BLUEFIELD PROCESS SAFETY

Are You Ready for an SIS?

Why I&E Engineers Have Become Responsible for Organizational Risk

YOKOGAWA

Mike Schmidt
Principal
Bluefield Process Safety, LLC

2012 USERS GROUP CONFERENCE & EXHIBITION

Mike Schmidt

- Principal of Bluefield Process Safety
- Formerly an SIS consultant with a major process automation vendor
- Joined Union Carbide in 1977
- Began working in process safety following the 1984 tragedy in Bhopal, India
- Joined faculty at Missouri S&T in Rolla in 2009, teaching on safety and process risk
- Work includes
  - Facilitating PHAs, LOPAs, RTC establishment
  - SIS conceptual design and SIL verification calcs

Why I&E? “We need an SIS!”

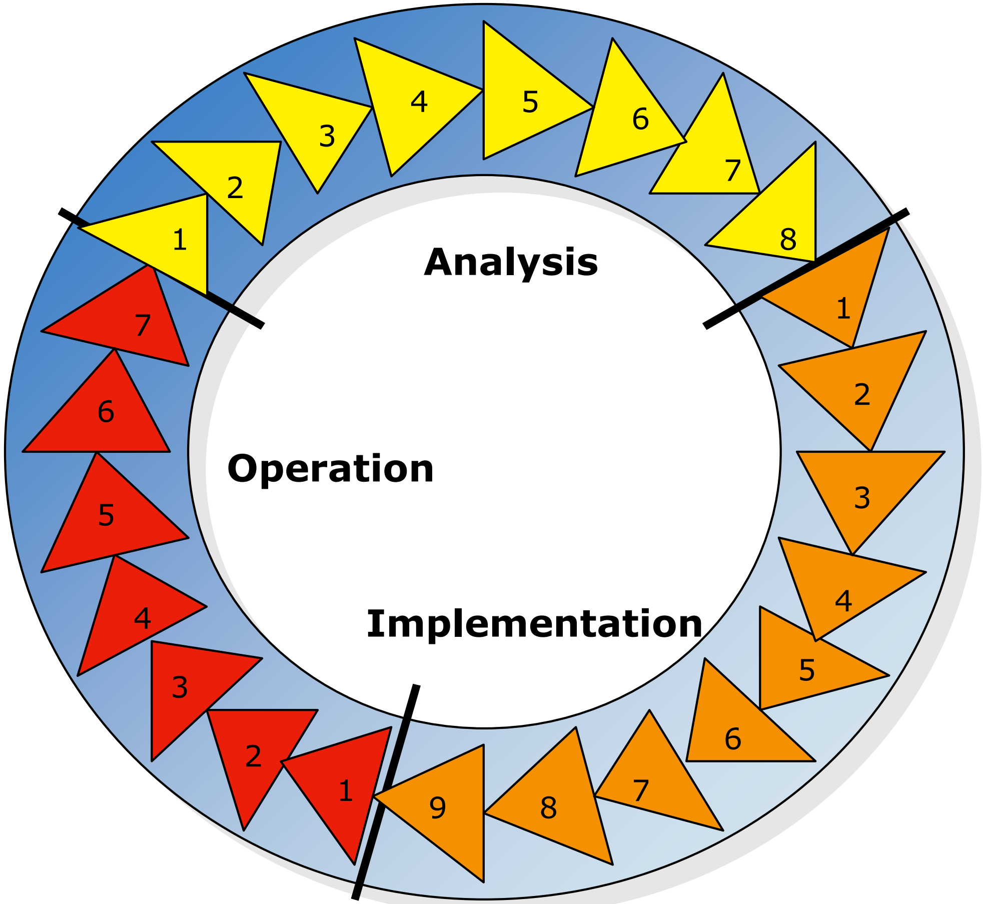
Safety **INSTRUMENTED** System, so obviously, I&E engineering should take care of it.

The SIS Standards

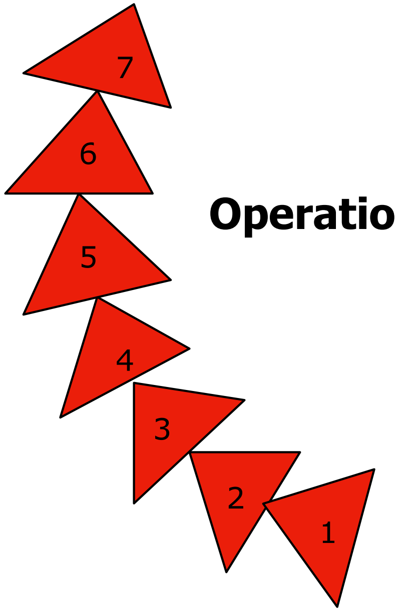
- ANSI/ISA 84.00.01-2004
- IEC 61511
- IEC 61508

- All call for addressing the safety lifecycle

What is the Safety Lifecycle?



The Safety Lifecycle - Operation

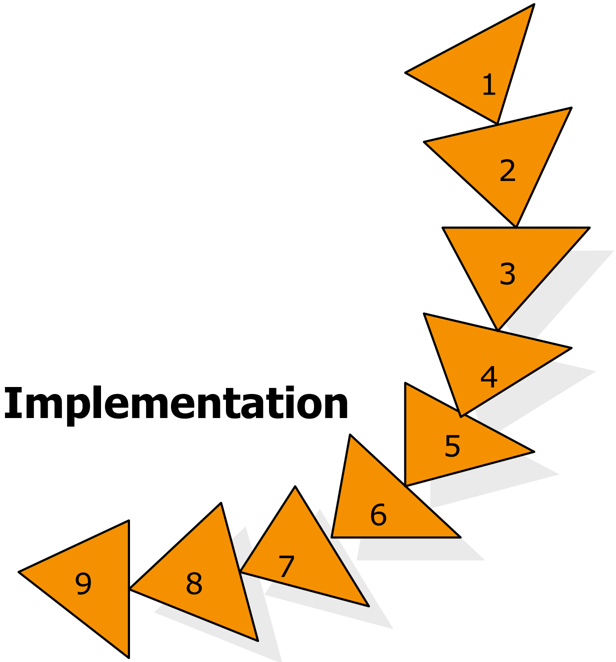


Operation

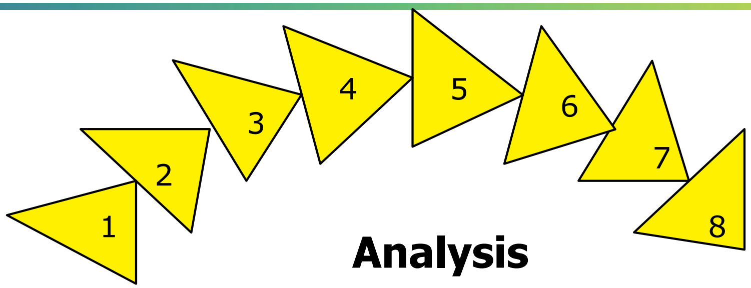
1. Operation
2. Training
3. Proof Testing
4. Inspection
5. Maintenance
6. Management of Change
7. Decommissioning

