Tell Me Again, Why Am I Deciding Our Risk Tolerance Criteria?

Presented to

ISA-Kansas City Section

Thursday, March 10, 2016

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**

Topics for today

- **New responsibilities that have fallen to I&E engineers**
- **Getting PHAs right**
- **Need for risk tolerance criteria**
- **How to establish RTC**

New responsibilities for I&E

Whether they want them or not, I&E engineers are being charged with responsibility to:

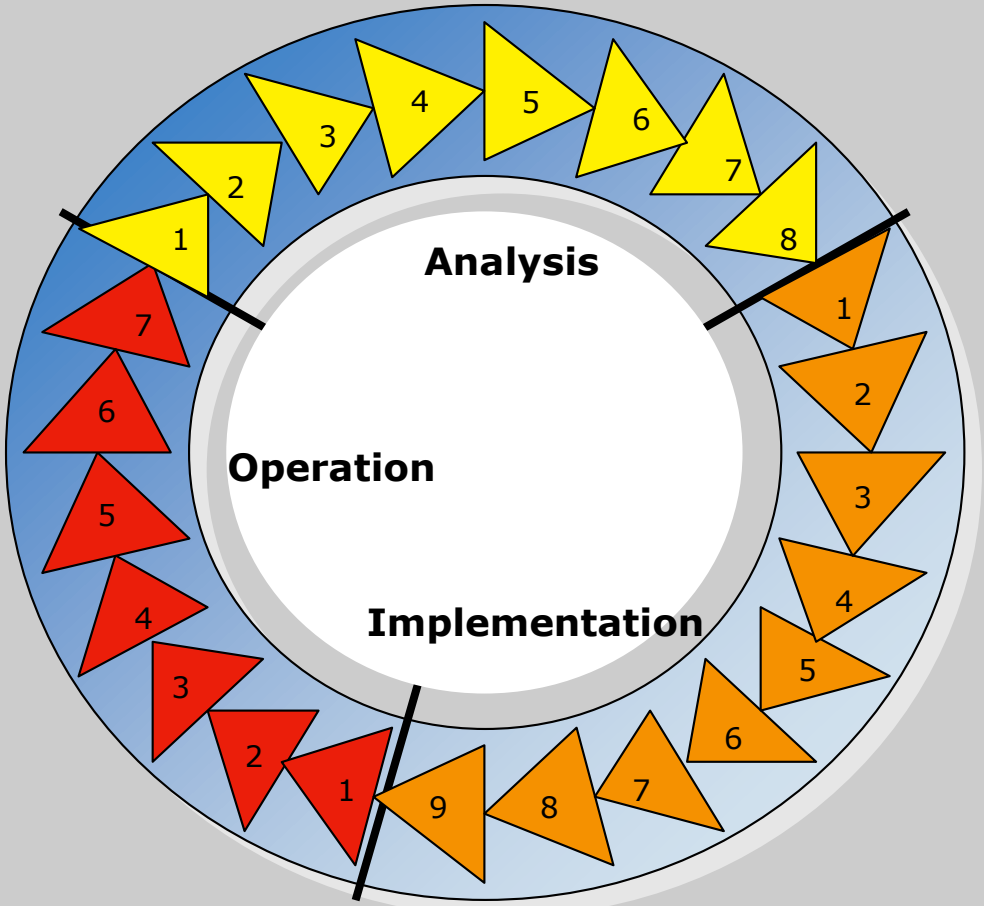
- **Operate and maintain SISs in compliance with regulations and standards**
- **Design and install SISs according to rigorous standards**
- **Establish risk tolerance criteria**
- **Assure hazard and risk assessments are done well**

The SIS Standards

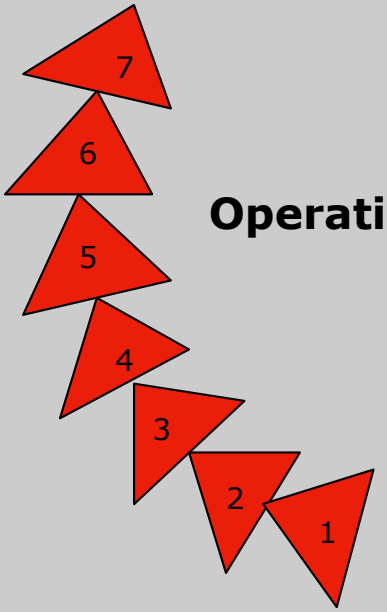
- **ANSI/ISA 84.00.01 Ed. 2 (2004)**
- **IEC 61511 Ed. 1 (2003, Ed. 2 in 2016)**
- **IEC 61508 Ed. 2 (2010)**

- **All call for addressing the safety lifecycle**

What is the Safety Lifecycle?



