KENEXIS

DESIGNED FOR SAFETY, SECURITY, & RELIABILITY

Layer of Protection Analysis (LOPA) Participant Training

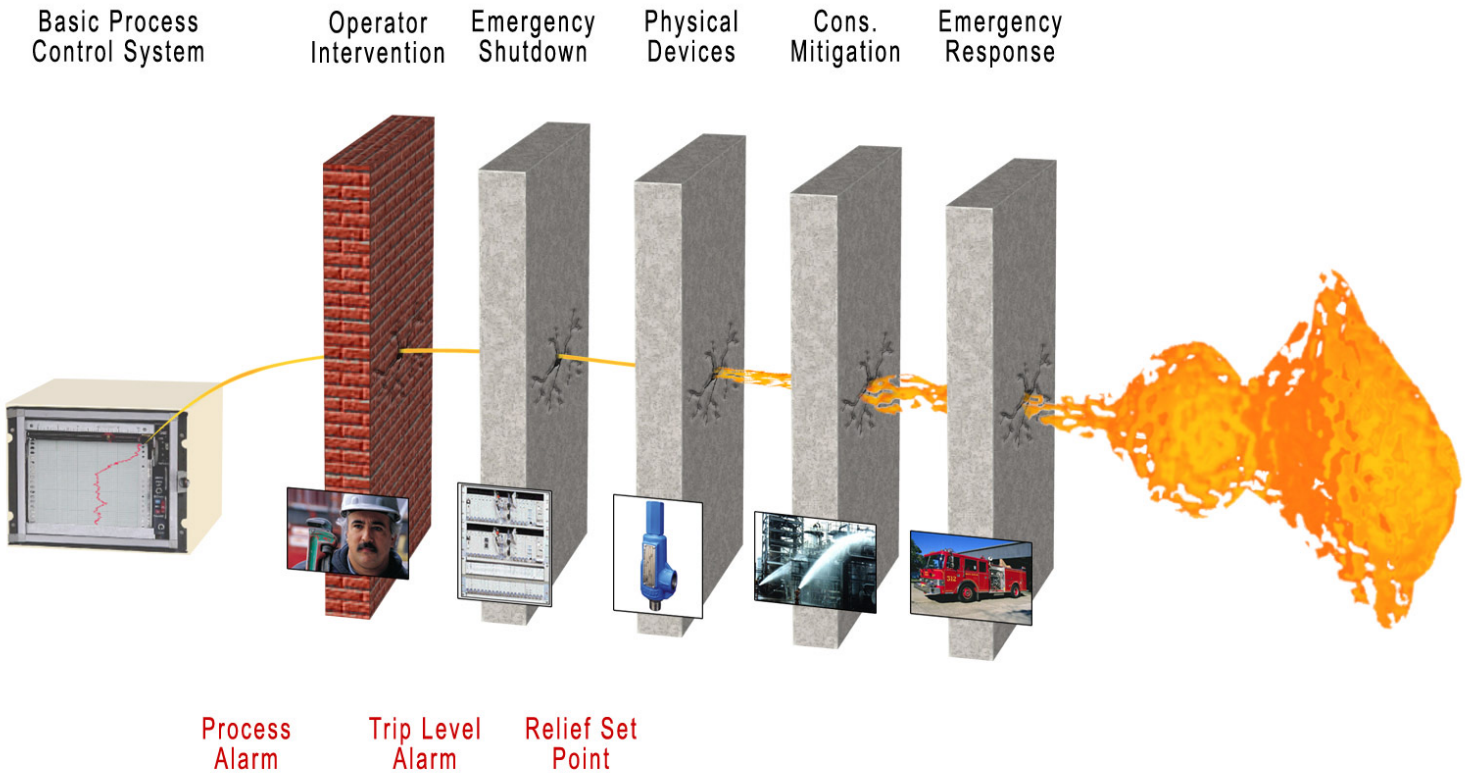
Objectives

- To understand the safety instrumented system lifecycle
- To understand how hazards are assessed in order to ensure tolerable risk is achieved
- To understand the concept of an independent protection layer
- To understand how required risk reduction is determined and allocated to independent protection layers

