Overview of ISA 84
SIS for the Process Industries

Presented to
ISA-St. Louis Section
October 12, 2011

BLUEFIELD
PROCESS SAFETY

Mike Schmidt

- Principal of Bluefield Process Safety
- Formerly an Emerson SIS consultant
- Joined Union Carbide in 1977
- Began work in process safety, following tragedy in Bhopal in 1984
- Joined faculty at Missouri S&T in Rolla in 2009, teaching on safety and risk
- Work includes
  - Facilitating PHAs, LOPAs, RTC establishment
  - SIS conceptual design
  - PSM compliance

Key Points

- **Safety Instrumented Systems**
- **SIS standards**
- **Safety Lifecycle and Tolerable Risk**
- **Layer of Protection Analysis**
- **Controversies and Challenges**

Overview of ISA 84
SIS for the Process Industries

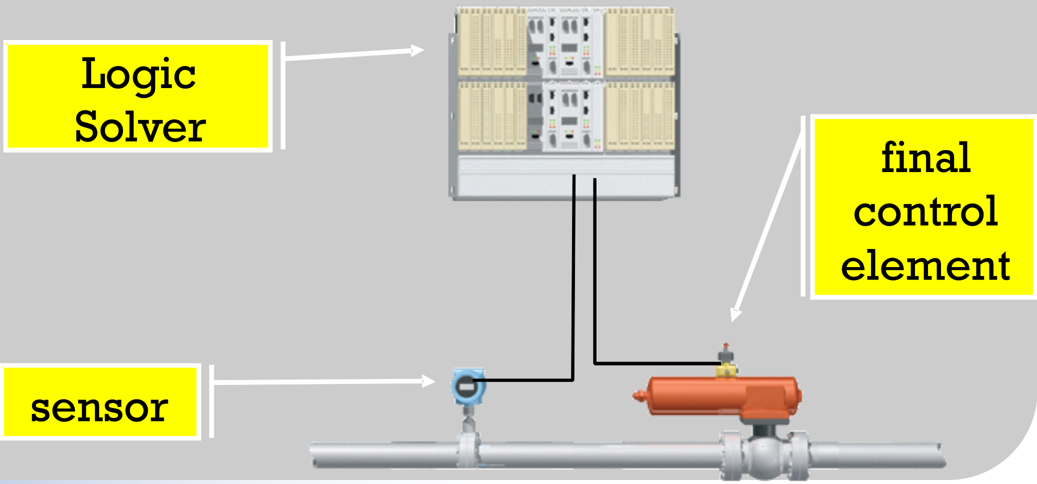
Safety Instrumented Systems

BLUEFIELD
PROCESS SAFETY

What is an SIS?

Safety Instrumented System:

- **Set of components (sensors, logic solvers, and final control elements) executing SIFs separate from the BPCS.**



What is a BPCS?

Basic Process Control System:

- **Control system designed and used to control normal operations of the process**
- **Allows operators to start, stop, and modify the process to achieve production**

What is the difference?

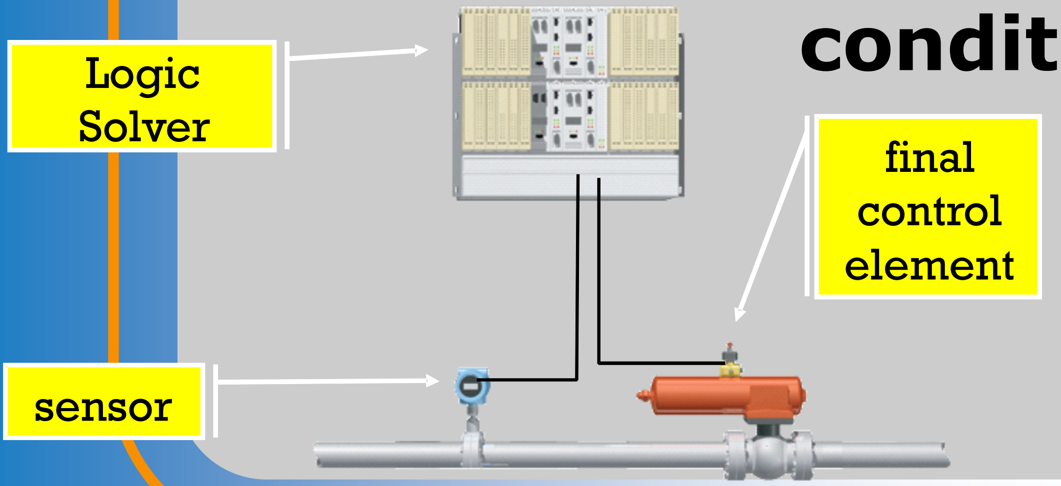
BPCS vs. SIS

- **BPCS**
  - **Control process parameters**
  - **Startup, shutdown, and run process**
  - **Operator Interaction**
- **SIS**
  - **Intervene to take process to safe state**
  - **No operator interaction**
  - **Dedicated emergency response system**

What is a SIF?

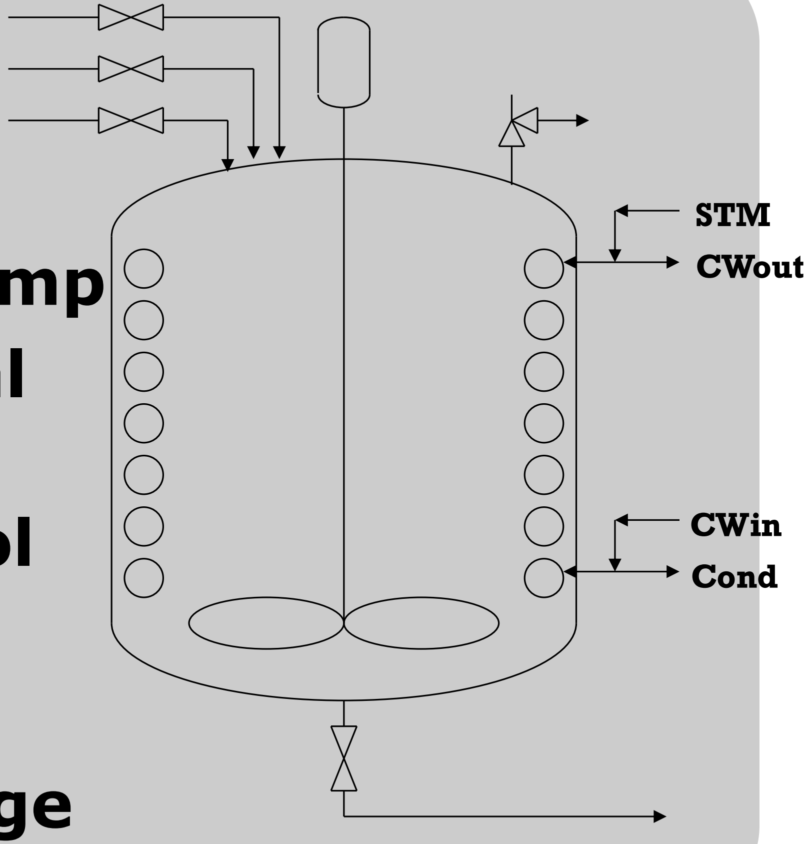
Safety Instrumented Function:

- **A combination of sensor(s), logic solver(s), and final element(s) with a specified SIL that detects an out-of-limit (abnormal) condition and brings process to a functionally safe state; "Interlock"**