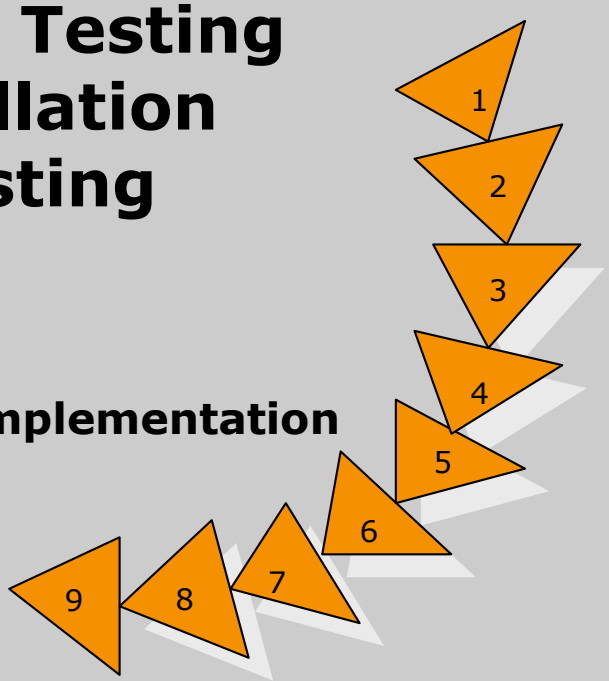
SLC—Operation



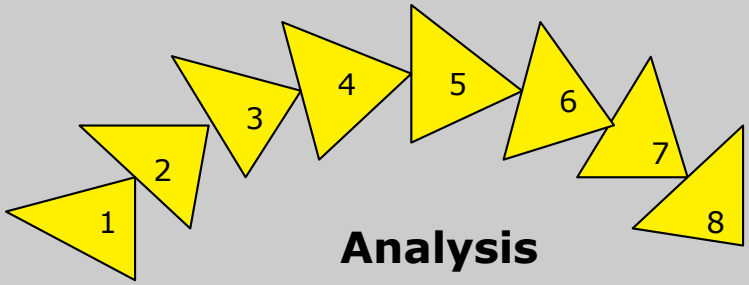
1. **Operation**
2. **Training**
3. **Proof Testing**
4. **Inspection**
5. **Maintenance**
6. **Management of Change**
7. **Decommissioning**

SLC—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**



SLC—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**

Steps before working on an SIS

- **Assess risk, which has two components: consequence and likelihood. Both require assessment.**
- **Before risks can be assessed, hazards must be identified.**
- **Hazards are identified during a PHA.**
- **HazOp is the most common form of PHA in the process industries**

Identify hazards

- **Hazards are identified during a PHA.**
- **HazOp is the most common form of PHA in the process industries**

Steps of the HazOp method

Performed node-by-node

- **Considers defined deviations**
  - **Considers causes of deviations**
    - **Considers consequences of deviations**
      - **Identifies safeguards to protect against causes and consequences**
        - **Assesses risk**
          - **Makes recommendations**

HazOp: Deviations

- **Use a standard list of deviations**
- **Mark "N/A" when the parameter has no meaning for the node, or when a limit does not exist**
- **Mark "NCOI" (No Cause of Interest) when a limit exists, but there is no conceivable way to exceed the limit**

HazOp: Causes

- **Faults (equipment failures or human errors), not other deviations**
- **The failure of a safeguard is not a cause; something else must first cause the deviation**
- **No "Double jeopardy" exemption; multiple failures reduce likelihood, but do not make impossible**

HazOp: Consequences

- **Two parts: events and impacts**
- **Events**
  - **Fires**
  - **Explosions**
  - **Toxic releases**
- **Impacts**
  - **Personnel safety**
  - **Community safety**
  - **Environment**
  - **Assets (Commercial, Financial)**

HazOp: Safeguards

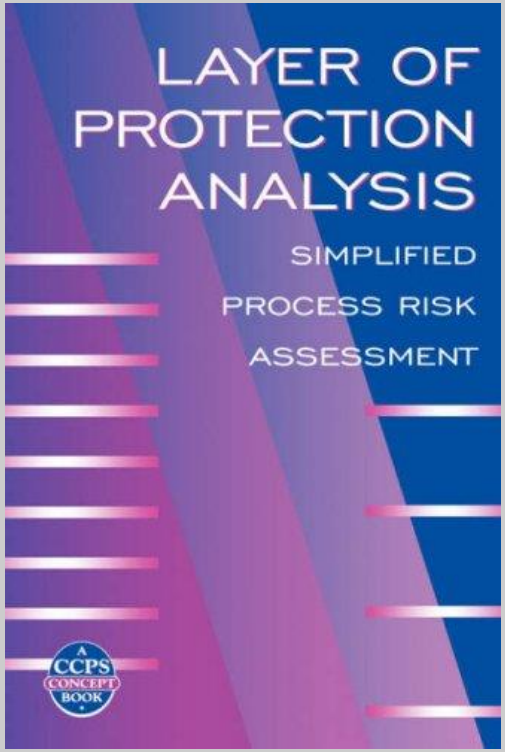
- **Typically reduce likelihood of events (Preventative)**
- **Occasionally reduce severity of impacts (Mitigative)**
- **List everything that helps, not just IPLs per LOPA**
- **Exception: Do list protective functions that are based on something that has been identified as the cause**