Course Roadmap

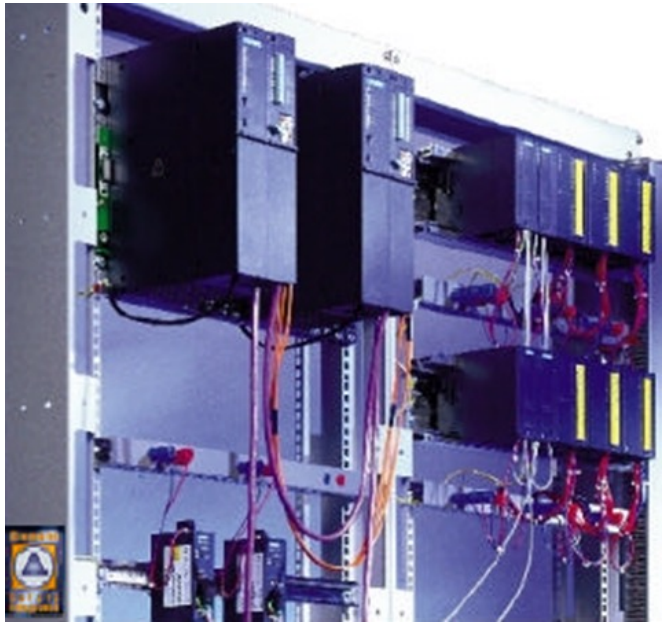
- Overview of Safety Instrumented Systems
- Relevant Regulations and Standards
- Safety Integrity Levels and LOPA
- LOPA Overview
- Initiating Events
- Independent Protection Layers
- Calculating Results
- Example LOPA

