Optimizing Layers of Protection for Robust Process Safety

Tekin Kunt, Ph.D.

May 6, 2026

Process Safety and Reliability Group
800 W. Sam Houston Pkwy. South
Suite 107
Houston, Texas 77042-1908
Tel: 713-532-8800 800-250-8511 Fax: 713-532-8850
Email: psrghouston@psrg.com Web: www.psrg.com

P2SAC
Purdue Process Safety & Assurance Center

Presenter – Tekin Kunt, Ph.D.

Tekin Kunt, Ph.D.
tkunt@psrg.com

- PSRG Director, EMEA (9+ years)
- Based in Houston, Texas (29+ years)
- Ph.D., Chemical Engineering – University of Maryland @ College Park (1993)
- Risk Assessments / Audits / Training
- Weatherford / Chevron / AspenTech / NIST
- Bridge / Macro Photography

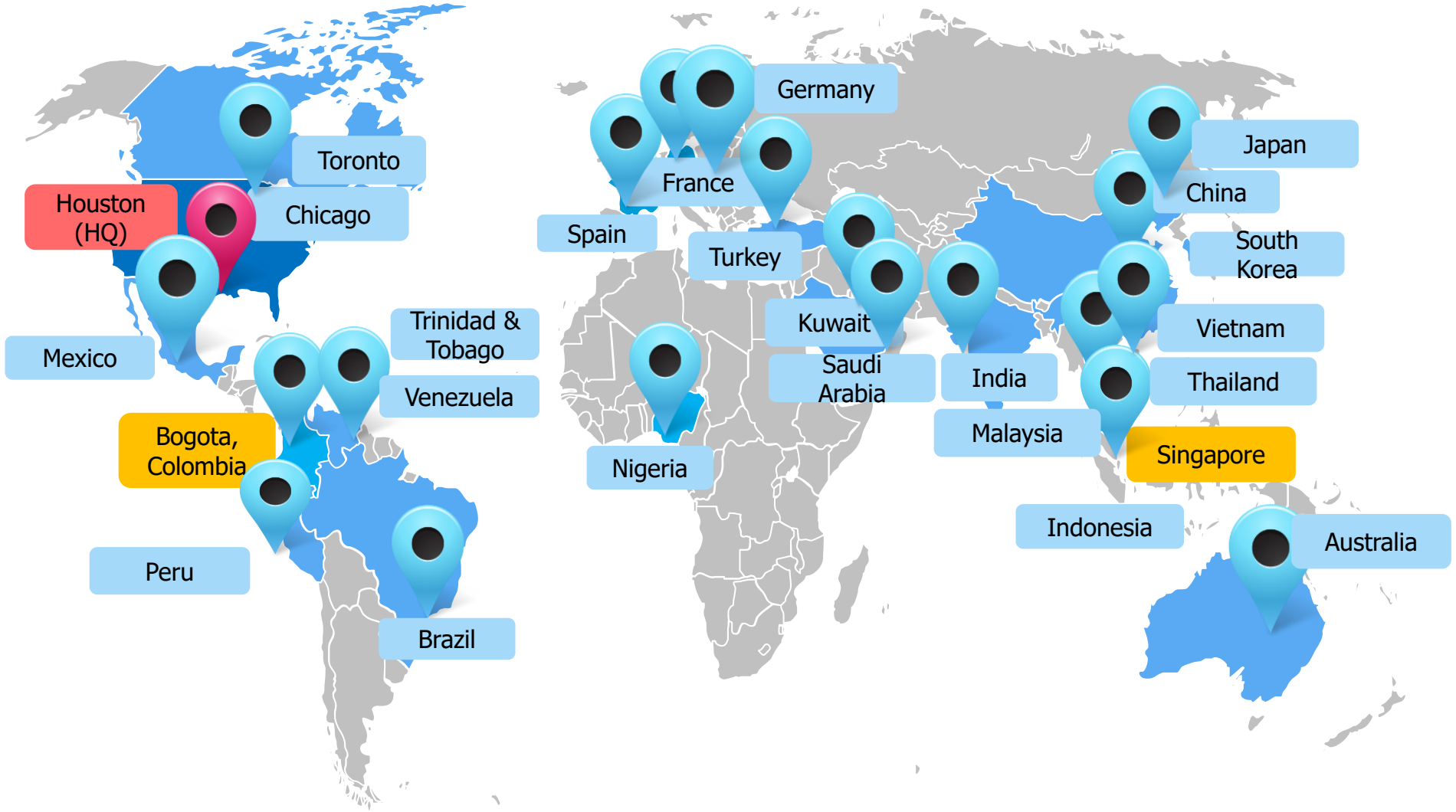
About PSRG

- Established in 1997 in Houston, TX (~30 years)
- Global Process Safety, Risk Management & Plant Reliability consulting and training firm
- More than 100 technical professionals averaging 29+ yrs experience
- Diverse industry experience with more than 1000 customers in 90 countries