HazOp: Risk Assessment

- **Two parts: consequence (impact) and likelihood**
- **"Worst case" vs. Likely case**
- **Risk assessments by HazOp teams:**
  - **Good at estimating events**
  - **Passable at estimating impacts**
  - **Terrible at estimating likelihood**
- **Match likelihood to consequence**

Estimating likelihood

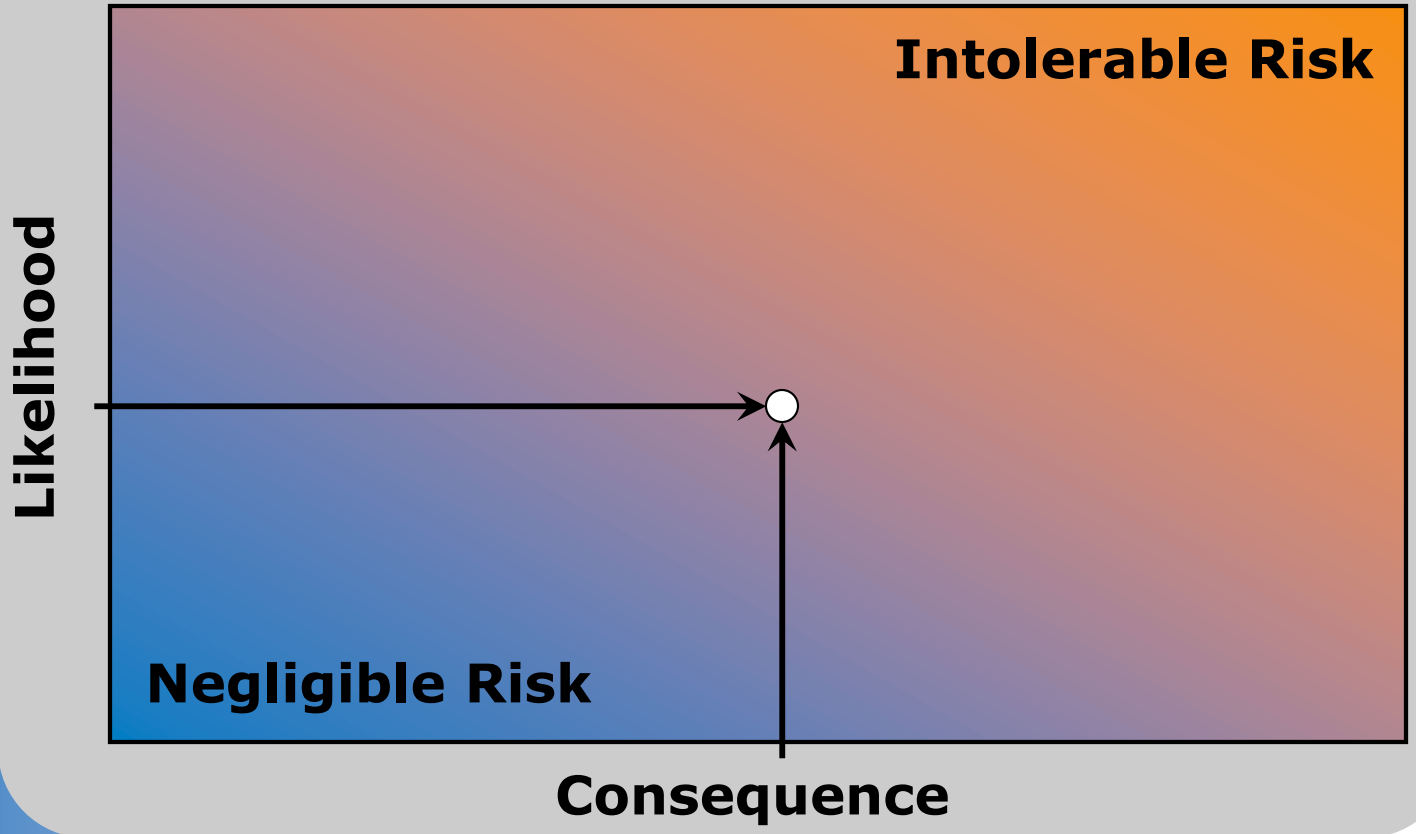
- **Fault tree analysis (FTA)**
- **Event tree analysis**
- **Markov modeling**
- **Layer of Protection Analysis (LOPA)**