Layer of Protection Analysis Overview

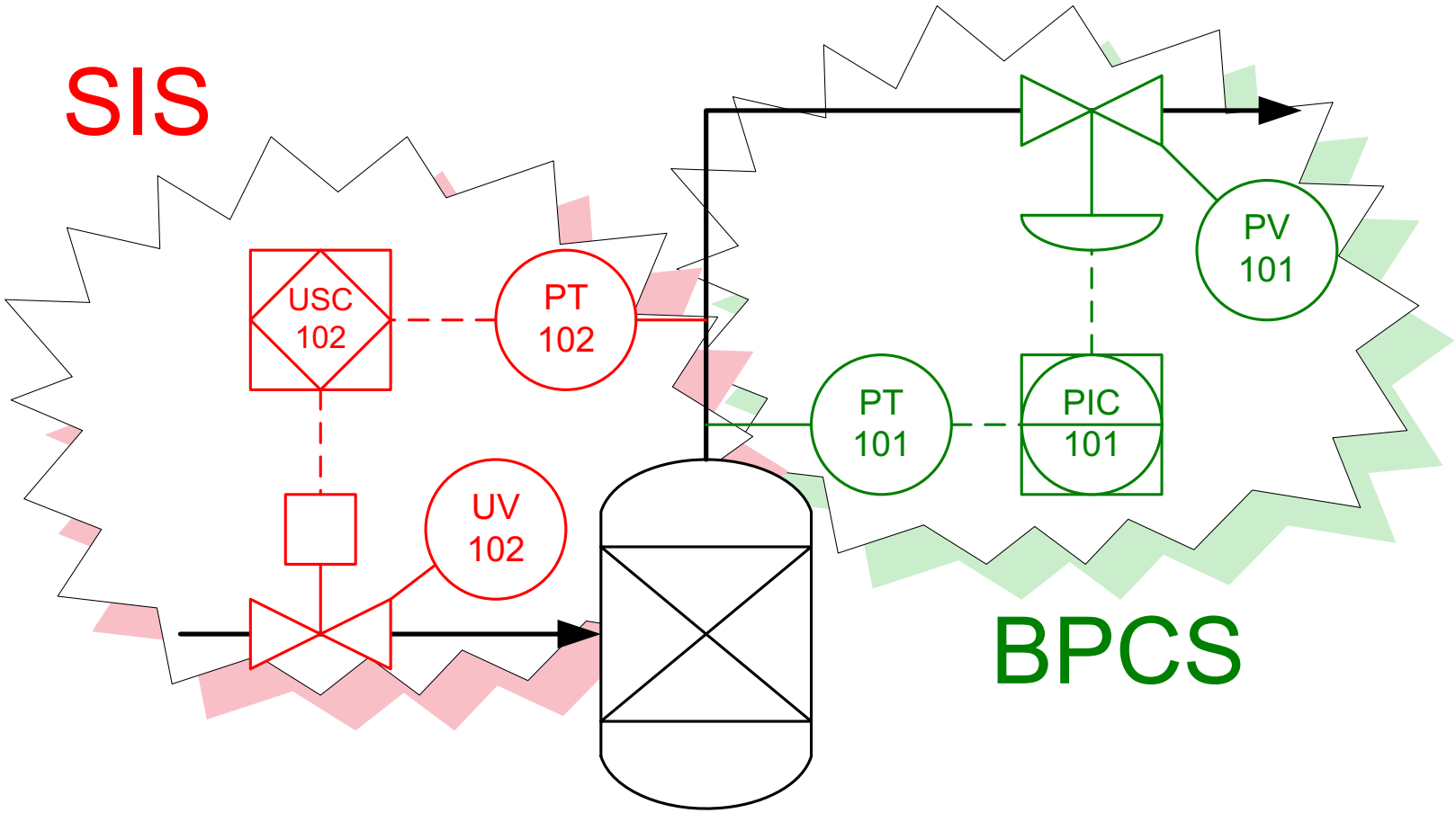


Safety Instrumented Systems

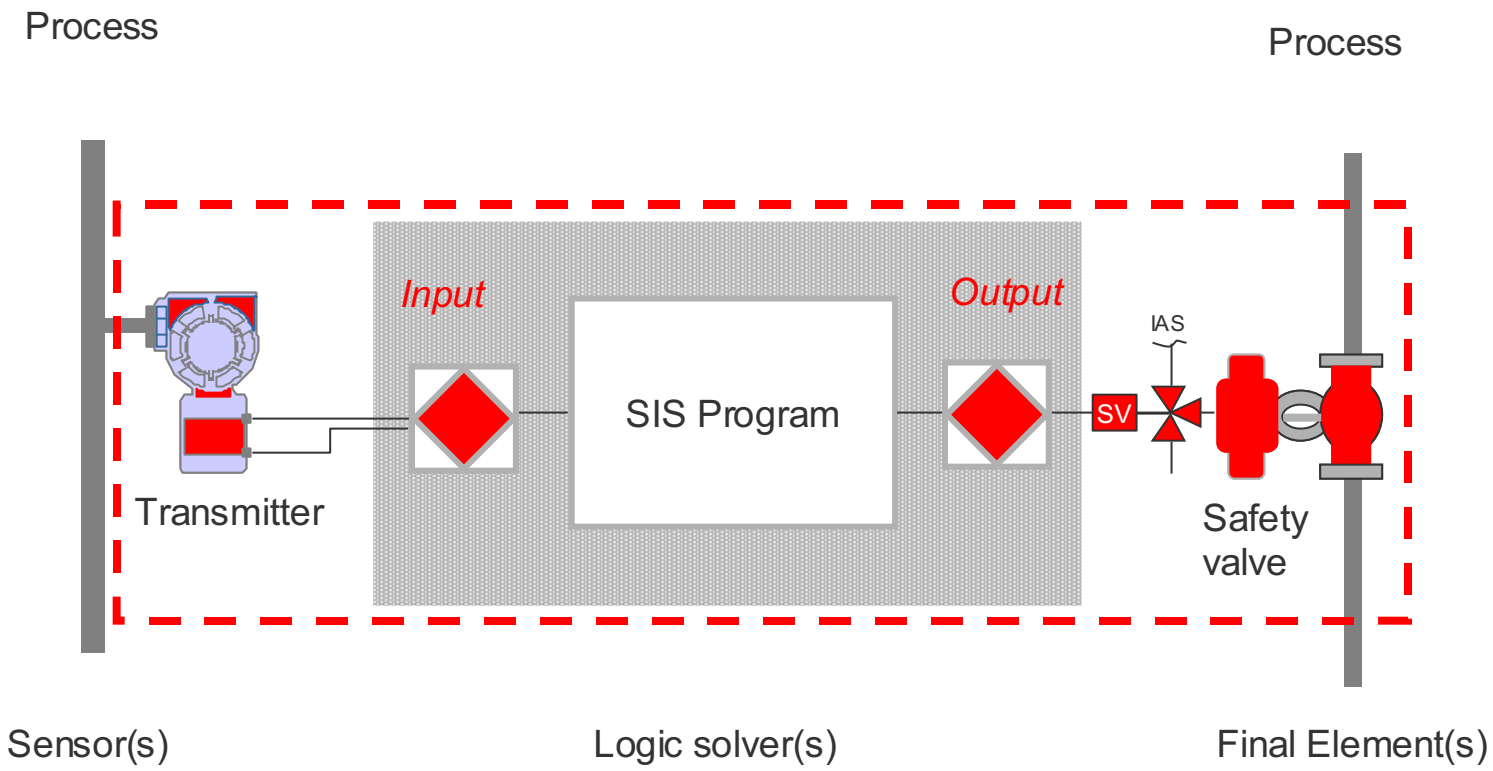
- Informal Definition
  - Instrumented Control System that detects “out of control” conditions and automatically returns the process to a safe state
- “Last Line of Defense”
  - Not basic process control system (BPCS)