Example process

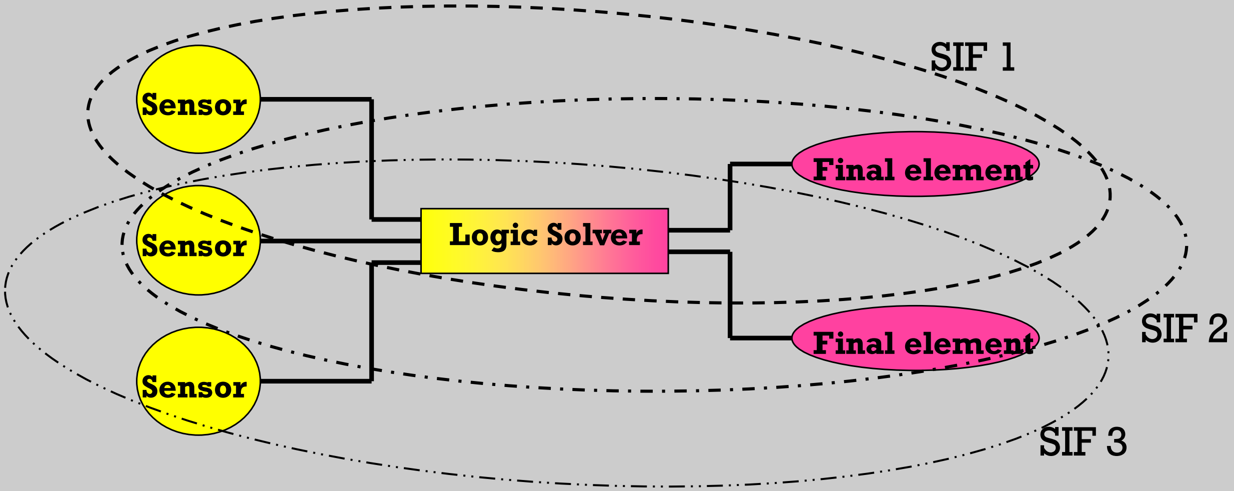
- Charge raw materials
- Agitator on
- Steam heat to temp
- Last raw material feed
- Cooling to control
- Steam to finish batch
- Discharge to surge tank



Example SIFs

- On high temp,
  - Stop all feeds
  - Set cooling water full open
  - Close steam valves
- On high pressure,
  - Stop all feeds
  - Open discharge valve
- On utility failure,
  - Stop all feeds
  - Open cooling, close steam

SIFs in a SIS?



- **It is not uncommon for different SIFs to share field devices – sensors and final elements**

Overview of ISA 84
SIS for the Process Industries

SIS Standards

BLUEFIELD
PROCESS SAFETY

Applicable Standards

- **IEC 61508 – Functional Safety of Electrical/Electronic /Programmable Electronic Safety Related Systems**
- **IEC 61511 – Functional Safety: Safety Instrumented Systems for the Process Industry Sector**
- **ISA S84.01 – Application of Safety Instrumented Systems for the Process Industries**

What is IEC 61508?

"Functional Safety of Electrical/ Electronic/Programmable Electronic Safety Related Systems"

- **A"generic" standard**
- **Applies to all industry sectors**
  - **Process Industries**
  - **Manufacturing Industries**
  - **Transportation**
  - **Medical**

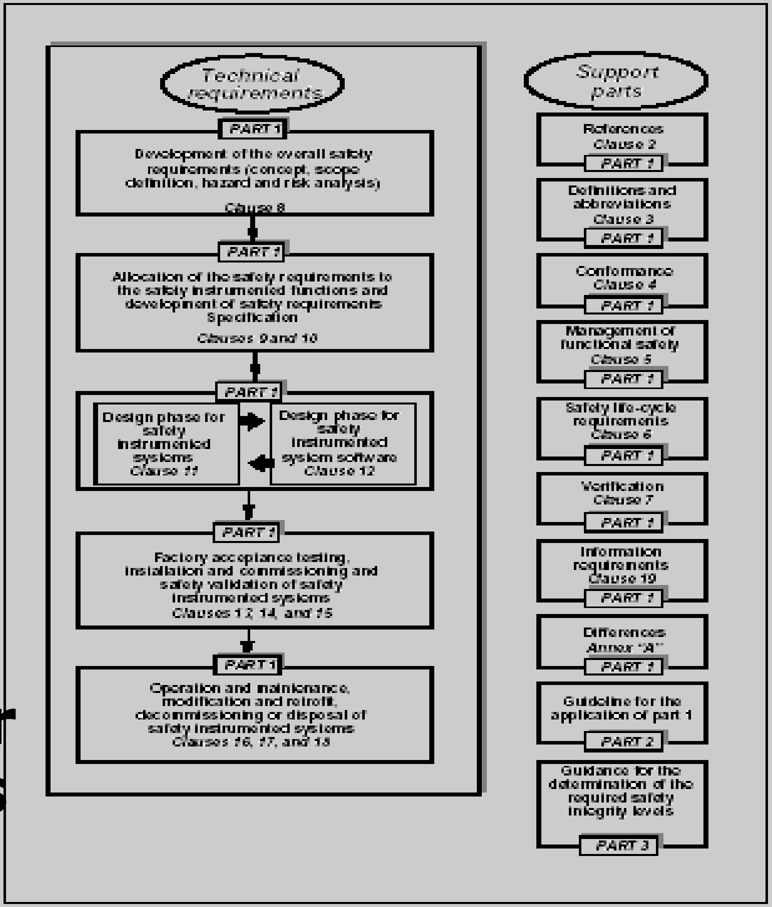
What is IEC 61511?

"Functional Safety: Safety Instrumented Systems for the Process Industry Sector"

- **Exists as a standard under the umbrella of IEC 61508**
- **Targeted to the process industries**
- **Specifically for the "USERS" of safety instrumented systems**

Requirements of IEC 61511

- **Hazard and Risk Assessment**
- **Allocation of safety req'mnts including to SIS**
- **Works within Safety Lifecycle framework**
- **Details requirements for certain activities**



Three parts of IEC 61511

1. **Part 1: Framework, definitions, system, hardware and software requirements**
2. **Part 2: Guidelines in the application of IEC 61511-1**
3. **Part 3: Guidance for the determination of the required safety integrity levels**

Normative

Informative

What is S84.01

"Application of Safety Instrumented Systems for the Process Industries"

- **Developed by ISA and adopted by American National Standards Institute (ANSI)**
- **Objective: to define requirements for Safety Instrumented Systems**
- **Goal: to provide uniformity in the field of instrumentation.**

History of S84.01

- **Originally issued as ANSI/ISA-84.01-1996**
- **Developed prior to work done by IEC**
- **Did not address the total safety life-cycle; assumed SIL was set**
- **ANSI/ISA-84.00.01-2004 harmonized with IEC 61511; identical with exception of “grandfather” clause**

Grandfather Clause

- **A provision to allow safety systems built prior to the issuance of the 1996 standard:**

  "For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of ANSI/ISA-84.01-1996, the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner."