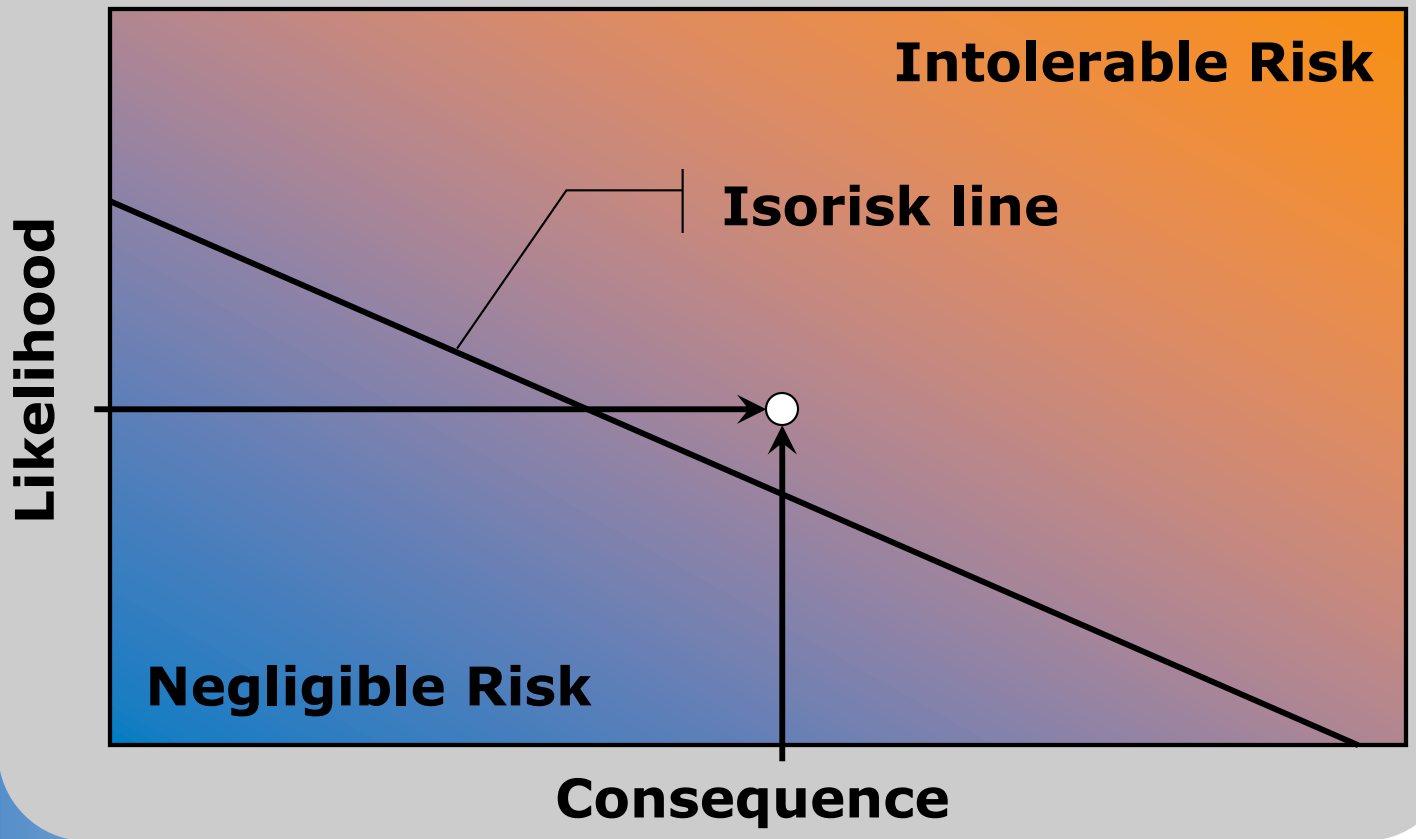
HazOp: Recommendations

- **All PHA recommendations must be resolved**
- **"Consider" or "Confirm"**
  - **"Consider" because there may be better approaches**
  - **"Consider" still requires resolution and documentation**
  - **"Confirm" when there is not certainty that safeguard is in place; may still not be required**
- **"Perform LOPA"or"Perform QRA"**