- Tailored solutions to meet and exceed client expectations
- Member of AIChE CCPS, IChemE PSC, P2SAC and VPPPA

www.psrg.com

Process Safety and Reliability Group

PSRG – Global Reach



P2SAC / PSRG

- PSRG has been a supporter of P2SAC since 2021 (online presentation on Common Cause Failure)
- Many presentations since then such as MoC tutorial, PSKM, Wearables in PS, PS performance measurement, AI in PS, to list a few.

- This one is with Ms. Aishwarya Shetye and Mr. Jonathan Marquardt

- THANKS !!

Question

- Based on a Risk Assessment (e.g., HAZOP/LOPA), there is a need for a Risk Reduction Factor of 100 – to be closed by a Safety Instrumented System (SIS)
- Would you prefer 2 layers of protection, each with SIL1, OR
- Would you prefer a single layer with SIL2 ?

- ANSWER: It depends !!

Safety Moment(s) – BP Texas City / Bouncefield

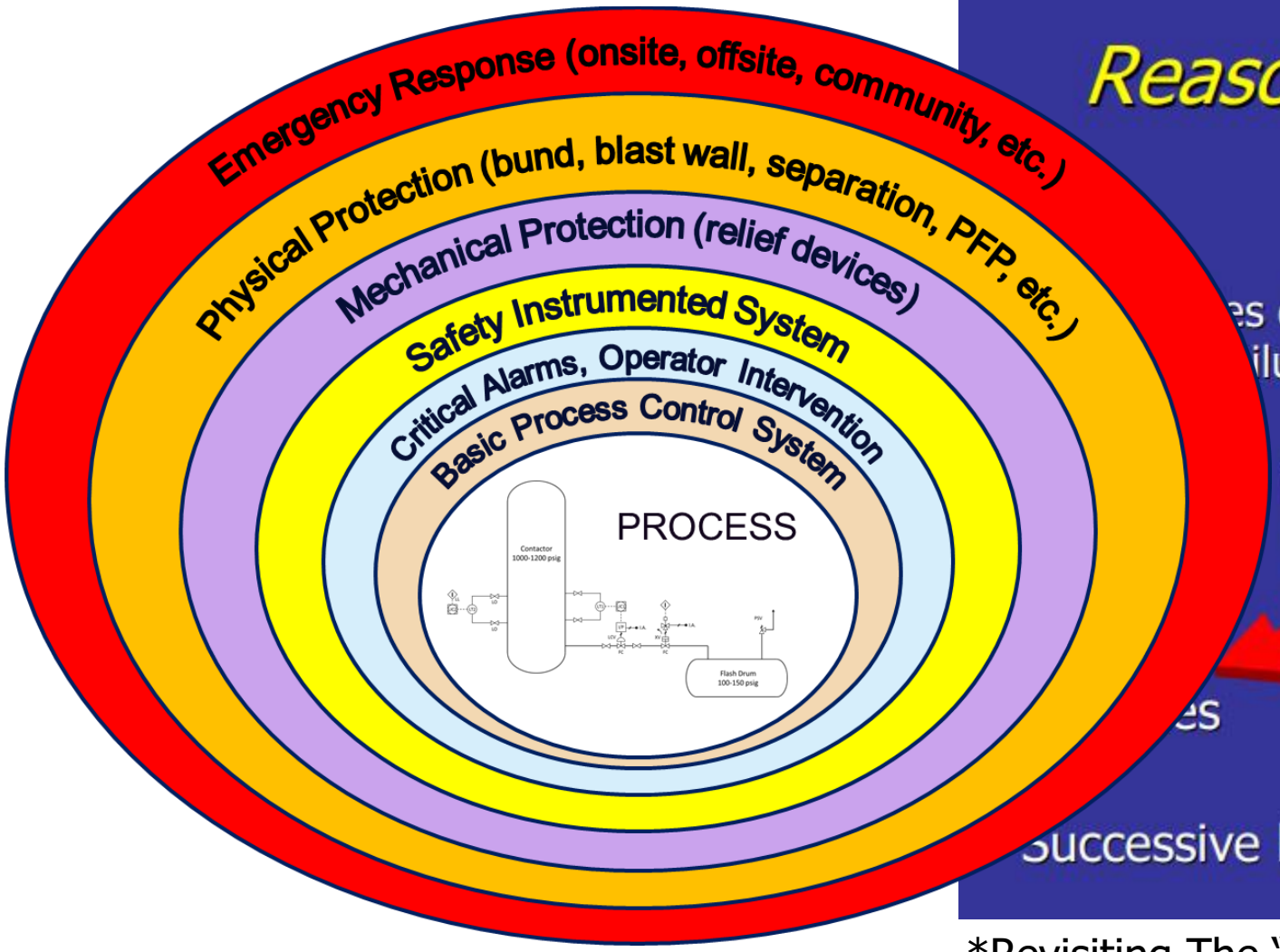
- Isom Unit overfilling
- Tank overfill scenarios