Difference Between SIS and BPCS



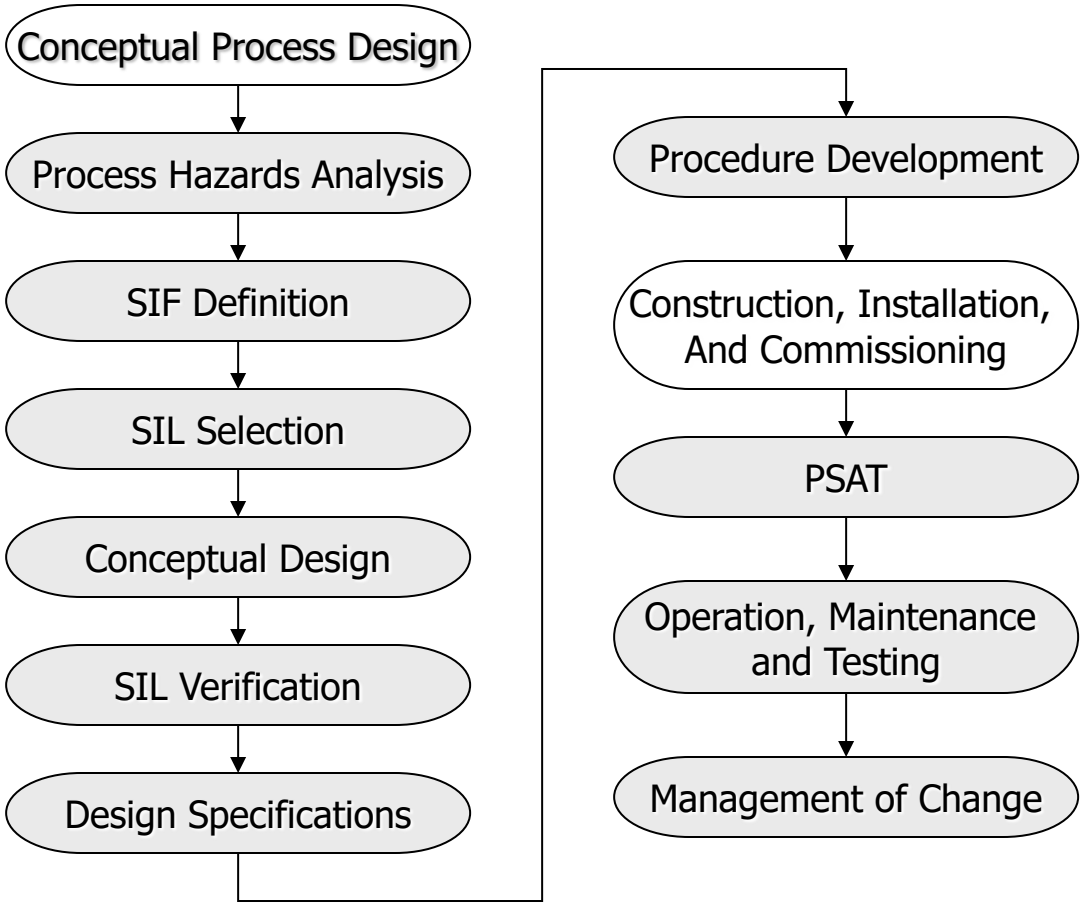
SIS Components



Industry Standards (US)