Overview of ISA 84
SIS for the Process Industries

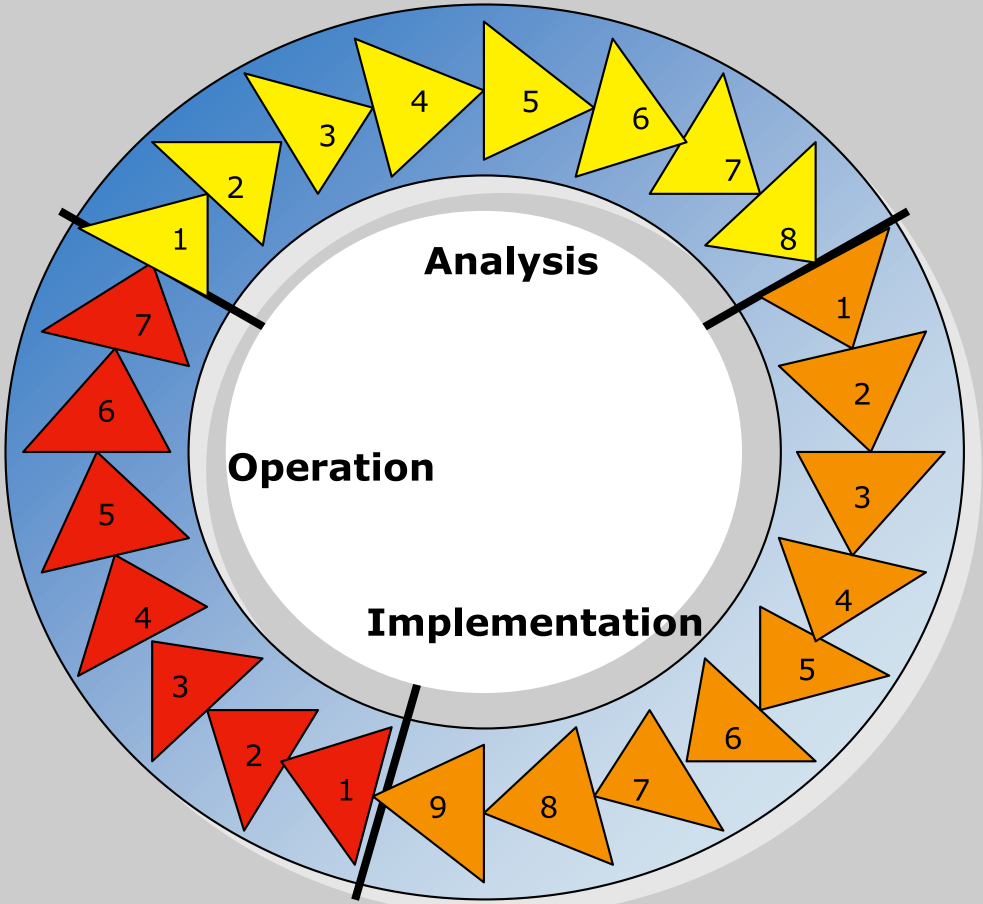
Safety Lifecycle and Tolerable Risk

BLUEFIELD
PROCESS SAFETY

Phases of the Safety Lifecycle

- ***Analysis***
  - **Concept**
  - **Process Specification**
- ***Implementation***
  - **Design**
  - **Build**
  - **Install**
- ***Operation***
  - **Support**

The Safety Lifecycle



BLUEFIELD
PROCESS SAFETY

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**

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**

Safety Lifecycle - Operation

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

Hazard Identification

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

Risk Assessment

- **Consequence Analysis**
- **Likelihood Analysis**

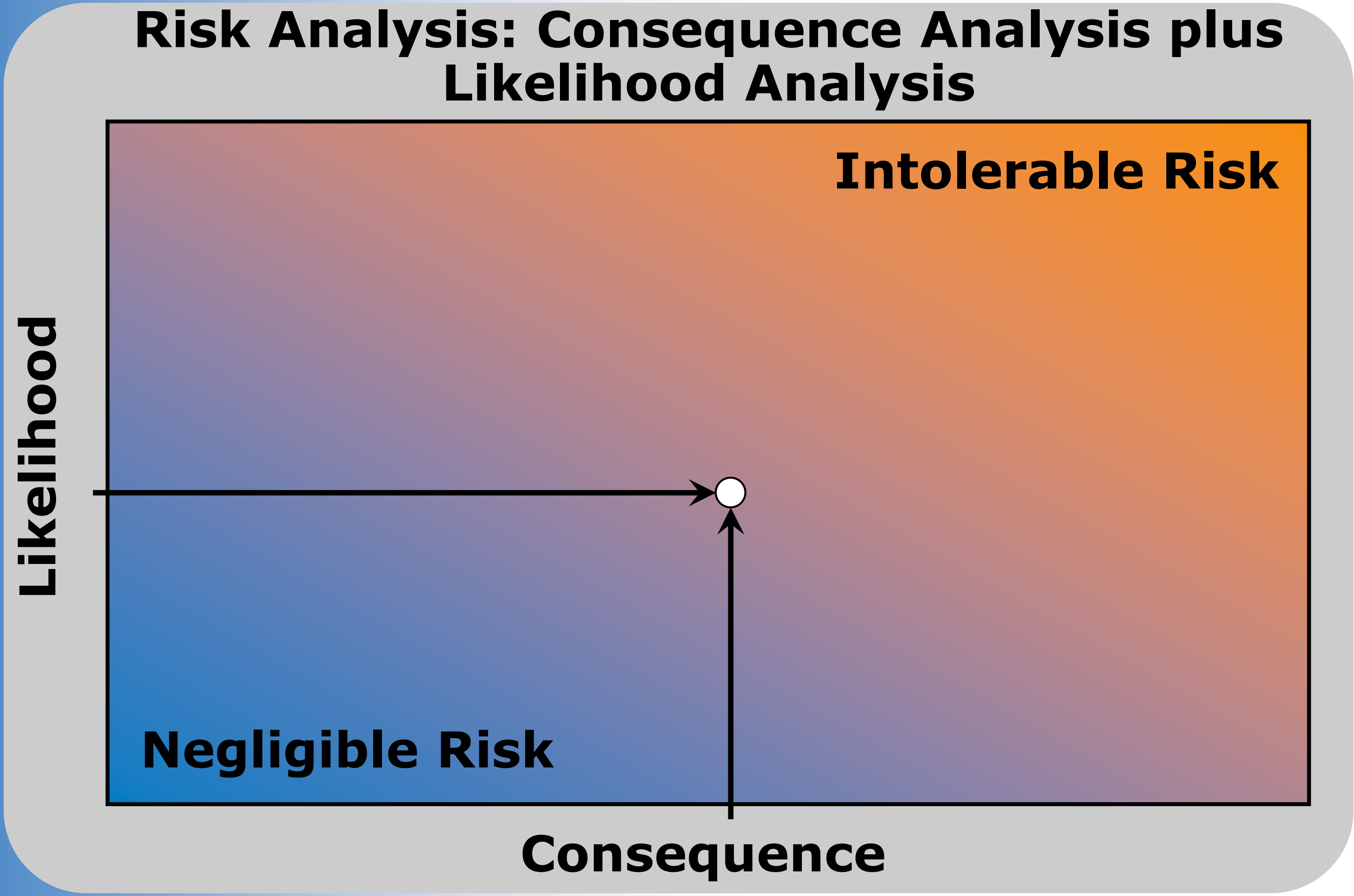
Consequence Analysis

- Statistical Analysis
  - Determined from loss experience in previous events
- Consequence Modeling
  - Determine extent of release
  - Determine effect zone for release
  - Calculate consequences based on extent and effect zone