The Safety Lifecycle - Implementation

1. Mechanical/Electrical/Structural
2. Software Configuration
3. Equipment Build
4. Factory Acceptance Testing
5. Construction/Installation
6. Site Acceptance Testing
7. Validation
8. Training
9. Pre-Startup Safety Review



The Safety Lifecycle - Analysis



- 1. Process Design
- 2. Hazard Identification
- 3. Risk Assessment
- 4. RTC Confirmation
- 5. Risk Reduction Allocation
- 6. Safety Function Definition
- 7. Safety Function Specification
- 8. Reliability Verification

I&E Engineering - New Responsibilities

- Whether they want to or not, I&E engineers are being charged with responsibility to:
  - Operate and maintain SISs in compliance with regulations and standards
  - Design and install SISs according to rigorous standards
  - Establish risk tolerance criteria
  - Assure hazard and risk assessments are done well

Analysis in the Safety Lifecycle

What needs to be done? What needs to be different?

Hazard Identification

- Before risks can be assessed, hazards must be identified
- Hazards are identified during Process Hazard Analysis
- Most common PHA in the process industries is the HazOp

HazOps – Key points

- Deviations
  - N/A: The parameter has no meaning, or a limit does not exist
  - NCOI: A limit exists, but there is no conceivable way reach limit
- Causes
  - Faults (equipment failures or human errors), not other deviations
  - "Double jeopardy" reduces likelihood, but doesn't eliminate possibility
- Consequences
  - Focus on event, then on impact

HazOps – Key points

- Safeguards
  - List everything, not just IPLs per LOPA
  - Exception: Do not list safeguards that are based on the failure that has been identified as the cause
- Risk Assessment
  - "Worst case" vs. Likely case
  - Teams are good at estimating consequence impacts, not so good at estimating likelihood
  - Traditionally determines urgency not required risk reduction
- Consequences
  - "Conduct a LOPA of this scenario"

Risk Assessment

Risk has two components:

- Consequence (impact)
- Likelihood

Risk Assessment consists of

- Likelihood Analysis
- Consequence Analysis
  - Event Analysis
  - Impact Analysis

Consequence Analysis

- Statistical Analysis
  - Determined from loss experience in previous events
  - Frequently relies on experiences of team members
- Consequence Modeling
  - Determine extent of release—the event
  - Determine effect zone for event
  - Calculate impacts of event based on extent and effect zone

Impacts

- Personnel safety
- Environmental
- Community
- Financial
  - Operational
  - Quality
  - Capital
  - Business Interruption
  - etc.

Likelihood Analysis

- Qualitative Analysis
  - Derived from PHA team
- Statistical Analysis
  - Fault Tree Analysis
  - Event Tree Analysis
  - Layer of Protection Analysis

What is LOPA?

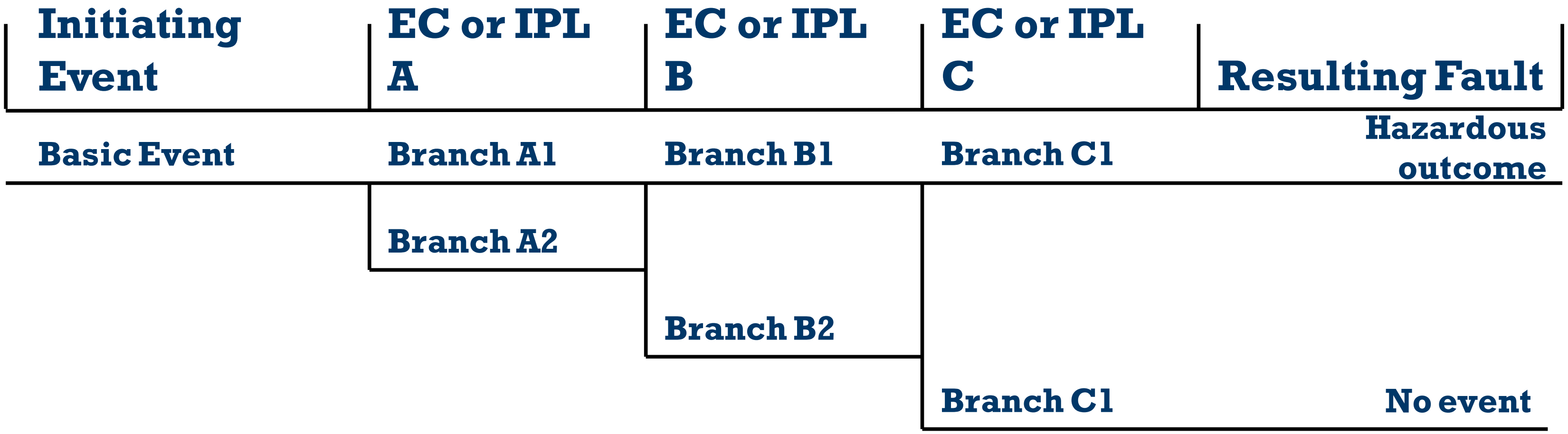
Likelihood analysis linking:

- Frequency of initiating event (cause)

  TO

- Frequency of resulting event
- Through chain of enabling conditions and independent layers of protection, each with their own probability

The LOPA Tree



Initiating Event

EC or IPL A

EC or IPL B

EC or IPL C

Resulting Fault

Basic Event

Branch A1

Branch B1

Branch C1

Hazardous outcome

Branch A2

Branch B2

Branch C1

No event

Some Typical Failure Rates

Initiating Cause	Frequency (1/yr)
Pump trip	1
Seal or flange leak	1
Unit trip	1
BPCS control loop failure	0.1
Heat tracing failure	0.1
Tube leak-corrosive service	0.1
Control valve-opposite of design	0.01
Relief valve-spurious operation	0.01
Total packing failure	0.01
Lightning strike	0.001
Rupture of rotating equipment	0.001
Tube failure-mild service	0.001

Enabling Conditions

- Time at Risk
- Occupancy Factor
- Ignition Probability
- Vulnerability Factor

Time at Risk

- Standard failure rates are based on continuous operation
- Many components are only vulnerable to failure part of the time
- "Time at risk" takes this into account

Occupancy Factor

- Safety impacts based on personnel being present to become victims
- In many operations, personnel are not always present
- “Occupancy factor” takes this into account