- OSHA 1910.119 – Process Safety Management Rule
  - Requires Process Hazards Analysis
  - Requires Mechanical Integrity of Engineered Safeguards
- International Electrotechnical Commission (IEC), IEC 61511 (ANSI/ISA 61511 in the US), Functional Safety: Safety Instrumented Systems for the Process Sector
  - Defines safety lifecycle
  - Defines “allocation” of required risk reduction

The Safety Lifecycle

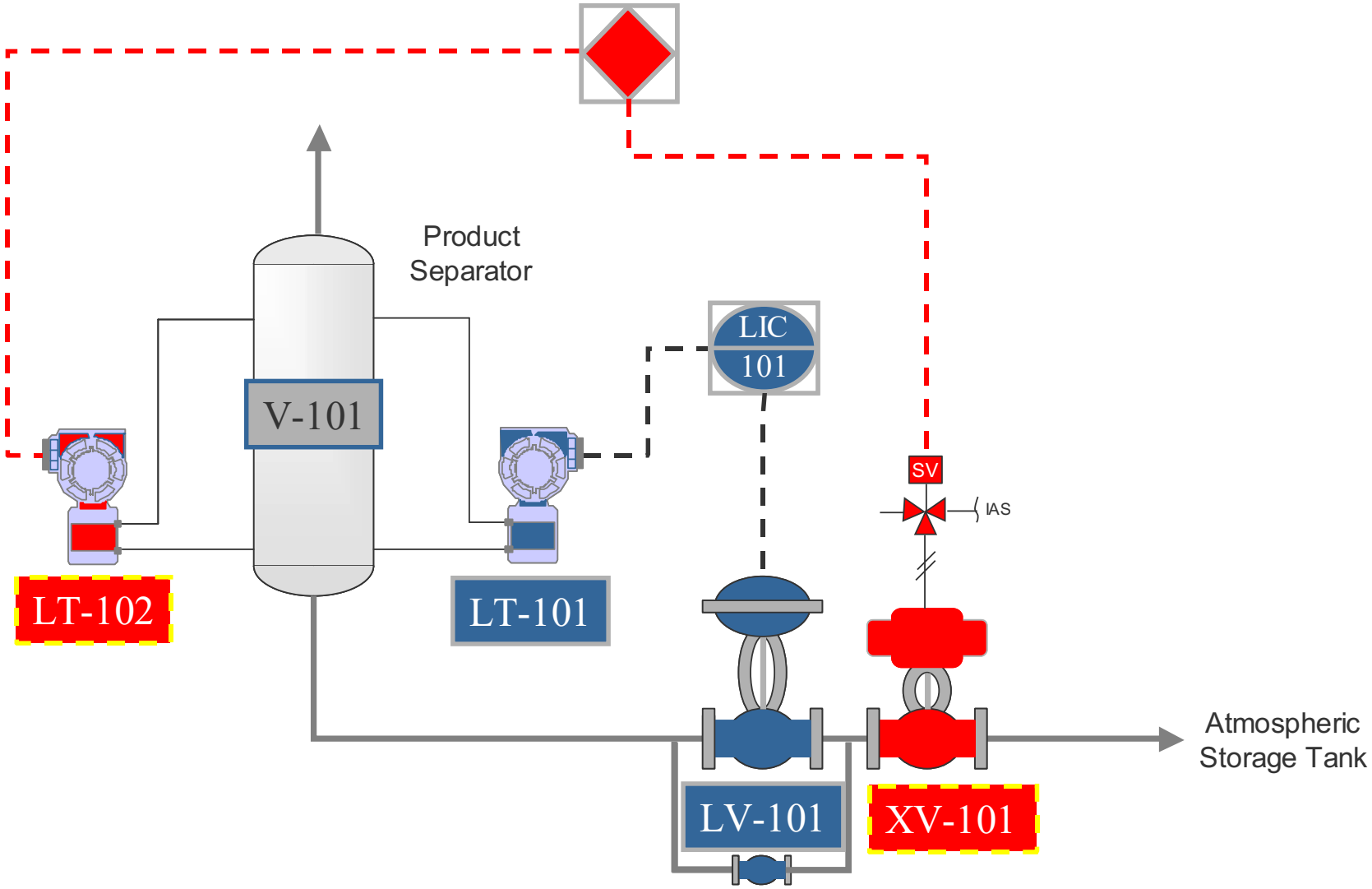


