Where are we going ?

From	To
Separate Equipment and Personnel Safety	Integrated Equipment and Personnel Safety
m oo n shutdown	n oo n shutdown
Processor with remote I/O	Distributed smart safety interlock cells
Manual Audits	Fully Automated Audits
Semi annual test intervals	Continuous test

감사합니다.

Kamsa-haminda

Thank You

System Safety and Safety Systems for Accelerators

June 28-July 2, 2004
University of Wisconsin
Madison, Wisconsin

Kelly Mahoney and Sandra Prior, TJNAF

http://uspas.fnal.gov/programs/wisc.html