Likelihood Analysis

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

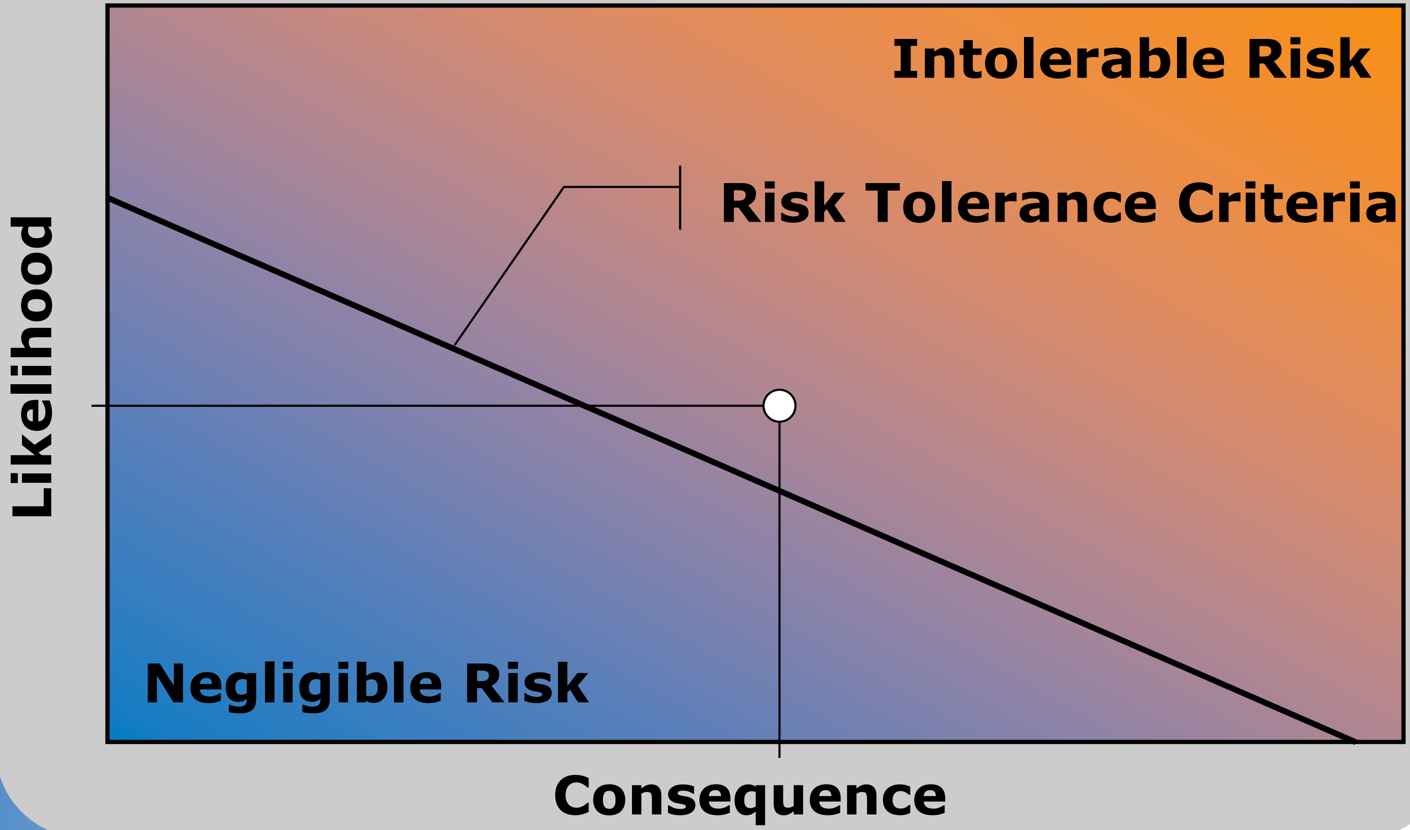
But is the risk tolerable?



Risk Analysis: Consequence Analysis plus Likelihood Analysis

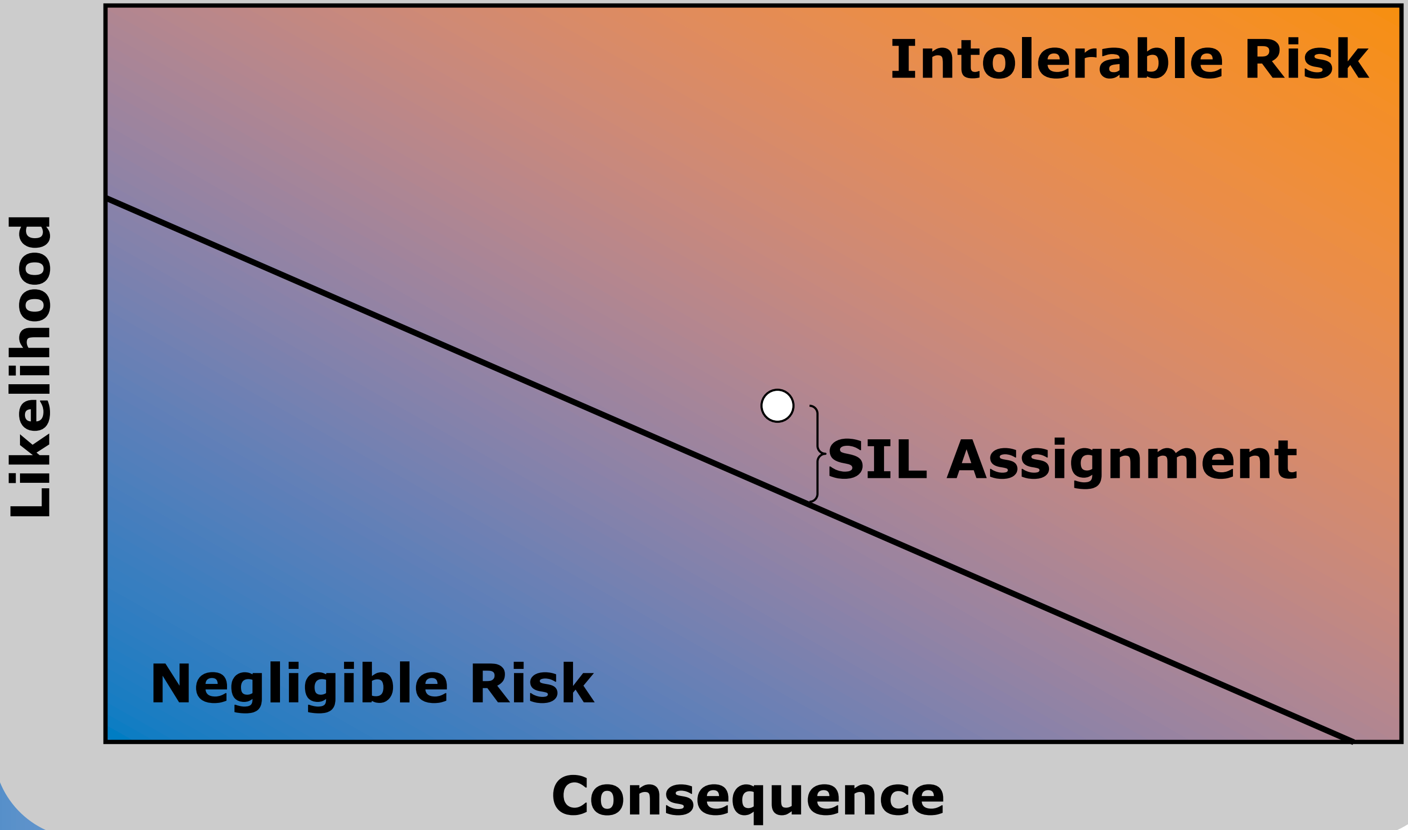
How much risk is too much?