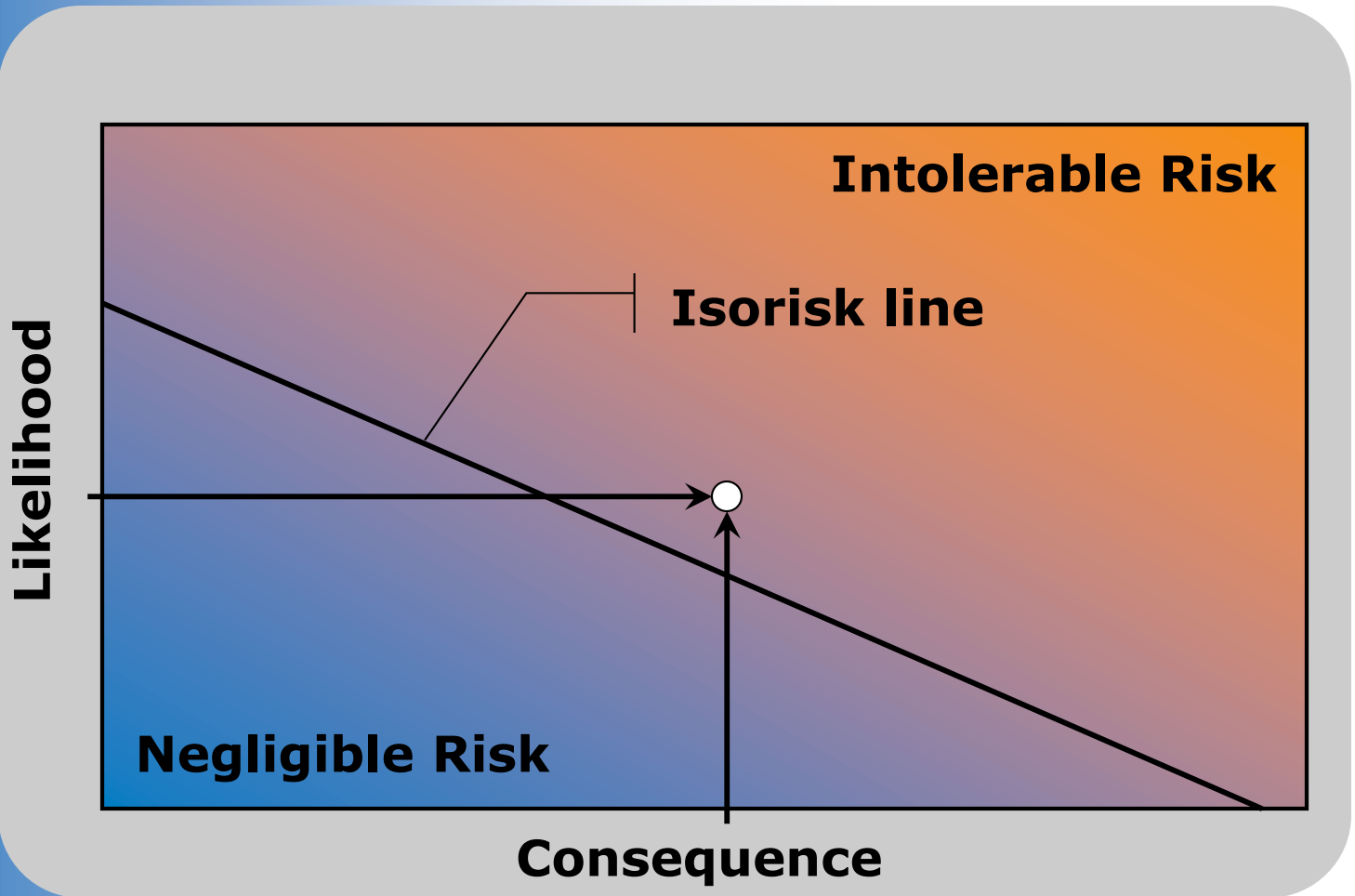
But is the risk tolerable?