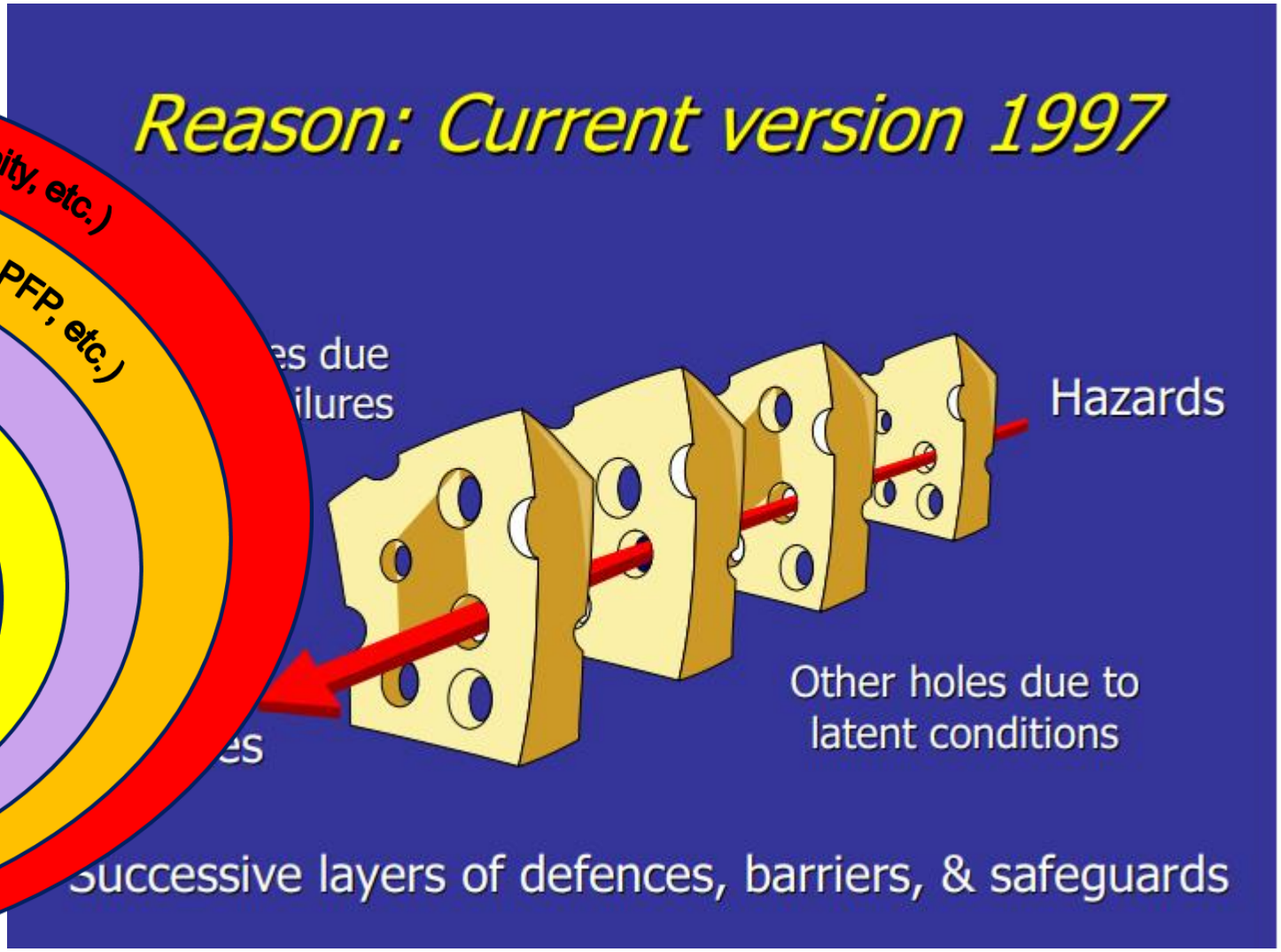
Layered Protection in Process Safety

"A chain is only as strong as its weakest link".

First appeared in 1786 in Thomas Reid's book, *Essays on the Intellectual Powers of Man*

Onion or Cheese?





*Revisiting The "SWISS CHEESE" Model of Accidents, EUROCONTROL EXPERIMENTAL CENTRE (2006)

Determining the Layers of Protection Needed

- HAZOP (qualitative)
- LOPA (semi-quantitative)
- QRA (quantitative risk analysis)
- In essence: 1) understand what could go wrong, 2) how bad it can get and how likely that might happen, 3) what we must do to prevent / mitigate this unwanted outcome

Setup of the Problem

- Let's assume that we need a Risk Reduction Frequency (RRF) of 100
- Should we use one layer of protection with an RRF of 100?
- OR, should we use two layers of protection, each with an RRF of 10?
- The answer depends on many factors plus each company might have a different safety philosophy

Question

How does your Company tackle this question?

Factors in Selecting Process Safety Philosophy

"There's an old saying that if you think safety is expensive, try an accident. Accidents cost a lot of money. And, not only in damage to plant and in claims for injury, but also in the loss of the company's reputation."

Dr. Trevor Kletz

Optimization Framework* - Assumptions

- Assume $\boldsymbol{L}$ is the optimum number of Layers; $L \in \{1, 2, 3\}$
- Assume $\mathbf{N_i}$ is the SIL level for the i^{th} Layer; $N_i \in \{SIL1, SIL2, SIL3\}$

- An alarm (or safety action) is generated when any of the layers is activated. A layer's activation is independent from the other layers.

- Failure of each layer is independent of any other layer (independence)

* Kulahci and Kunt, 2026, GCPS Poster

Optimization Framework – Set up costs

- Assume set up costs go up linearly with each layer but increase exponentially as SIL level increases in each layer.

- a_i is the fixed cost of activating layer i
- b_i is the base cost scaling for layer i
- $r_i > 1$ is the exponential growth rate for layer i

$$\sum_{i=1}^{L} \left(a_i + b_i r_i^{N_i} \right)$$

False Alarm vs. Probability of Failure on Demand (PFD)

- For each SIL level at each layer N_i:
- $p_i(N_i)$: probability that the layer **correctly detects a fault** (true positive)
- $q_i(N_i)$: probability that the layer raises alarm **when no fault exists** (false positive)
- As N_i (SIL level in Layer i) increases p_i increases but also q_i increases

