Application of Standards to Accelerator Safety Systems

Kelly Mahoney

Fermi Standards ID Workshop

June 13, 2000

Outline

- Overview
- Context and Risk
- Standards
- Software
- Future
- Recommendations

Computer Safety

Help?

Hi! I'm from the government……

…….. And I'm here to help you

Background

National Technology Transfer and Advancement Act of 1995 [Public Law (PL) 104-113]

"Federal Participation in the Development and Use of Voluntary Standards..."

"PL 104-113 is a true shift in the paradigm for many Federal agencies regarding the conduct of their technical standards activities. Where DOE, in its continued transition to a "work smart", standards-based operating culture, identifies the need for new or revised technical standards, PL 104-113 compels us to focus all technical standards development efforts deemed necessary toward voluntary standards in lieu of DOE technical standards. "

Assistant Secretary for EH

Pedigree of a DOE Standard

PL104-113

Necessary and Sufficient

Work Smart Standards (DOE 450.1)

Policy

Implementation

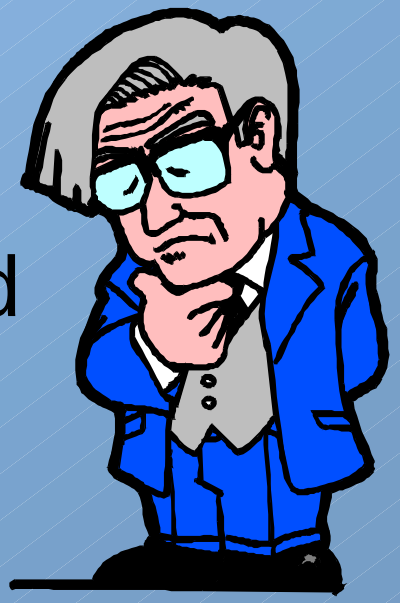
Evolution of Requirements

Chemical Hazard	Ionizing Radiation	High Power Laser
29CFR1910.1000	10CFR835	29CFR1910.97
EH&S Manual	RadCon Manual	EH&S Manual
SEMI S93.2	NCRP 88	ANSI/Z136.1
	ANSI/dN43.1	
Safety System	Safety System	Safety System

ANSI/ISA S84.01-1996

Why Standards?

- Need to move from a qualitative to a more quantitative evaluation of risk and risk reduction.
- Establish a context where ideas and solutions can be exchanged



Why Standards?

- The trick is to develop standards that are not overly prescriptive.
- Standards that are applicable to a wide group of users.
- Standards that add value to the organization and tasks at hand.
- Standards that are not obsolete the day they are published.

Definition of a Safety System

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.

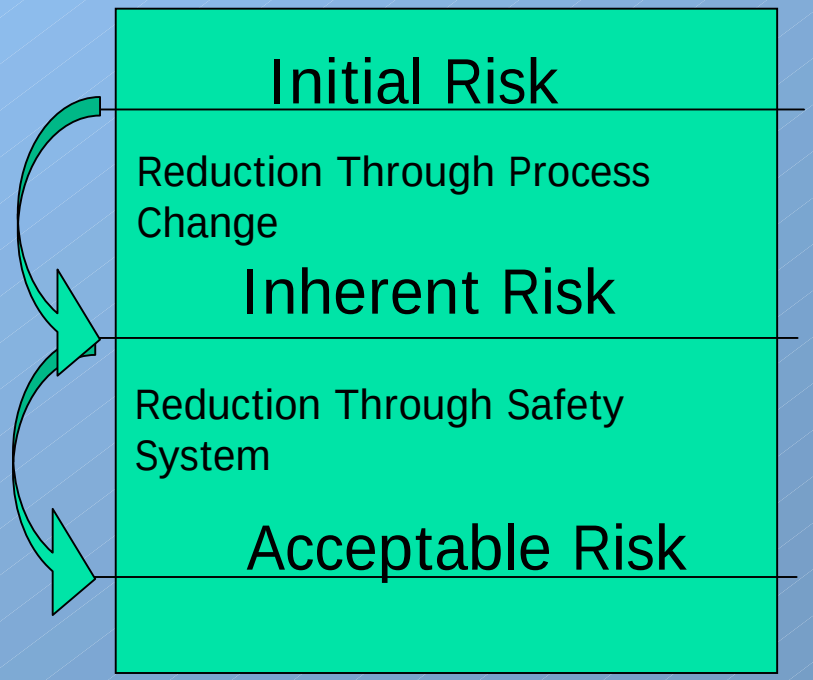
General Attributes of a Safety System:

- Autonomous – acts on it's own to achieve a safe state
- Requires kinetic energy to function
- Sensor $\Rightarrow$ Logic $\Rightarrow$ Final Control Element

Risk Reduction Factor

$$RRF = \frac{\text{Inherent Risk}}{\text{Acceptable Risk}}$$

Inherent Risk – Risk left over after other methods to reduce risk have been taken.