Ignition Probability

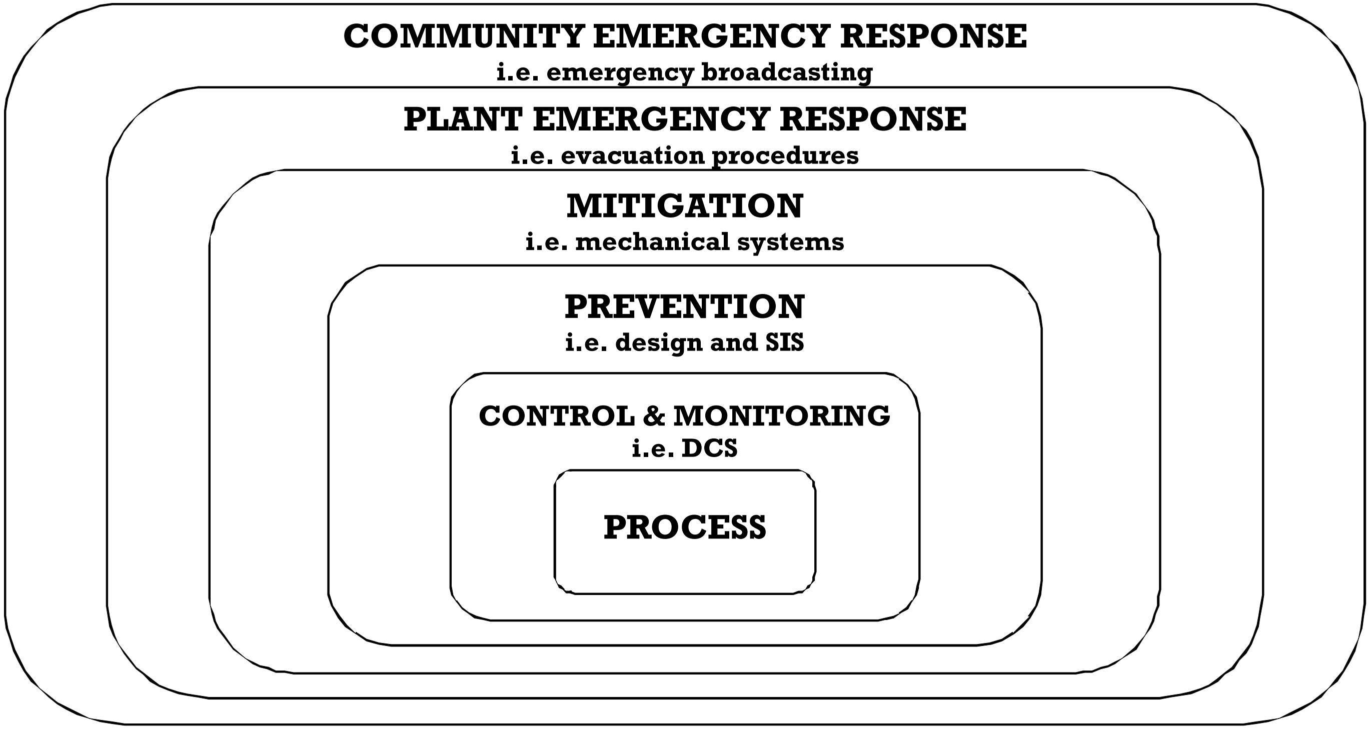
- Conservative assumption: Given fuel and oxidizer, ignition is certain
- Less conservative assumption: Ignition has probability based on
  - Type of release
  - Size of release
  - Release environment

Vulnerability Factor

- Not everyone exposed to an event will suffer the worst impact
- Vulnerability Factor is a way to address this
- Not applicable if vulnerability has already been taken into consideration when defining impact or occupancy factor

Layers of Protection

- Each layer is independent
- Failure of one does not affect the next

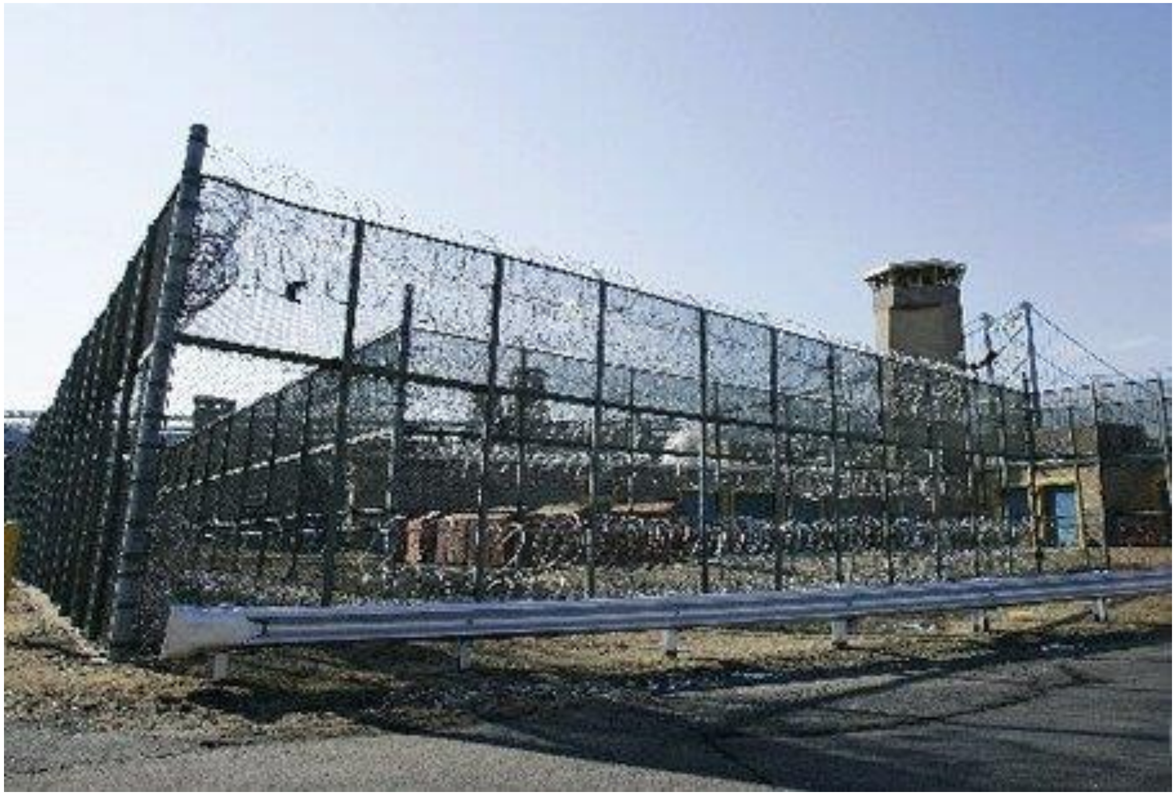


Layers of Protection

- Less like an onion…

Layers of Protection

- …and more like a prison



Not all safeguards are IPLs

In order to be considered an IPL, a safeguard must be

- Effective
- Independent
- Auditable

Effectiveness

- When it works, does it prevent the outcome event?
- If it is the only thing that works, is it enough to prevent the outcome event by itself?