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 also have N/R (not rated) SILs

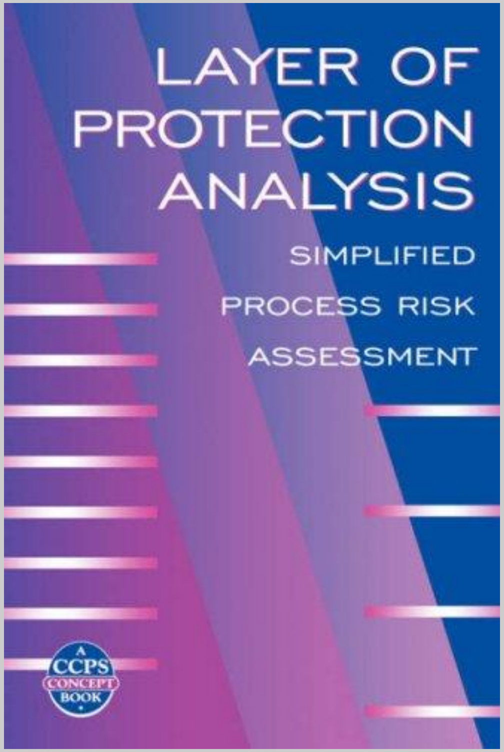
Overview of ISA 84
SIS for the Process Industries

Layer of Protection Analysis

BLUEFIELD
PROCESS SAFETY

Key Publication

- **2001 – *Layer of Protection Analysis: Simplified Process Risk Assessment (CCPS)***



So, what is LOPA?

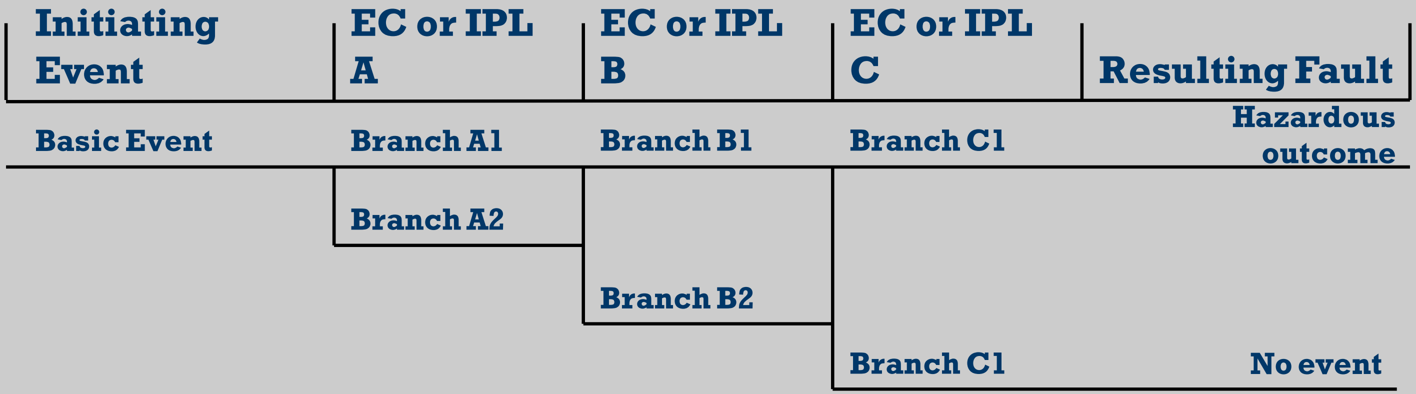
Likelihood analysis linking:

- **Frequency of initiating event (cause)**

  TO

- **Frequency of resulting fault (consequence)**
- **Through chain of enabling conditions and 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

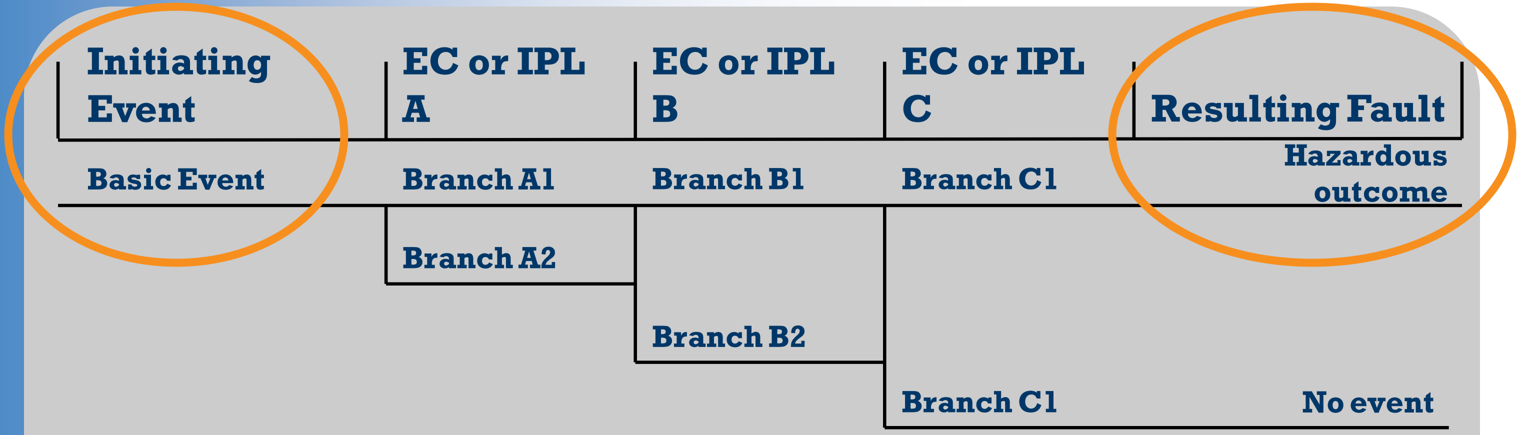
Branch A2

Branch B2

Branch C1

No event

Cause-Consequence Pair



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

- **Initiating Event (Basic Event)**

LEADING TO

- **Resulting Fault (Hazardous Outcome)**

Cause-Consequence Pairs

- Each LOPA scenario has one and only one cause-consequence pair
- Linked through frequency modifiers
  - Enabling conditions
  - Layers of protection

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

Frequency Modifiers

- **Must occur or be present before initiating event can lead to hazardous outcome**
- **May be either an ongoing state or a specific event**
  - **Ongoing states are always called enabling conditions**
  - **Specific events are sometimes called enabling events**

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

Time at Risk – Examples

- **Unit is down for turnaround 15 days each year:**
  350/365 = 0.959 → 0.96
- **Weather is cold enough to freeze line 3½ months a year:**
  3.5/12 = 0.2917 → 0.3
- **Batch with 8.3 hour average cycle time is in raw material charge phase for 1.6 hours**
  1.6/8.3 = 0.1927 → 0.2