The New Jargon

- Safety Function
  - Function to be implemented by a safety system which is intended to achieve or maintain a safe state for the process, in respect to a specific hazardous event
- Safety Instrumented System
  - A Safety System
- Safety Integrity Level
  - Discrete level for specifying the safety integrity requirements of the safety functions allocated to a safety system

Safety Integrity Level (SIL)

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 $<10^{-5}$

Safety Integrity Level (SIL)

- A classification of the risk reduction needed or provided by a safety system
  - Expressed in numbers tied to Probability of Failure on Demand (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.”

Why Have SILs?

- SILs allow a common understanding of the required target risk reduction level that a safety system must achieve.
- In a 1995 survey of accelerator safety systems the following were some of the responses given to the question " Was there a design goal for safety system reliability ?"
  - 86% Said No failures — SIL - Never
  - 14% said 10^{-6} per year — SIL – 1 (Continuous Mode)
    SIL – 4 (Demand Mode)
  - 4% said 0.5 To 1 per year — SIL – Get a new job

Range = 10^{0} to $10^{-\infty}$!

Experience

- Experience has shown that accelerator applications are generally around SIL 2-3

i.e. PFD = 10^{-2} to 10^{-4}

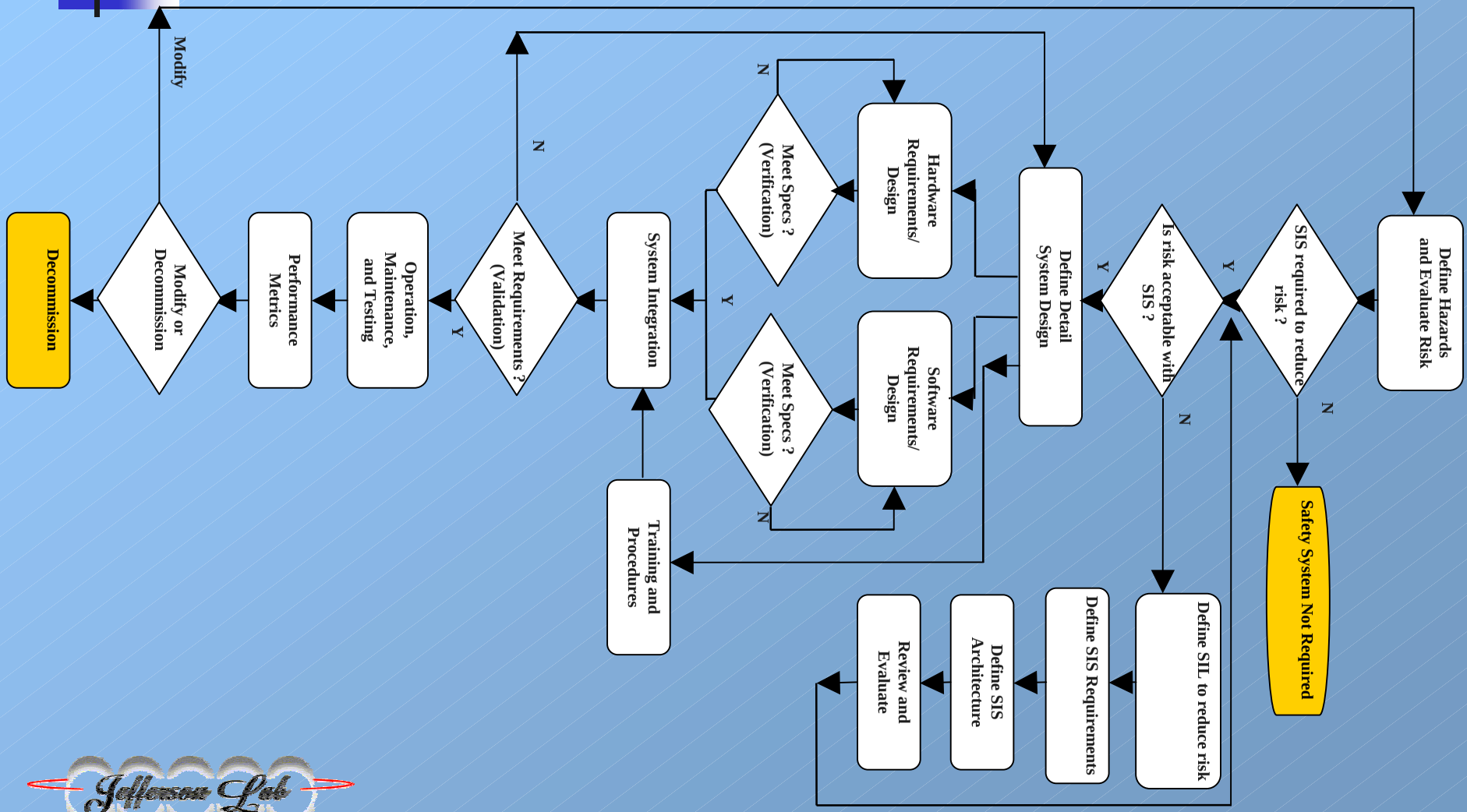
Hazards Requiring Interlocks

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

Process Steps in Reducing Risk

- Define and Evaluate the Risk
- Design out as much of the risk as possible
- Define Safety Functions
- Evaluate the need for a safety system
- Define the Risk Reduction required
- Develop a Safety System architecture to meet required level of risk reduction
- Maintain the necessary degree of safety over the lifetime of the application

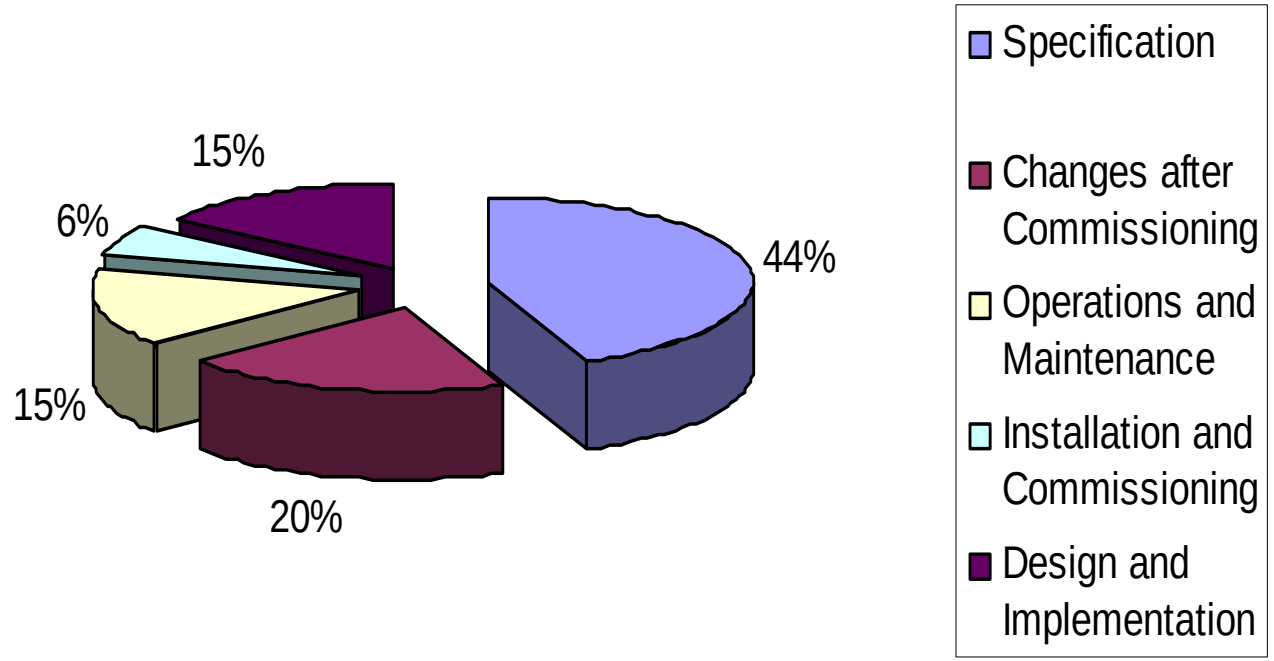
Safety System Lifecycle Model



No Room for Error

1995 UK HSE survey of 34 accidents that were a result of safety system failures.

64% of the failures were attributed to poor specifications or changes after commissioning.