Only in comparison to RTC

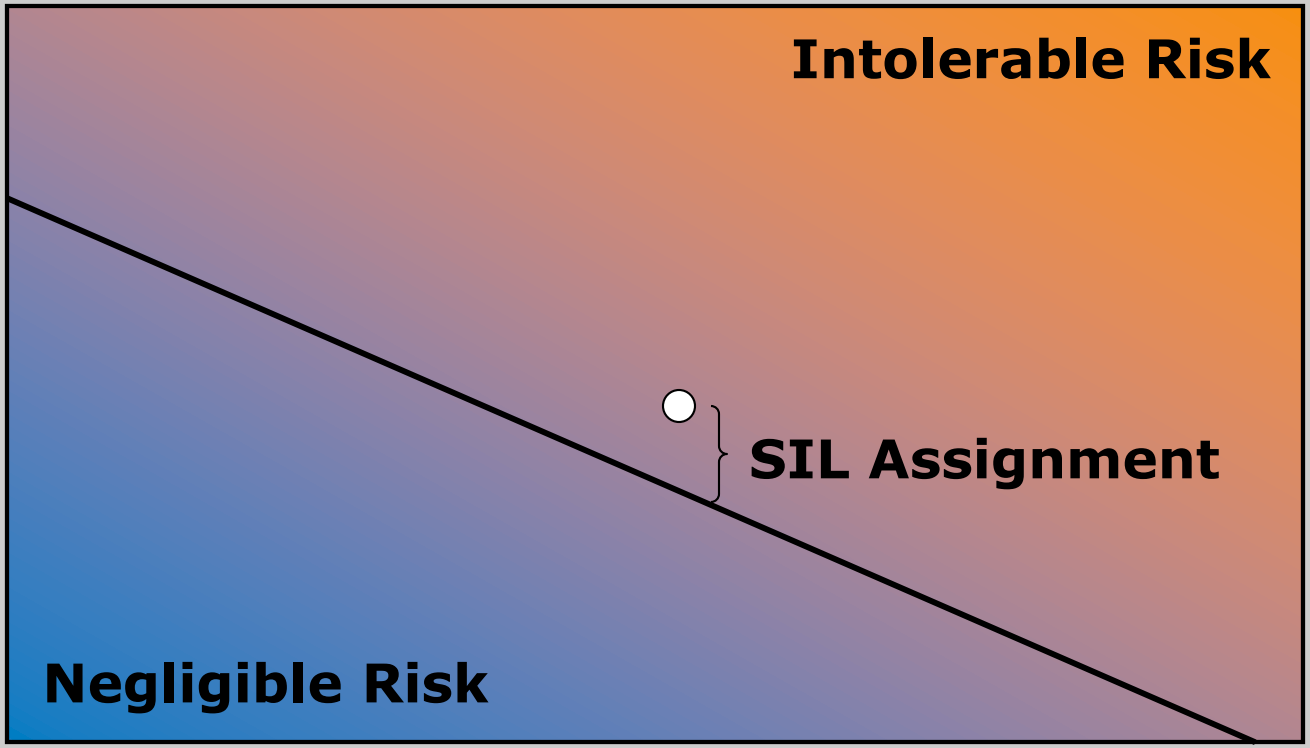


Only in comparison to RTC



Comparison determines RRF

Risk reduction factor is ratio of estimated risk to tolerable risk, which assigns SIL for safety functions.



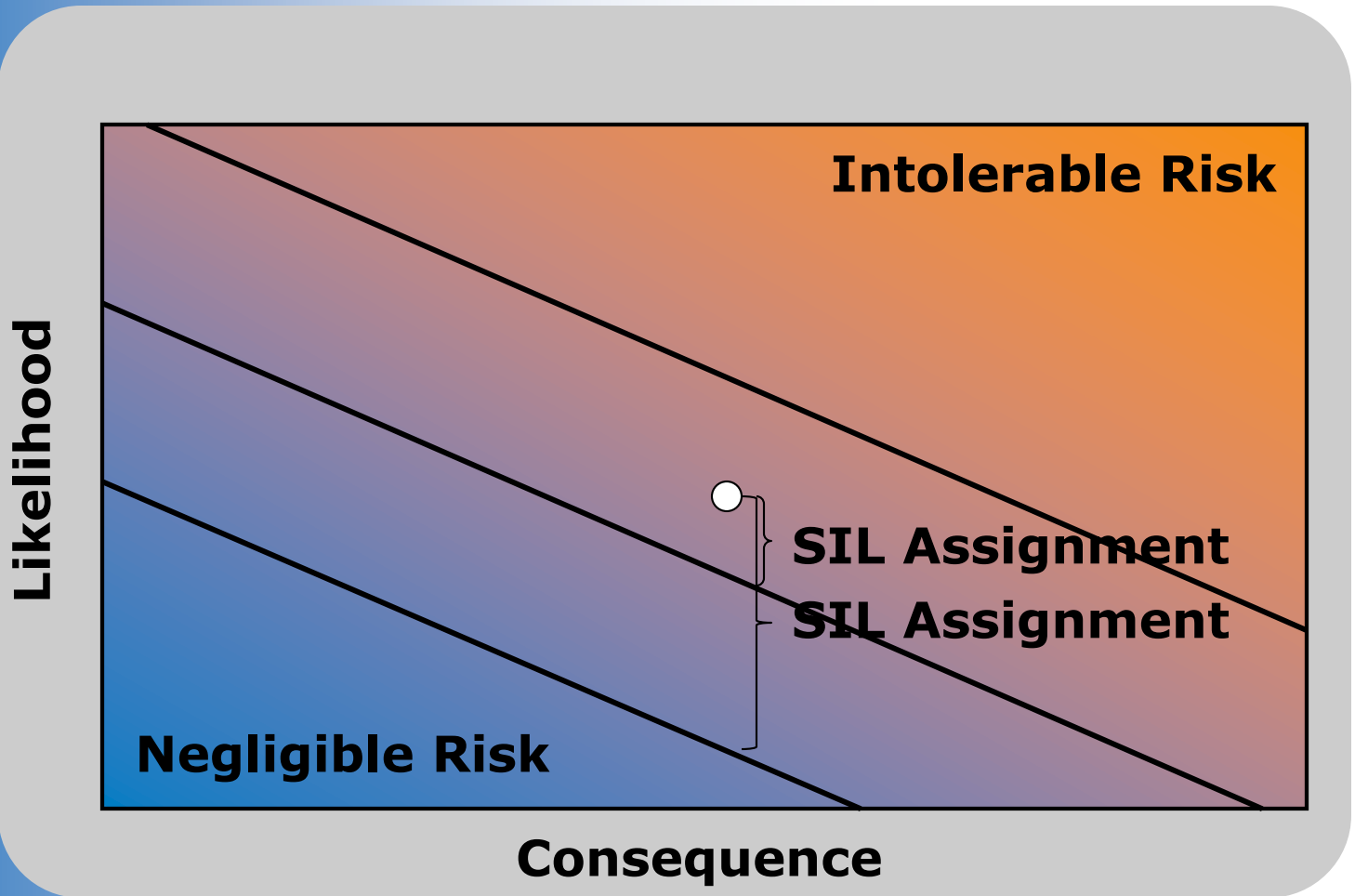
What is a SIL?