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

Occupancy Factor – Examples

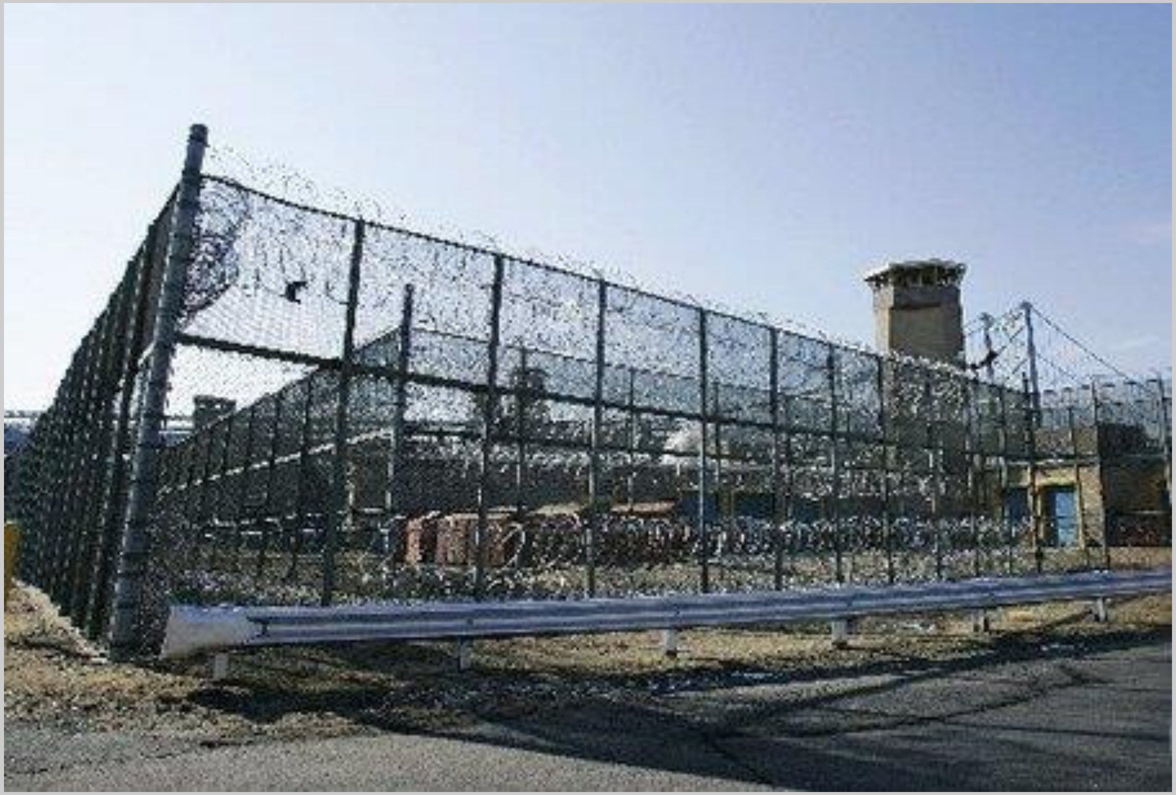
- **Personnel always present:**
  1.000 → 1
- **In area 8 hours a day, 200 days a year:**
  8/24x200/365 = 0.1826 → 0.2
- **In area 10 minutes each 12 hour shift:**
  10/60/12 = 0.01388 → 0.01
- **In area one hour per month**
  1/24/30 = 0.001388 → 0.001

Layers of Protection

- **Less like an onion…**

Layers of Protection

…and more like a prison



IPL rules

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

- **Effective**
- **Independent**
- **Auditable**

Effectiveness

- **Does it act in time?**
  - **Time to detect condition**
  - **Time to decide**
  - **Time to act**
  - **Time to take effect**
- **When it works, does it prevent the outcome event?**
- **Is it enough?**

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

- **It functions as designed?**
- **When it 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**

Overview of ISA 84
SIS for the Process Industries

Challenges and Controversies

BLUEFIELD
PROCESS SAFETY

Challenges and Controversies

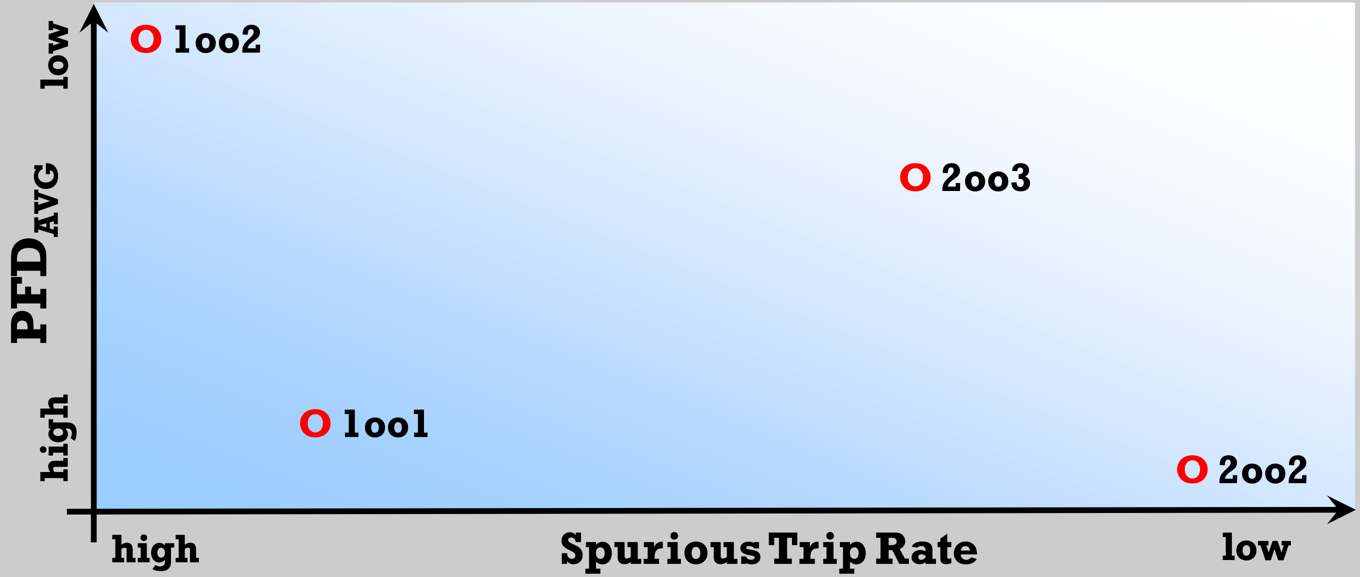
- "Best" architecture
- Proof testing
- BPCS loops
- OSHA enforcement
- Third party certification vs. proven-in-use
- Fault tolerance requirements

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 <u>o</u>ut <u>o</u>f N vote to trip
- **For final control elements:**
  M <u>o</u>ut <u>o</u>f 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