From: 'Safety Shutdown Systems', P. Gruhn and H. Cheddie
ISA Press 1998

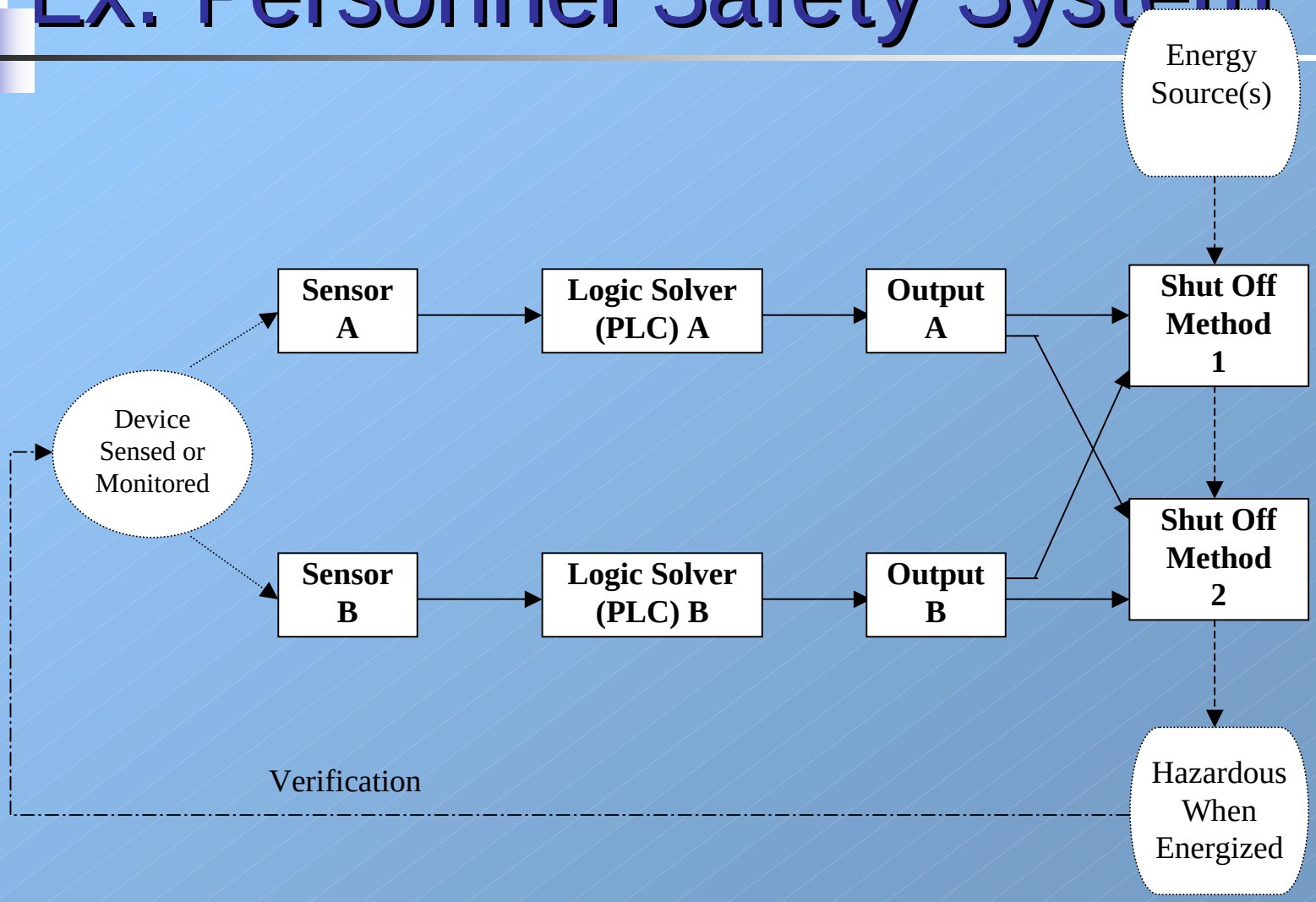
One Standard Does Not a Policy Make

- Requires management commitment to entire lifecycle
- Includes risk evaluation and classification
- Design Evaluation
- Responsiveness to Customer Input
- Management of Change

The Benefits of Risk Based Design

- Safety System design can be appropriate to address the level of risk
  - Prescriptive approaches can be avoided
- Hazards of similar risk level can be addressed similarly
  - Moves safety system implementations from a vertical, hazard specific approach to a horizontal, safety system based approach.