System Level Alarm Logic

- Action is taken if any layer activates and layers are independent from each other, so:

- Probability that the system detects a fault (i.e., **true positive**) is

$$P_{TP}(L, \mathbf{N}) = 1 - \prod_{i=1}^{L}\left(p_i(N_i)\right)$$

- Probability that the system raises a **false alarm** is

$$P_{FP}(L, \mathbf{N}) = 1 - \prod_{i=1}^{L}\left(q_i(N_i)\right)$$

Optimization Framework – Cost Functions

- Assume that π is the probability of initiating event being present (i.e., fault)
- Cost of not having safety system activated (Cs – safety cost)

$$C_s \pi \left(\prod_{i=1}^{L} (1 - p_i(N_i)) \right)$$

- Cost of production loss due to a false alarm (Cp)

$$C_p (1 - \pi) \left(1 - \prod_{i=1}^{L} (1 - q_i(N_i)) \right)$$

Putting All Together

Optimization Framework – Objective Function

$$\min C_{total}(L,N) =$$

$$\sum_{i=1}^{L}\left(a_i + b_i r_i^{N_i}\right) + C_s \pi \left(\prod_{i=1}^{L}\left(1 - p_i(N_i)\right)\right) + C_p(1-\pi)\left(1 - \prod_{i=1}^{L}\left(1 - q_i(N_i)\right)\right)$$

Optimization Framework – Discussion

Easy to solve when **parameter values** are given however the formulation can be **parameterized** for understanding when to switch the chosen safety scheme.

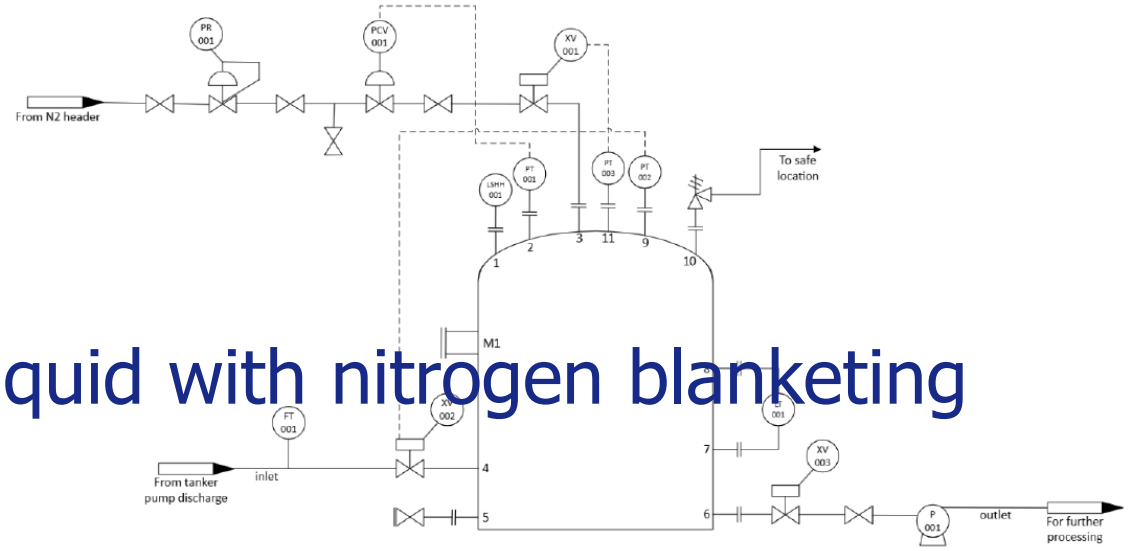
Illustrative Examples

"*Un bon croquis vaut mieux qu'un long discours.*"