Independence

Is the safeguard independent of

- The initiating event and its effects?
- The failure of any component of another IPL claimed for the same scenario?

Auditability

Can it be shown that

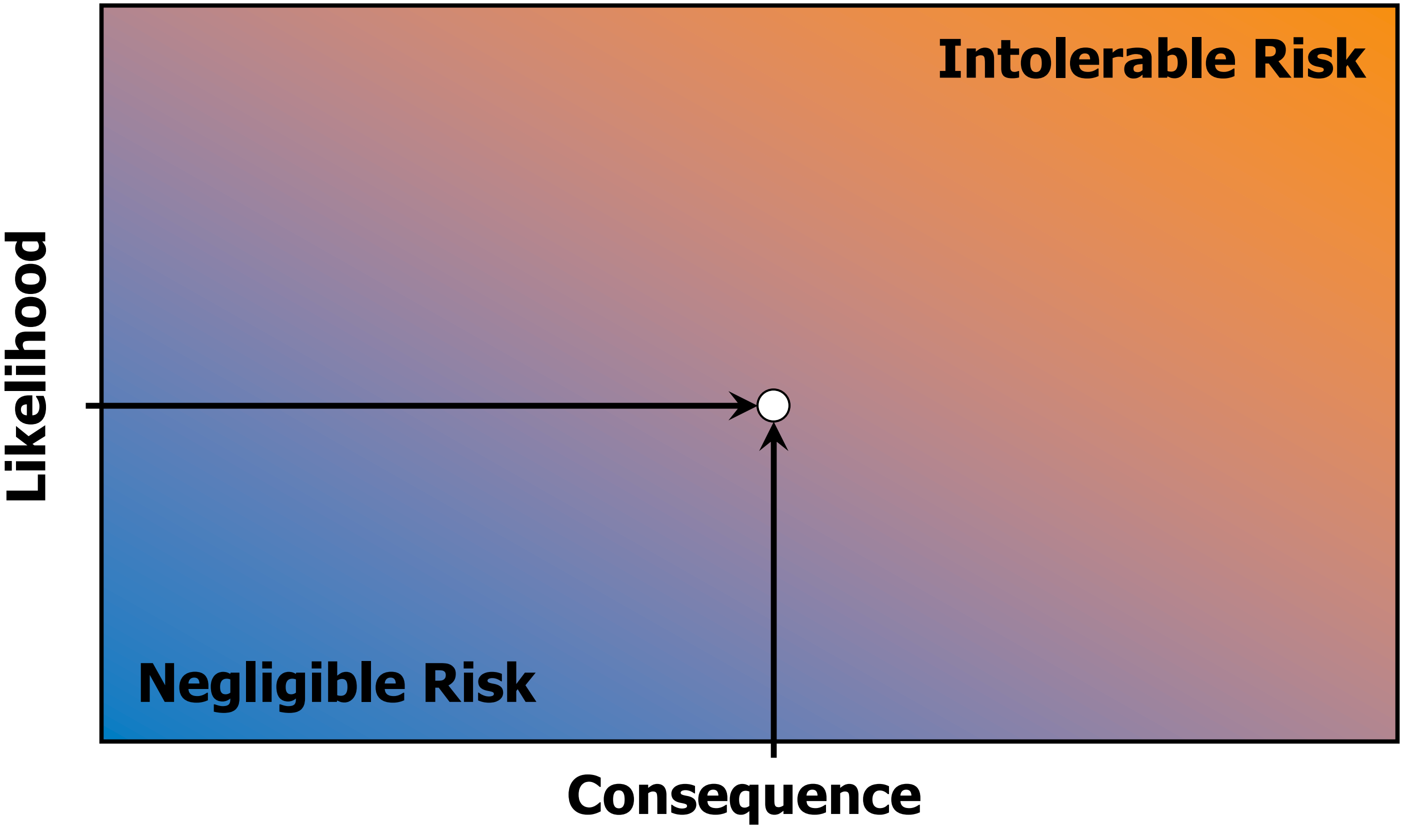
- The safeguard functions as designed?
- When the safeguard functions as designed, it prevents the hazardous outcome?
- Design, installation, functional testing, and maintenance testing are in place?

Example IPLs

Administrative controls	0.1
Blast wall/bunker	0.001
BPCS control loop	0.1
Dike/bund	0.01
Relief valve	0.01
Rupture disk	0.001
Spare w/auto start	0.1
Vacuum breaker	0.01

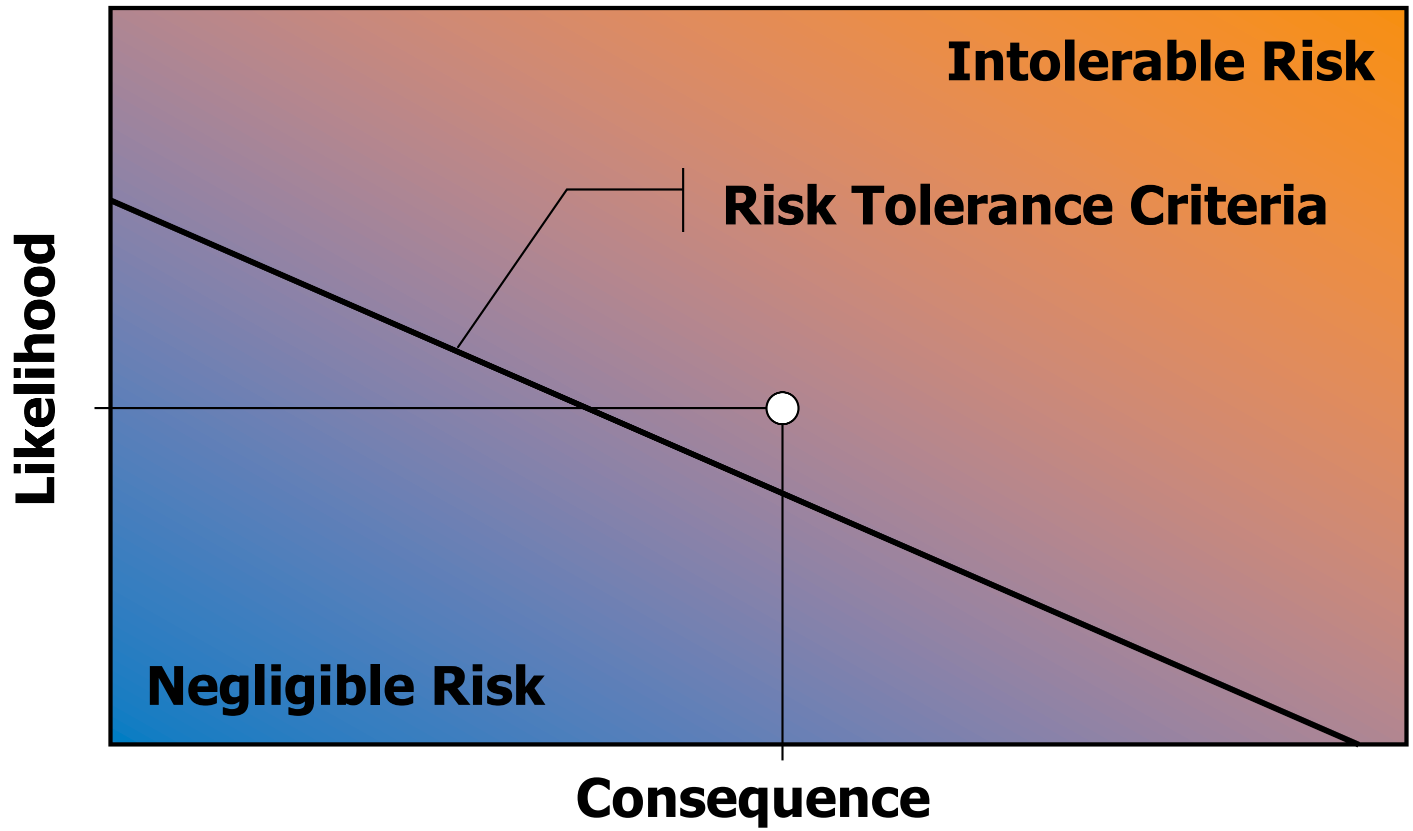
But is the risk tolerable?