Ex. Personnel Safety System



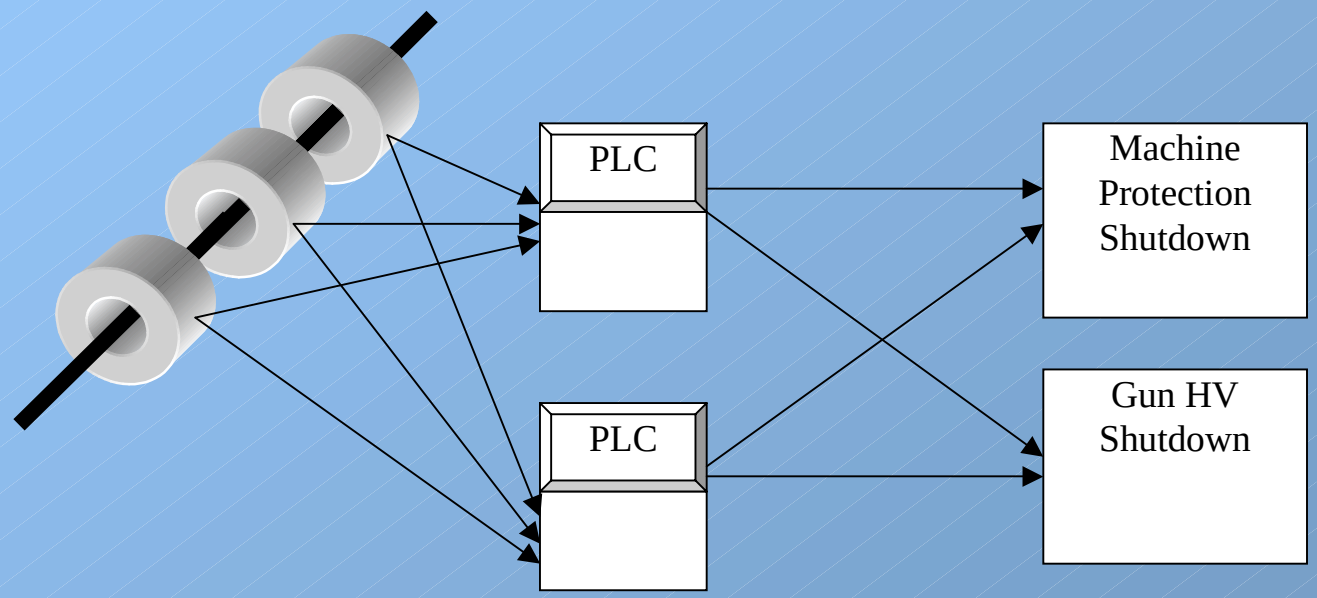
Ex. Beam Envelope Monitor Sys.