Some common architectures

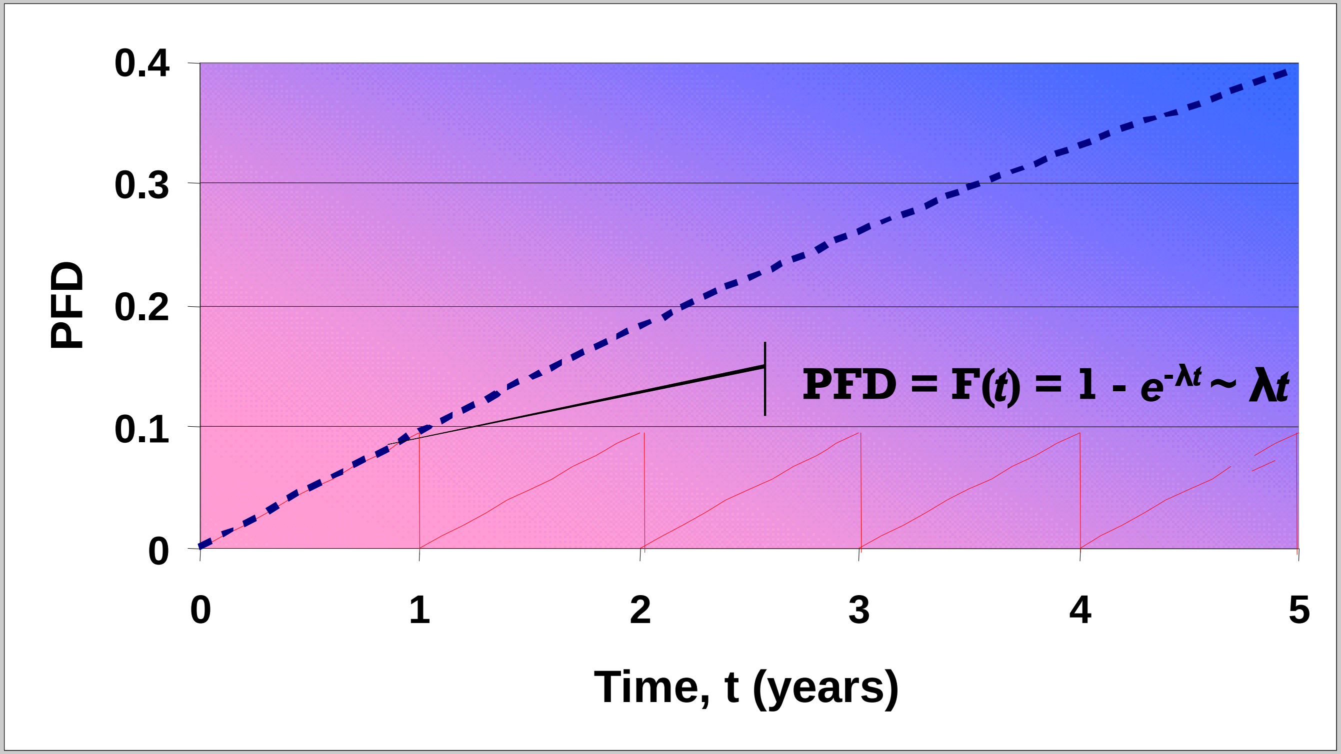
Architecture	Average Probability of Failure on Demand (PFD_{AVG})	Spurious Trip Rate (STR)
1oo1	$\lambda_D T/2$	λ_S
1oo2	$(\lambda_D T)^2/3$	$2\lambda_S$
2oo2	$\lambda_D T$	$2\lambda_S^2 / (3\lambda_S + 2/T)$
2oo3	$(\lambda_D T)^2$	$6\lambda_S^2 / (5\lambda_S + 2/T)$

PFD_{AVG} and STR approximations, given component failure rate data

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



$PFD = F(t) = 1 - e^{-\lambda t} \sim \lambda t$

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

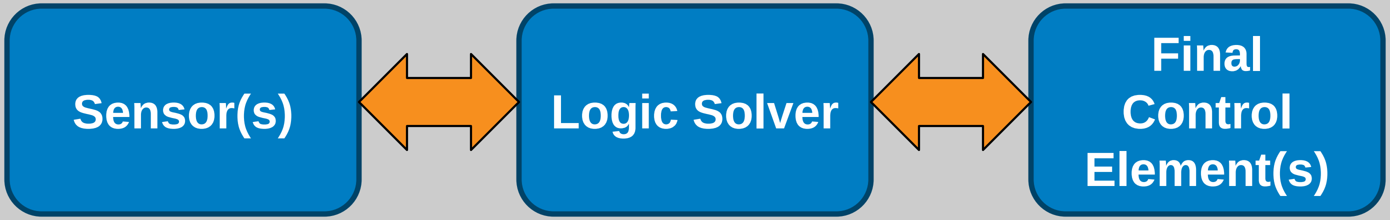
More than one BPCS function?

Two approaches—

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

Credit for Control System

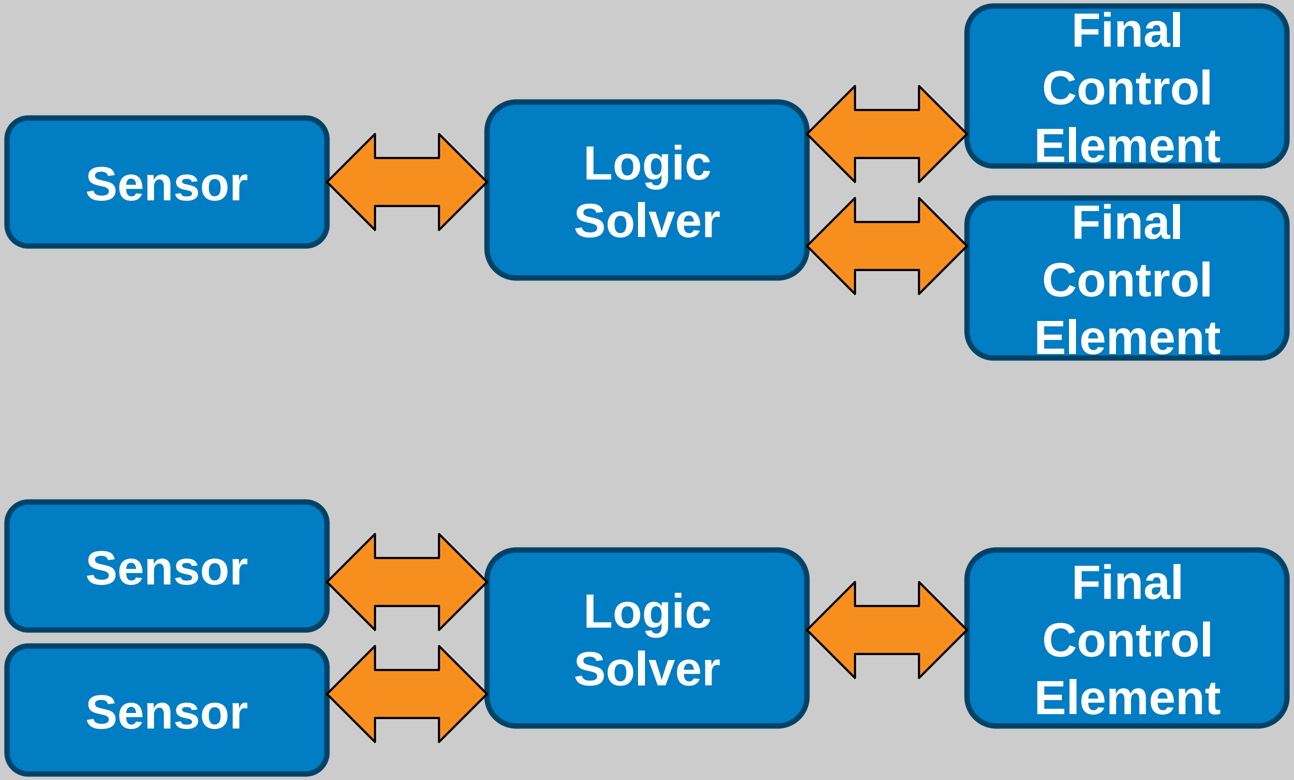
- **BPCS function: $\mathrm{PFD}_{\mathrm{AVG}} = 0.1$**


Sensor(s)

Logic Solver

Final Control Element(s)