- **Safety Integrity Level**

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 SILs of N/R (not rated), aka SIL 0, SIL A**

But what risk tolerance criteria?



No SIS without RTC

- **Safety Instrumented Systems require engineering specifications for risk tolerance criteria before a SIL can be assigned**
- **SILs must be assigned before a SIS can be designed**
- **"ZERO RISK" is rhetoric, not an engineering specification**

What, me worry?

He is insubordinate to officers and noncoms alike, and is an excellent candidate for court martial or reform school.

Yes, I'm worried!

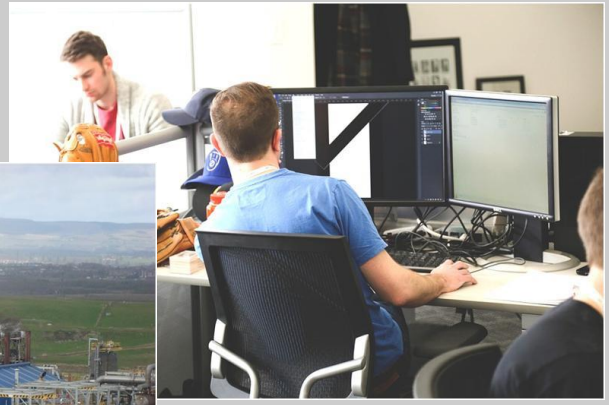
Safety Instrumented Systems require engineering specifications for Risk Tolerance Criteria before design can begin.

What is your tolerable risk?

- **As an individual, what do you believe the tolerable risk should be for a workplace?**

Tolerable Risk exercise

- **Imagine a workplace**



Tolerable Risk exercise

- **How great would the mean time between fatalities have to be for you to consider it a safe workplace?**

Tolerable Risk exercise

- **How many people work there?**

Tolerable Risk exercise

- **Calculate the tolerable fatality rate implied by those two assumptions.**
- **Express tolerable risk in terms of fatalities per 100,000 FTEs (200 million hours worked)**

Plant A – 1 fatality/1000 years

- **Assume that 1 fatality per 1000 years is "safe"**
- **Exposed workforce ~ 50 workers (FTEs)**

(1 fatality / 1,000 years)
x (1 year / 50 FTEs)
= 1 fatality / $5x10^4$ FTEs
= 2 fatalities per 100,000 FTEs

Is that safe?

The Bureau of Labor Statistics reports fatalities rates in units of

- **Deaths per 100,000 FTE (wk-yrs)**

  OR

- **Deaths per 200 million hours worked**

Safest occupations

- **0.4 – Mathematician**
- **0.4 – Business/financial**
- **0.4 – Educator/librarian**

BLS – 2014 Data

http://www.bls.gov/iif/oshwc/cfoi/cfoi_rates_2014hb.pdf

Overall

2014 statistics:

- **4,679 fatalities**
  in the U.S. workplace
- **3.3 fatalities**
  per 100,000 FTE
  per 200 million hours worked

BLS – 2014 Data

http://www.bls.gov/iif/oshwc/cfoi/cfch0013.pdf

How does example compare?