Risk Analysis: Consequence Analysis plus Likelihood Analysis



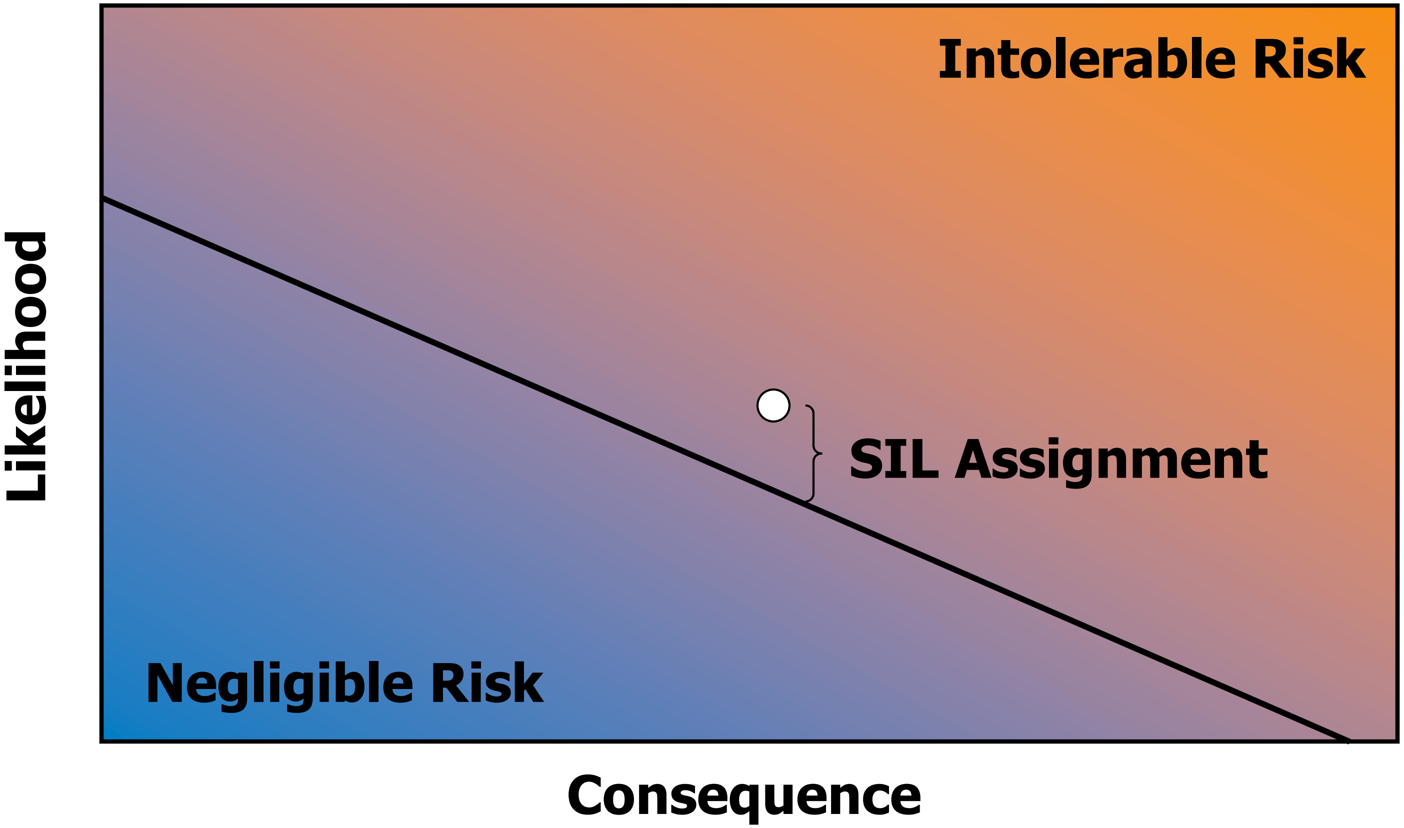
How much risk is too much?

Compare: **Risk against Risk Tolerance Criteria**



Required Risk Reduction

SIL: **Ratio of Risk to Risk Tolerance Criteria**



What are SILs?

Safety Integrity Levels

Safety Integrity Level	Probability of Failure on Demand (PFD_{AVG})	Risk Reduction Factor (RRF)
SIL 4	**10^{-4} > PFD > 10^{-5}**	**10000 < RRF < 100000**
SIL 3	**10^{-3} > PFD > 10^{-4}**	**1000 < RRF < 10000**
SIL 2	**10^{-2} > PFD > 10^{-3}**	**100 < RRF < 1000**
SIL 1	**10^{-1} > PFD > 10^{-2}**	**10 < RRF < 100**

SIFs can also have N/R (not rated) SILs

Safety Instrumented Systems

Challenges and Controversies

Challenges and Controversies

- “Best” architecture
- Proof testing
- BPCS loops
- OSHA enforcement
- Third party certification vs. proven-in-use