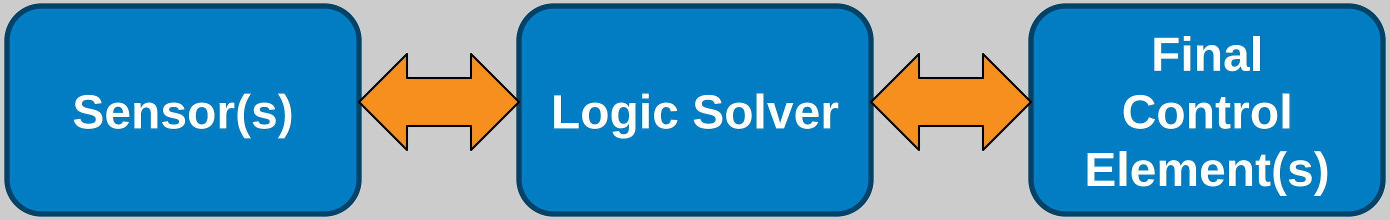
Regardless of instruments



Component contribution

- **For one BPCS function:**

  $PFD_{AVG} = 0.1$



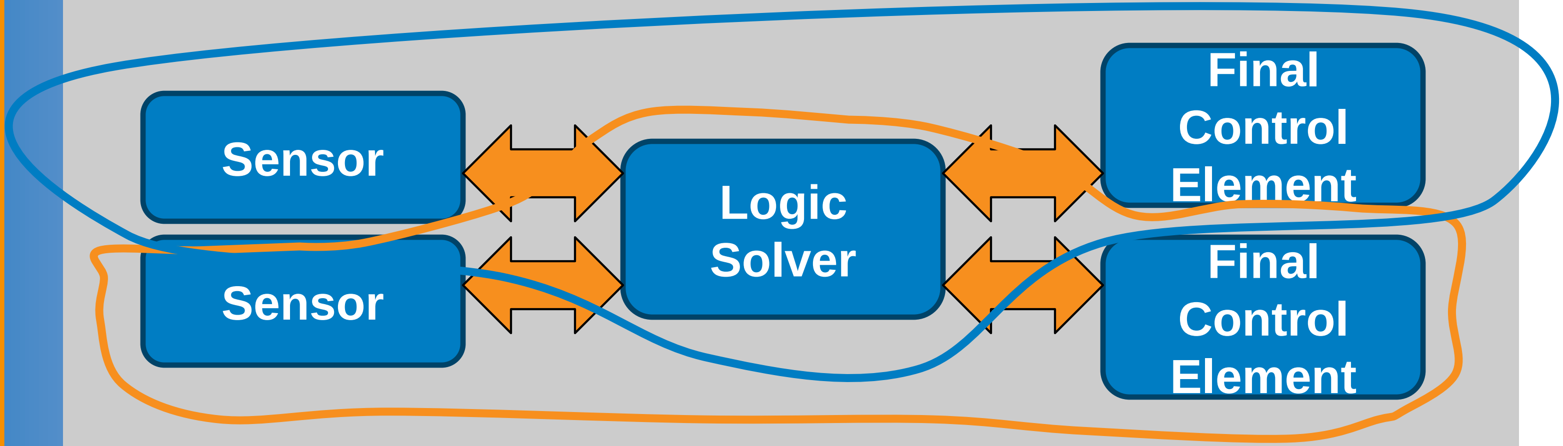
Sensor(s)	**Logic Solver**	**Final Control Element(s)**
~45%	**< 5%**	**~50%**
~0.045	**< 0.005**	**~0.050**

$(0.045 + 0.050) + 0.005 = 0.1$

For two functions

- **Two BPCS functions:**

  $PFD_{AVG} = 0.1 \times 0.1 = 0.01$

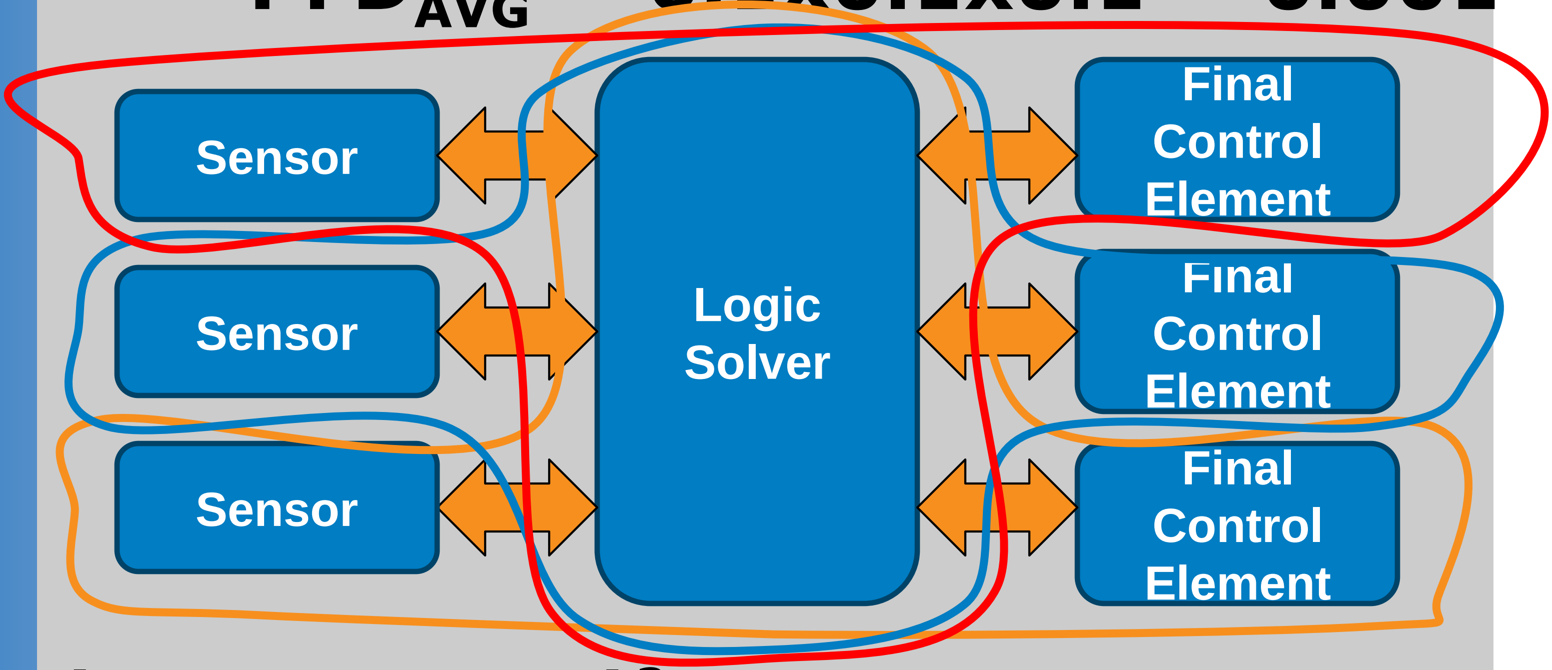


$(0.045 + 0.050)^2 + 0.005 = 0.014$
→ 0.01

How about three functions?

- **Three BPCS functions:**

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



$$(0.045 + 0.050)^3 + 0.005 = 0.0059$$

$$\rightarrow 0.006 \rightarrow 0.01 \neq 0.001$$

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."**

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.**

Summary

Whether they want to or not, instrument engineers are being charged with responsibility to:

- Operate and maintain SIS’s in compliance with regulations
- Design and install SIS’s according rigorous standards
- Establish risk tolerance criteria
- Assure hazard and risk assessments are done well