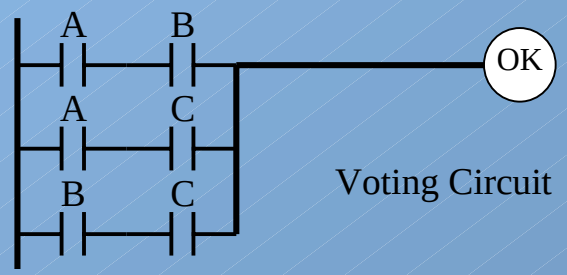
Non Traditional implementation

Inputs paralleled

Voting Circuit

Complex Math





Voting Circuit

Managing Risk

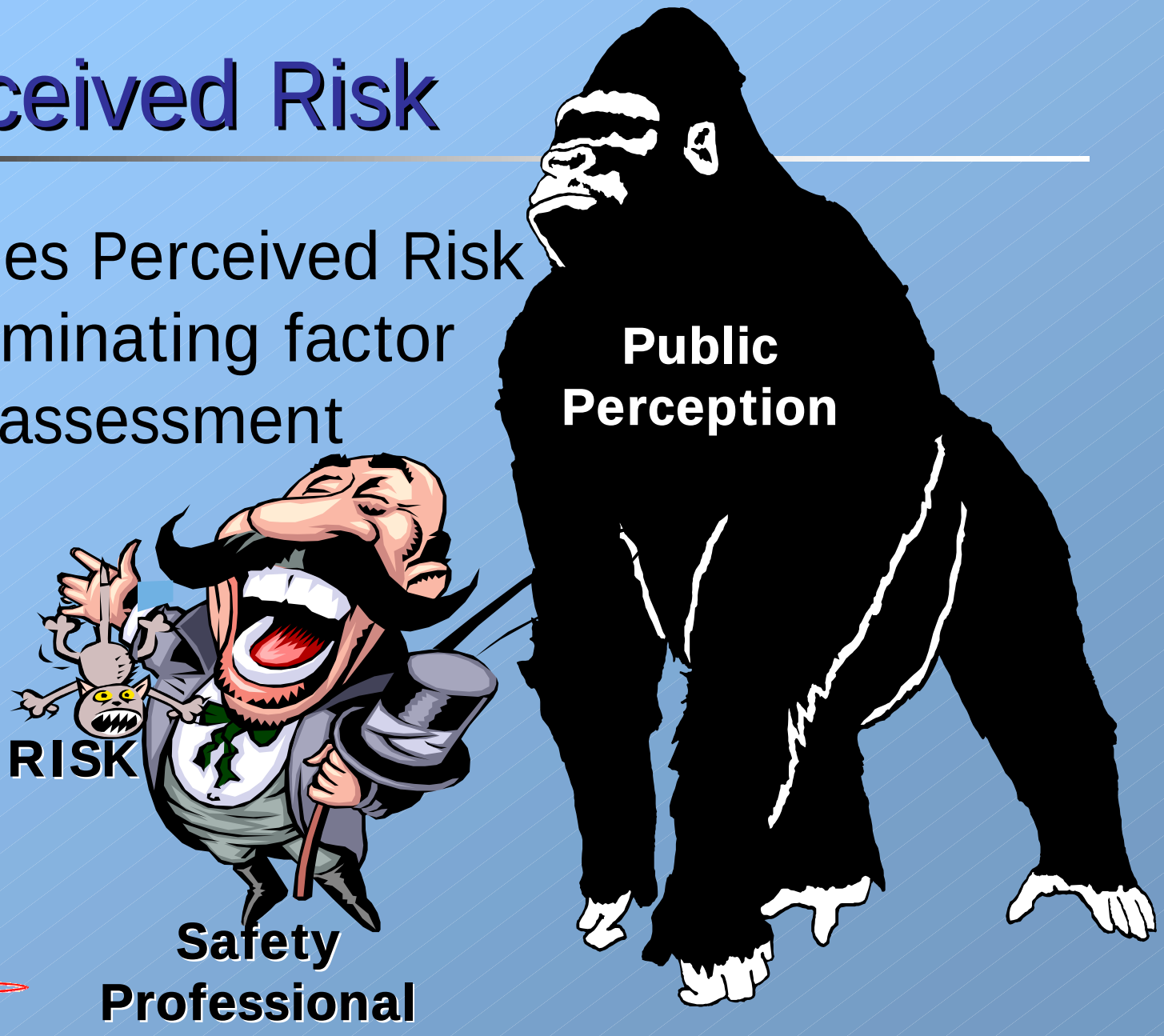
- Qualitative Risk Assessment
  - The target could explode within the next 4 years
- Calculated Risk Assessment
  - The probability of an event that could lead to the target exploding is 2.5×10^{-1} per year

Managing Risk

- Perceived Risk
  - Management
  - Safety Professional
  - Employee
  - Public
  - DOE

Perceived Risk

Sometimes Perceived Risk is the dominating factor in a risk assessment



Assigned Risk

- Assigned Risk is the product of the calculated and perceived risk reduction factors.
  - $R_A = R_c * R_p$

Management of Change

- Ensure that lifecycle is not broken
- Established procedures for change
- Plan for decommissioning

Management of Management

Management must understand their responsibilities

- Assume responsibility for acceptable level of risk
- Provide staff adequate resources and training
- Establishment of policy and strategy for achieving safety goals

Standards

- Non-Nuclear classified accelerators have the same level of hazards as found in private industry. (Perceived risk not withstanding)
- Radiation is classified as an industrial hazard.
- So why not use industry standards?