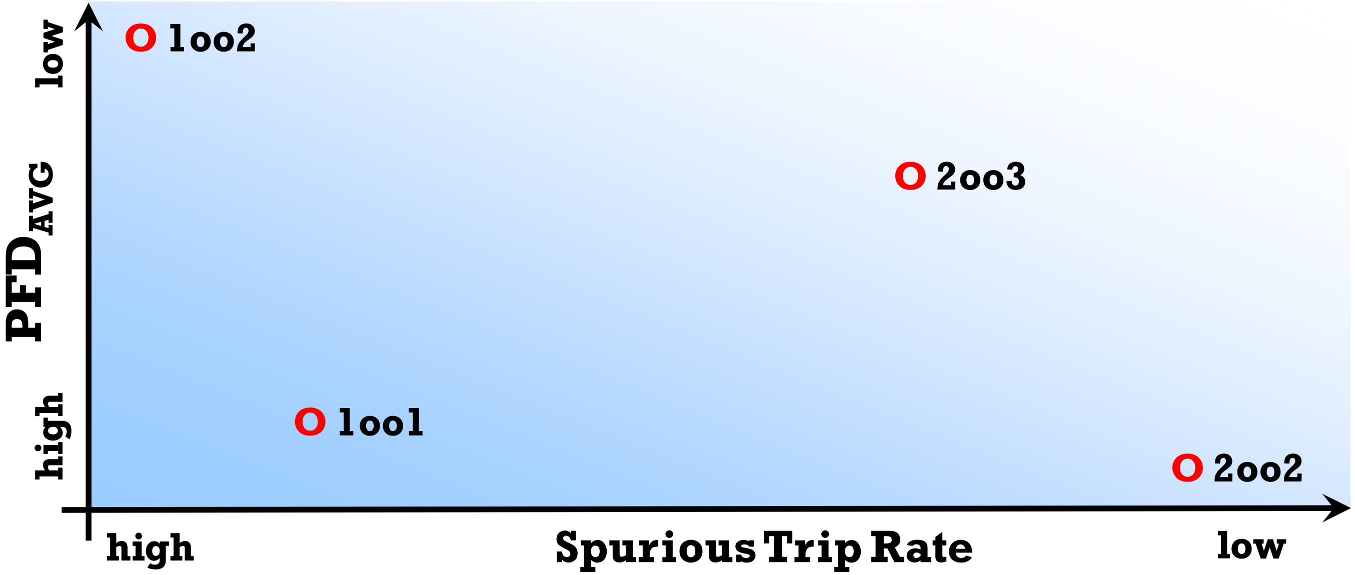
Architecture – what is it?

- One out of one (1oo1)
- One out of two (1oo2)
- Two out of two (2oo2)
- Two out of three (2oo3)
- "m" out of "n" (MooN)

- For sensors:
  M out of N vote to trip
- For final control elements:
  M out of N act on trip

Comparing architectures

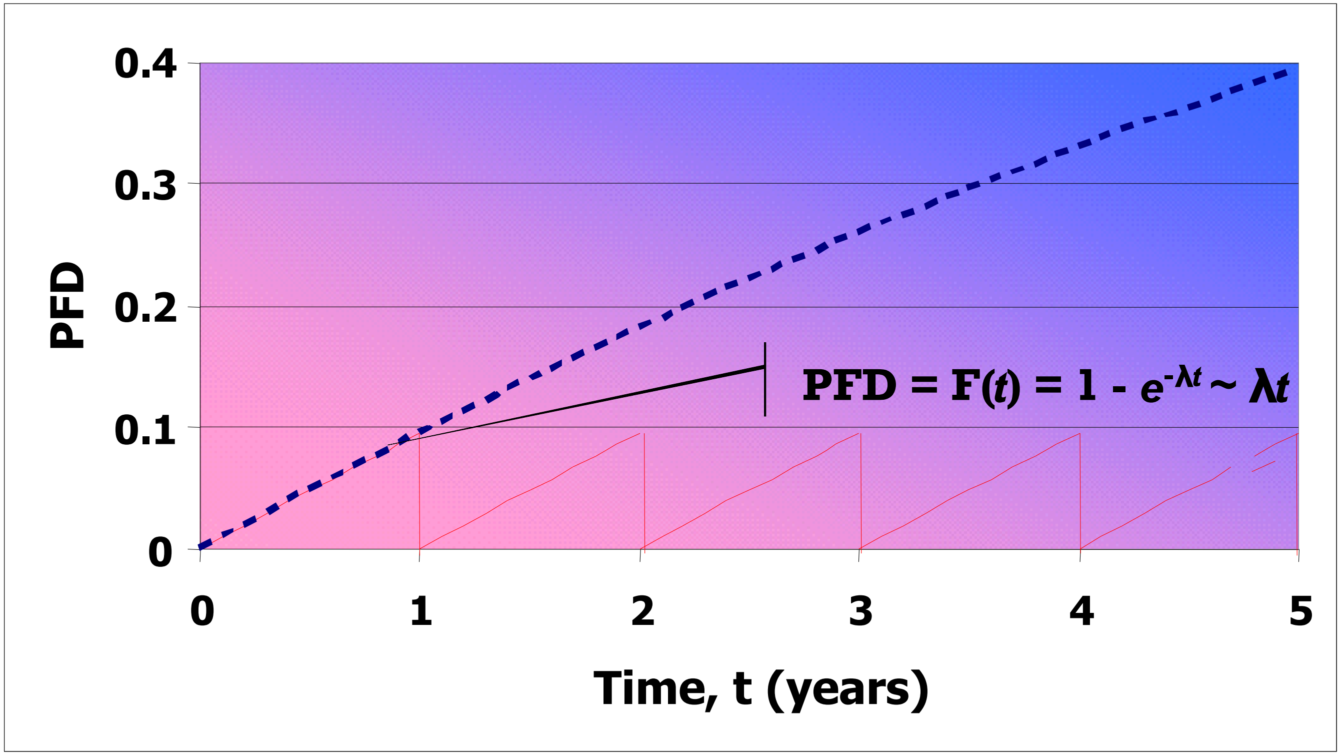
- PFD$_{AVG}$, spurious trip rate, and cost all have to be balanced to design SIFs that meet all the requirements of a project



Proof test intervals

- PFD_{AVG} for different architectures
  - 1oo1 $PFD_{AVG} = \lambda_D T/2$
  - 1oo2 $PFD_{AVG} = (\lambda_D T)^2/3$
  - 2oo2 $PFD_{AVG} = \lambda_D T$
  - 2oo3 $PFD_{AVG} = (\lambda_D T)^2$
- "T" refers to proof test interval
- As failure rate decreases, PFD_{AVG} gets better (smaller)
- As T decreases, PFD_{AVG} gets better (smaller)

Impact of proof test interval



Test interval of t=1 year

Proof Testing

- Full loop needs to be tested
  - As a complete loop

    OR
  - By component
- When testing by component, not necessarily at the same time or interval
- Combination of simulations and field tests

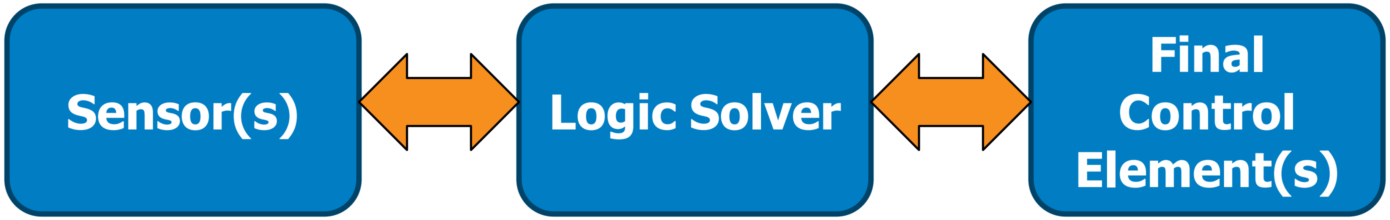
More than one BPCS function?