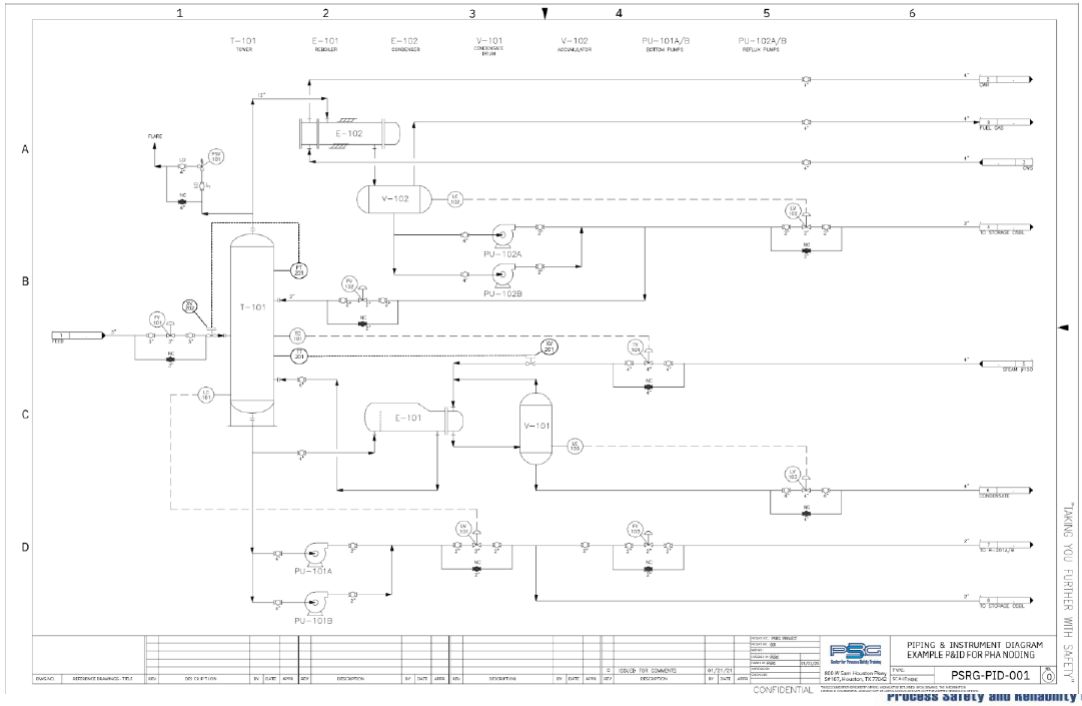
"*A good sketch is better than a long speech.*"

Napoleon Bonaparte

Test Problems



- Storage Tank handling flammable liquid with nitrogen blanketing
- Benzene-Toluene Distillation Column



Storage Tank Example

- Case 1: 2 X SIL1 layer → Total Cost 94K
- Case 2: 1 X SIL2 layer → Total Cost 140K

- Cs / Cp = 145 (false alarm and loss of production has a low impact compared to loss of containment due to tank collapse)

Distillation Column Example

- Case 1: 2 X SIL1 layer → Total Cost 157K
- Case 2: 1 X SIL2 layer → Total Cost 177K

- Cs / Cp = 13 (false alarm and loss of production has a high impact compared to loss of containment due to column overpressure)

Other Considerations

- Common Cause Failure – reducing effectiveness of multiple safety layers
- Process Safety Time (PST) – as the PST reduces, it might be more advantageous to use a single layer with a higher SIL level
- Existence of skilled and well-trained instrumentation / maintenance team
- The Proof Testing interval – as higher SIL level is needed, the more frequent testing might be required

What is Next?

- Set up a sensitivity analysis based on the optimization framework
- Understand when a company should switch from one safety philosophy to another one
- Investigate how the initial event probability distribution might affect the safety philosophy
- Develop other test examples that include both mass and energy balances (e.g., CSTR or other reactive systems)

Summary

- Safety philosophy is a function of many different (and always competing) factors
- Understanding these factors allow companies to optimize their safety systems
- Robust implementation of safety systems is a competitive advantage for companies for safely operating their processes

Thank you for your attention!

Dr. Tekin Kunt
PSRG Director, EMEA
Email: ***tkunt@psrg.com***

Process Safety and Reliability Group

800 W. Sam Houston Pkwy. South
Suite 107
Houston, Texas 77042-1908
Tel: 713-532-8800 800-250-8511 Fax: 713-532-8850
Email: psrghouston@psrg.com Web: www.psrg.com