Types of Standards

- Implementation Prescriptive
  - Nuclear Industry
  - Air Craft
  - Space
- Consensus
  - Process Industries
  - Manufacturing Industries
  - Research and Development

International Standards

SAFETY SYSTEM STANDARDS

Manufacturers & Suppliers of Devices

IEC 61508

Safety Instrumented Systems Designers, Integrators & Users

ANSI/ISA S84

IEC 61511 (CDV)

ISA S84

- Consensus Standard
- Designed to meet 10CFR1910.119
- Best Practice of AIChE
- Wide Body of Experience
  - Equipment Manufacturers
  - System Integrators
  - Reliability Engineers
  - Academia

ISA S84

- 12 Chapters
- 3 Informative Annexes
- Deals mostly with the programmable section of the safety system

S84 Gaining Acceptance

March 31, 2000 - "As S84.01 is a national consensus standard, OSHA considers it to be a recognized and generally accepted good engineering practice for SIS (Safety Instrumented Systems),"

Richard E. Fairfax, Director, Directorate of Compliance Program Assistance for OSHA

Refers to S84 in the context of requirements of 10CFR1910.119 Hazardous Chemical Controls

TR84.02

- Guidance to S84 for determining safety integrity level (SIL) of a safety system
- Gives Three methods for calculating SIL
  - Simplified Equations (Block Diagram)
  - Fault Tree
  - Markov Model
- Part 5 gives methods for calculation of PFD of logic solver using Markov models.

IEC61508

- Umbrella Standard intended to cover all industrial safety system applications
- Very detailed, almost prescriptive
- Meant as starting point for sector standards
- Intended for manufacturers

IEC61508

- 7 Parts
  - Part 1 General Requirements
  - Part 2 Systems Requirements
  - Part 3 Software Requirements

  Normative

  - Part 4 Definitions
  - Part 5 SIL Evaluation methods
  - Part 6 Guidelines on applying parts 1 and 2
  - Part 7 Overview of techniques

  Informative

‘In Country’ Clause

IEC61508 Part 1.4…

“In the USA and Canada, until the proposed sector implementation of IEC 61508 is published as an international standard in the USA and Canada, existing national process safety standards based on IEC61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC61508.”

IEC61511

- IEC version of ANSI/ISAS84.01
- In Committee Draft
- Desired Release Date around 3Q ’01
- 3 Parts
  - Part 1 General Requirements
  - Part 2 Guidelines for application
  - Part 3 Guidelines for Hazard and Risk Analysis

Software

- Languages
  - IEC61131-3 Defines PLC programming Languages
- Applications
  - Software application development is left to “Good Practice”
  - A good start is in IEC 61508 and 61511
  - IEC880 (Software for Computers in the Safety Systems of Nuclear Power Stations) is a good reference

Programming Languages

- Three Categories
  - Fixed Program Language
    - Application is unalterable
      - Ex. Smart Transmitter
  - Limited Variability Language
    - Well defined functions may be programmed within a structured framework
      - Ex. Ladder Logic, Instruction List
  - Full Variability Language
    - General purpose programming language
      - Ex. ADA, C, C++