Two approaches—

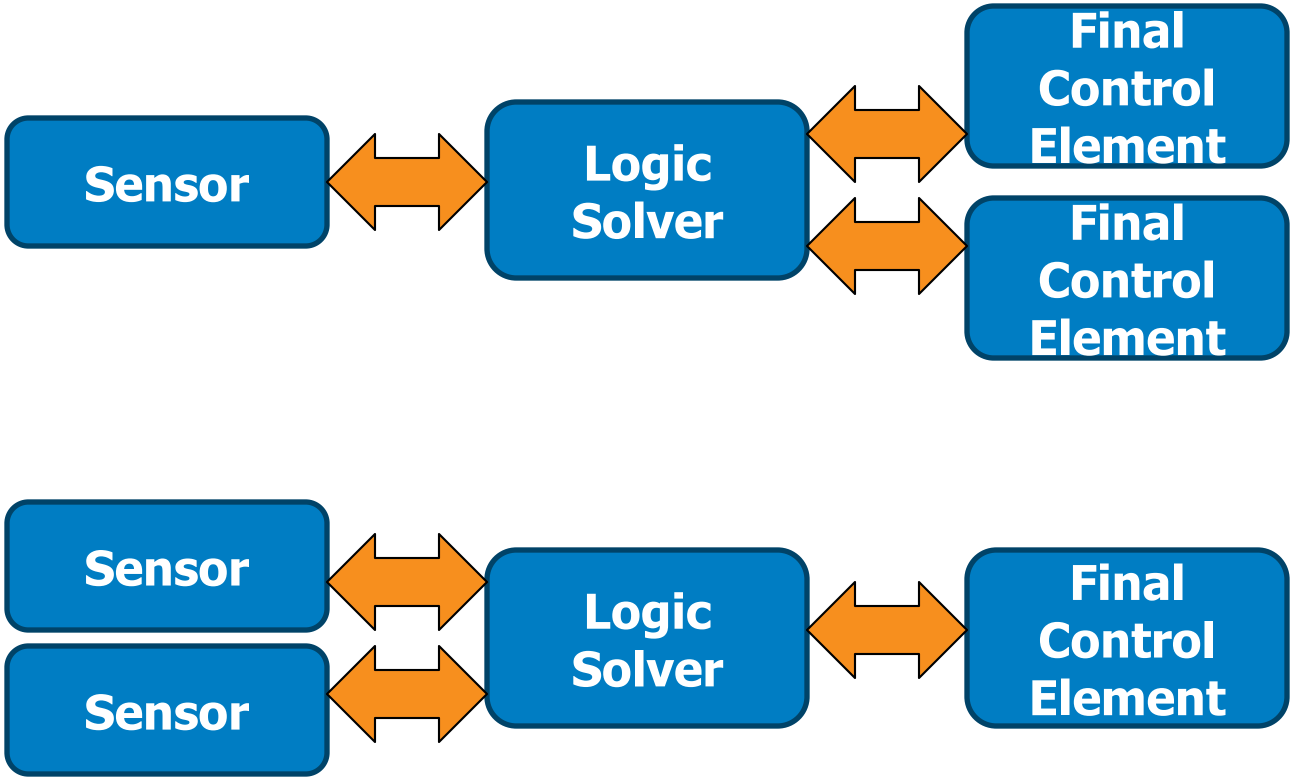
- Conservative approach: Only one BPCS loop per logic solver; additional loops not independent
- Less conservative: Probable failure of BPCS loop is failure of sensor or final control element. Logic solver much less likely to fail, so claim credit for more

Credit for Control System

- BPCS function: $PFD_{AVG} = 0.1$



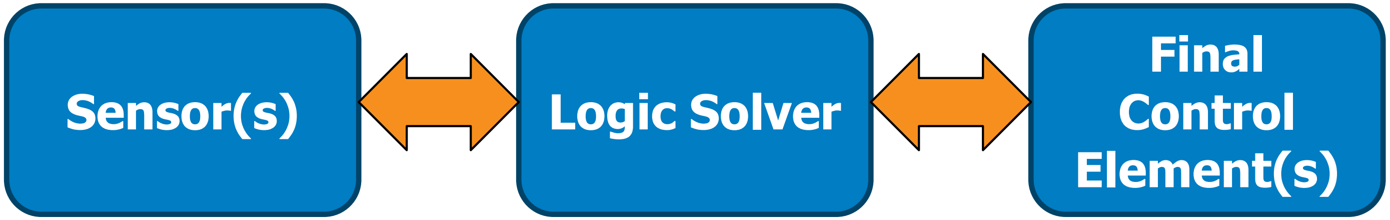
Regardless of instruments



Component contribution

- For one BPCS function:

  $PFD_{AVG} = 0.1$



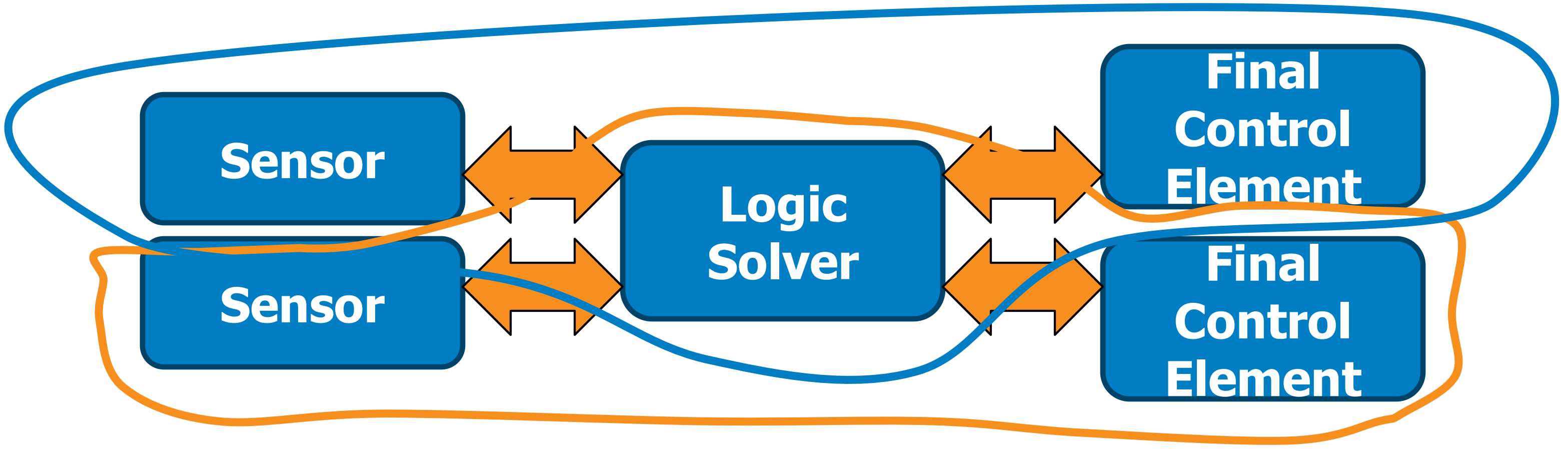
~45%	< 5%	~50%
~0.045	< 0.005	~0.050

$$(0.045 + 0.050) + 0.005 = 0.1$$

For two functions

- Two BPCS functions:

$$PFD_{AVG} = 0.1 \text{ x } 0.1 = 0.01$$

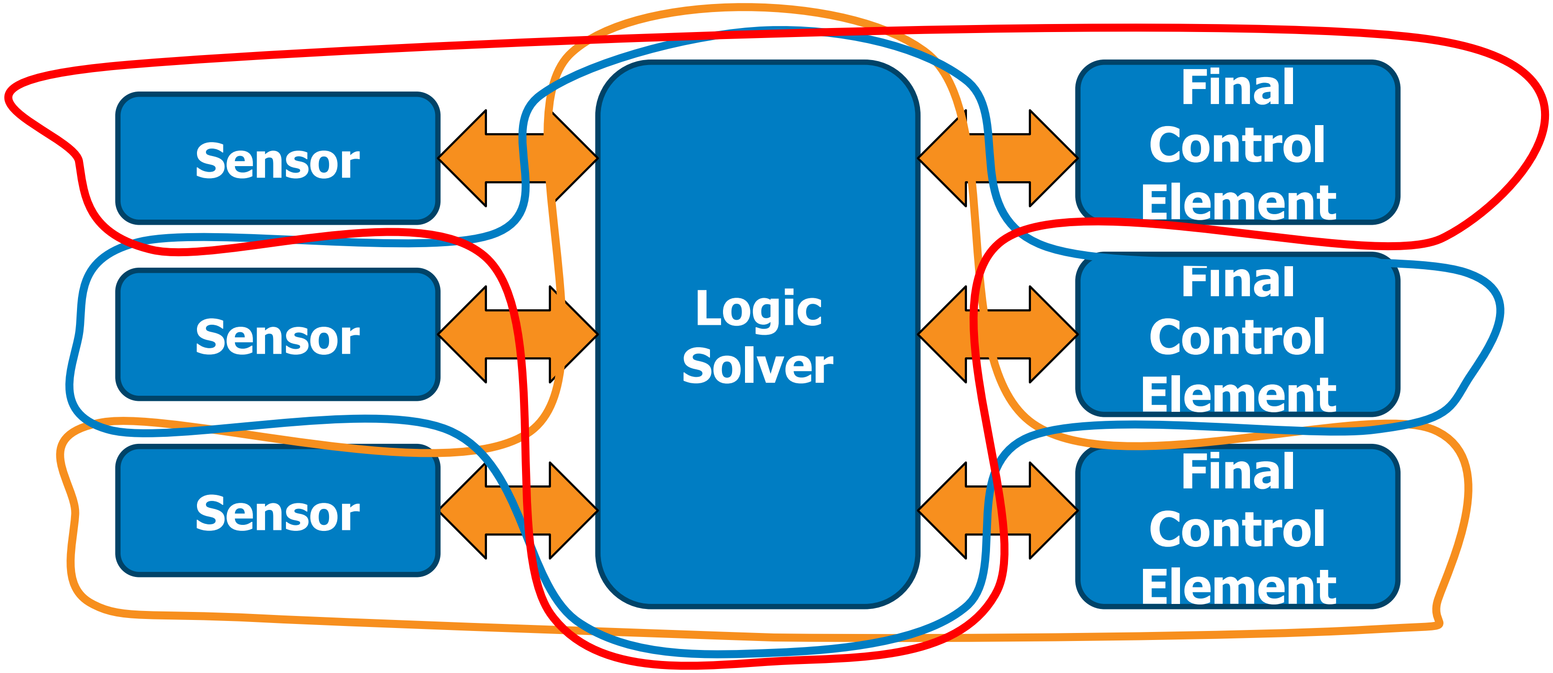


$$(0.045 + 0.050)^2 + 0.005 = 0.014 \rightarrow 0.01$$

How about three functions?

- Three BPCS functions:

$$PFD_{AVG} = 0.1 \times 0.1 \times 0.1 = 0.001$$



$(0.045 + 0.050)^3 + 0.005 = 0.0059$ → 0.006 → $0.01 \neq 0.001$

Taking credit for two functions

- Each BPCS function must have independent
  - Sensors
  - Input cards
  - Final control elements
  - Output cards
- BPCS functions involved in the initial failure count against the total of two functions
- Only one function may be alarm

Adoption of S84.01 by OSHA

- From OSHA Letters of Interpretation:
  - "As S84.01 is a national consensus standard, OSHA considers it to be a recognized and generally accepted good engineering practice for SIS."
  - "OSHA does not specify or benchmark S84.00.001-2004, Parts 1-3, as the only recognized and generally accepted good engineering practice."

- This is specifically in regard to PSM-covered processes
  - 29 CFR 1910.119(d)(3)(i), (ii)
  - 29 CFR 1910.119(j)(4)

Some recent OSHA citations

- Citation for a willful act of failure to follow IEC 61511. Reversed on appeal
- Citation for failure to document that equipment in the process and safety control systems complies with RAGAGEP.
- Citation for each failure to ensure that burner management systems for five different pieces of equipment complied with RAGAGEP.
- Citation for inadequate frequency of inspections and tests of process equipment, including two SIS systems.

3rd Party Certification or Proven-In-Use?

- Primary concern—does the device work in the given application? Use something that works, whether certified or not
- 3rd party certification – simplifies justification
- Proven-in-use – simplifies maintenance and operation

Summary

- I&E must see that PHAs are done correctly, and that safeguards and IPLs are identified appropriately
- SIL assignment depends on first establishing risk tolerance criteria for the organization
- SIS follows RAGAGEP, but these might not be IEC 61511 or ISA S84
- I&E Engineers must see that questions about architecture, proof-testing, using more than one BPCS function, and proven-in-use are settled for their organization

Thank-You

Mike Schmidt, Bluefield Process Safety, LLC
(314) 420-9350
bluefieldsafety@gmail.com
www.bluefieldsafety.com