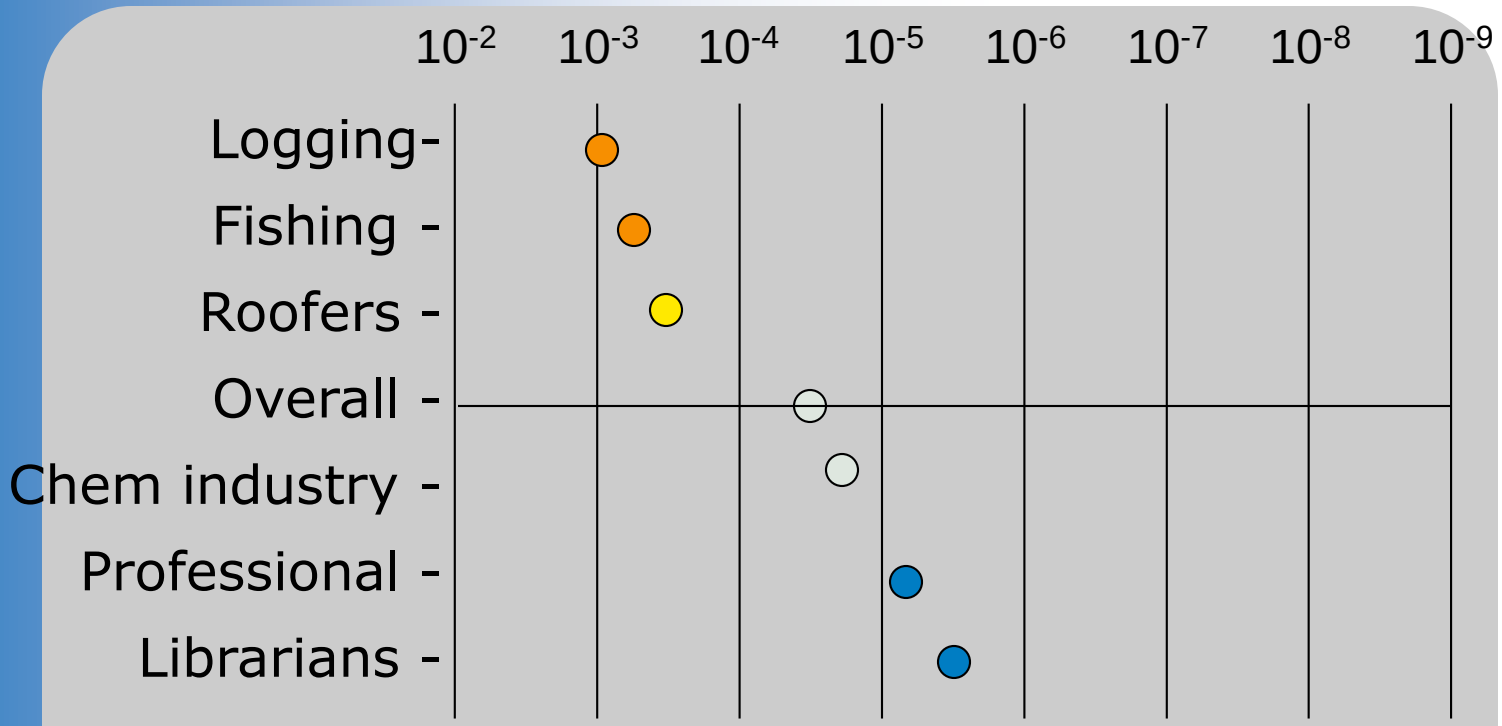
Example:

- **2.0 fatalities**
  per 100,000 FTEs
  per 200 million hours worked

U.S. workplace in 2014:

- **3.3 fatalities**
  per 100,000 FTEs
  per 200 million hours worked

Other industries/occupations?



Fatality rates range almost three orders of magnitude from safest to most fatal occupations.

Not all risk is process risk…

- **41% Transportation**
- **16% Violent acts**
- **15% Falls**
- **16% Contact with object**
- **3% Fires or explosions**
- **9% Exposure to harmful substances or environments**

BLS – 2006-2013 average Data – U.S. workplace

…even in the process industries

- 22% Transportation
- 13% Violent acts
- 7% Falls
- 20% Contact with object
- 24% Fires or explosions
- 14% Exposure to harmful substances or environments

BLS – 2006-2013 average Data – U.S. workplace

Allocating overall risk to process

- **How would you allocate process risk (in %)?**
- **It depends on the industry**
- **Process risk – about half of individual risk is process risk**

Return to RTC exercise

- **Total tolerable risk for individuals**
  = 2 x 10^{-5} fatalities/yr
- **Assume process safety risk accounts for half of all risk**
  = 1 x 10^{-5} fatalities/yr

Should all process safety risk be allocated to a single process hazard?

Allocating risk to a hazard

Do not allocate all process risk to a single hazard!

How much risk should a single hazard represent?

- **Process safety risk**
  = 1 x 10^{-5} fatalities/yr
- **Single process hazard risk**
  5% to 20% of process risk
- **Tolerable scenario risk (@ 20%)**
  = 2 x 10^{-6} fatalities/yr

Tolerable scenario frequency

- **From example: Tolerable frequency for fatal scenario is**

$$\frac{2 \times 10^{-6} \text{ fatalities/yr}}{1 \text{ fatality/event}} = 2 \times 10^{-6} \text{ event/yr}$$

- **Compare to typical RTC in the range of 1×10^{-4} to 1×10^{-6}**
- **Once this value is pinned down, the remaining RTC can be developed**

Summary

- **SIS projects impose responsibilities on I&E engineers that have nothing to do with instrumentation**
- **A successful SIS project depends on doing the PHA right—the old ways are no longer sufficient**
- **A successful SIS project also depends on having RTC; if you don't have them, you must develop them—and you can**

Questions?