IEC61131-3

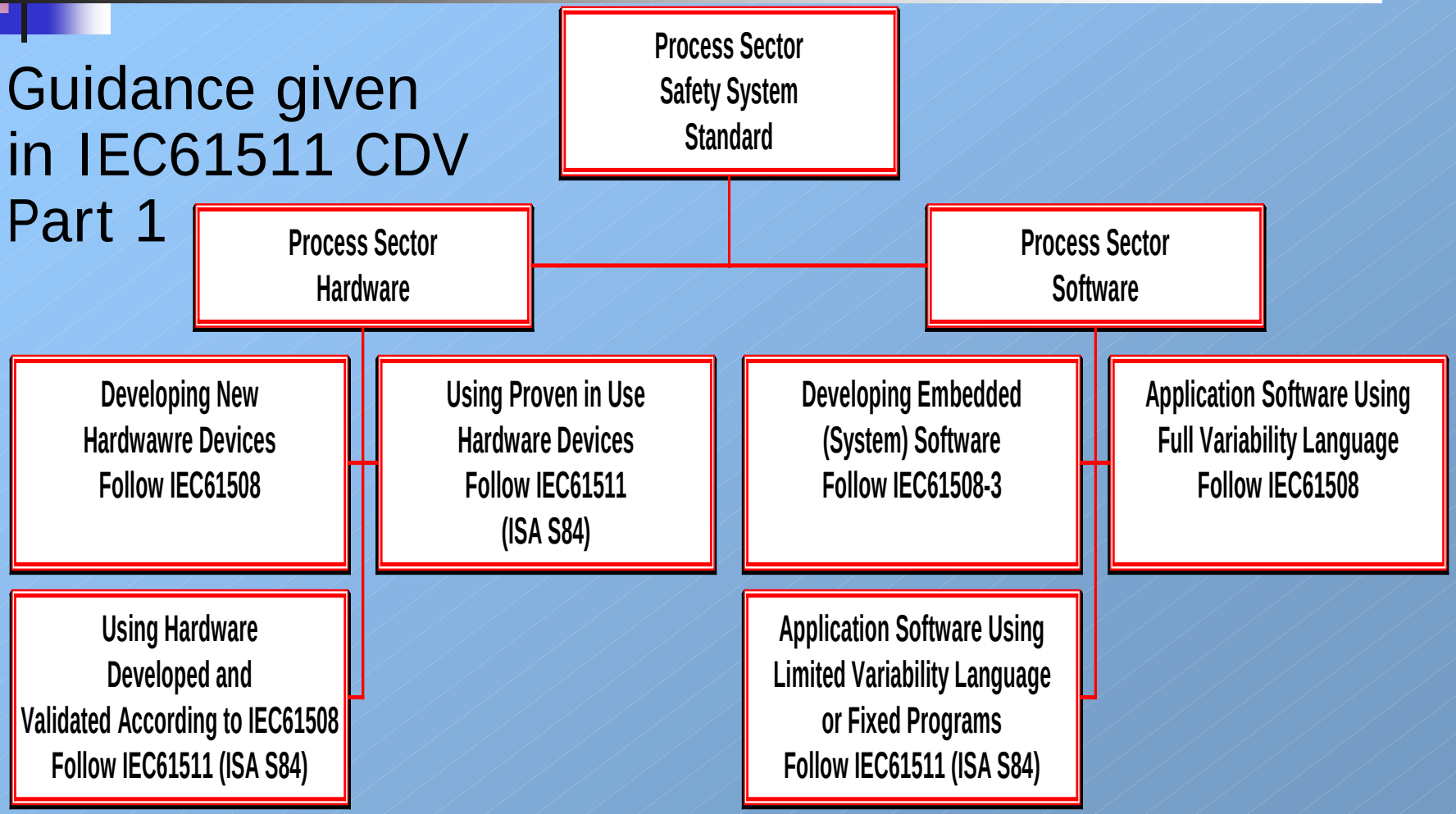
- Framework
  - Sequential Function Chart
- 4 Languages
  - Structured Text
  - Instruction List
  - Ladder Diagram
  - Flow Diagram

IEC61131-3

- Vendors claim “conforms to IEC1131”
- Organization ‘PLC Open’ is moving to certify vendor languages as 1131 compliant
  - Includes standards for implementation
  - Safety Functions (Technical Committee TC5)
  - Ideal goal is platform independence - but not likely

Application of IEC Standards

Guidance given in IEC61511 CDV Part 1



Evaluation Techniques

- Layer of Protection Analysis (LOPA)
  - Used to more realistically assign risk reduction factors to non-safety system functions
    - Operator Response
    - Dedicated Control System safety functions
- IEC61511 Part 3
  - Hazop/LOPA/Event Tree ...etc
- TR84.00.02
  - Guidance for evaluating SIL of the safety system
- IEC61511 Part 2
  - Same information as TR84.00.02

Software Evaluation Techniques

- HAZOP
  - Hazard and Operability analysis
  - Qualitative
  - Carried out on design, not a FMEA
- Fault/Event Trees
  - Quantitative
  - Only follows defined faults/events
- Formal Methods
  - Rigorous but unwieldy

What's Ahead?

- High Power Photon Sources
- NLC
- NIF
- JLab Hall D
- Meson Scattering
- RIA

Keeping up with Technology

- Smart sensors/actuators
  - Micro controlled sensors and actuators finding their way into industrial safety systems
- On line maintenance
  - Industries that require high availability allow on line testing and bypassing 1 of n redundant systems for maintenance.
  - An issue that has come up at RHIC and SNS

Recommendations for Fermi

- Establish a lifecycle model for protection systems
  - Benchmark existing policies and procedures against model
- Move away from Prescriptive Policies
- Adopt ANSI/ISA S84 as guidance for safety system implementations using proven in use hardware and limited variability software
- Adopt IEC61508 as guidance for safety systems using unproven or new designs or full variability programming languages

Conclusions

- Safety System design must take place within the context of a safety lifecycle
- Implementation should be appropriate for the level of risk