Safety Integrity Level

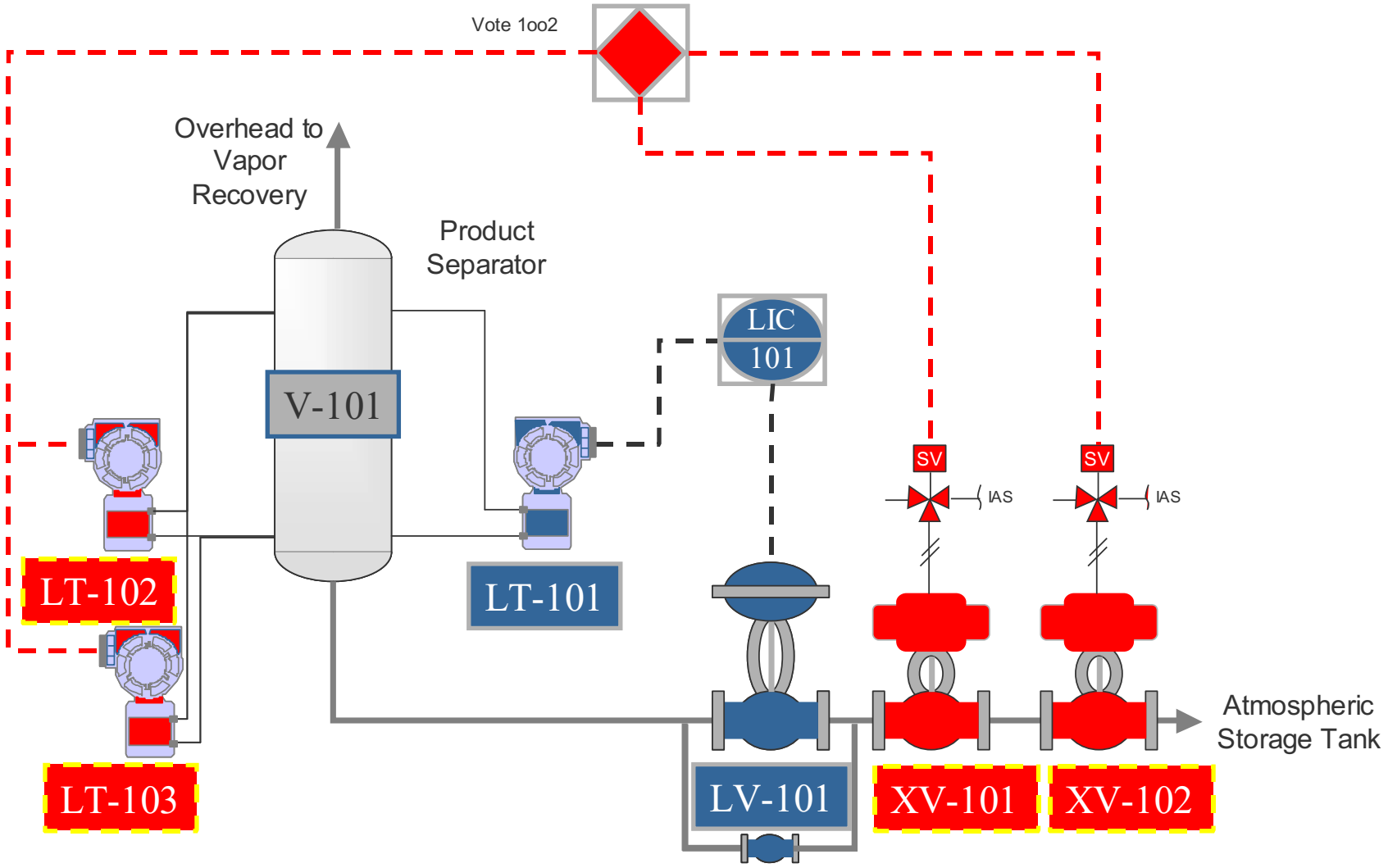
A measure of the amount of risk reduction provided by a Safety Instrumented Function (SIF)

Safety Integrity Level	Safety	Probability of Failure on Demand	Risk Reduction Factor
SIL 4	> 99.99%	0.001% to 0.01%	100,000 to 10,000
SIL 3	99.9% to 99.99%	0.01% to 0.1%	10,000 to 1,000
SIL 2	99% to 99.9%	0.1% to 1%	1,000 to 100
SIL 1	90% to 99%	1% to 10%	100 to 10

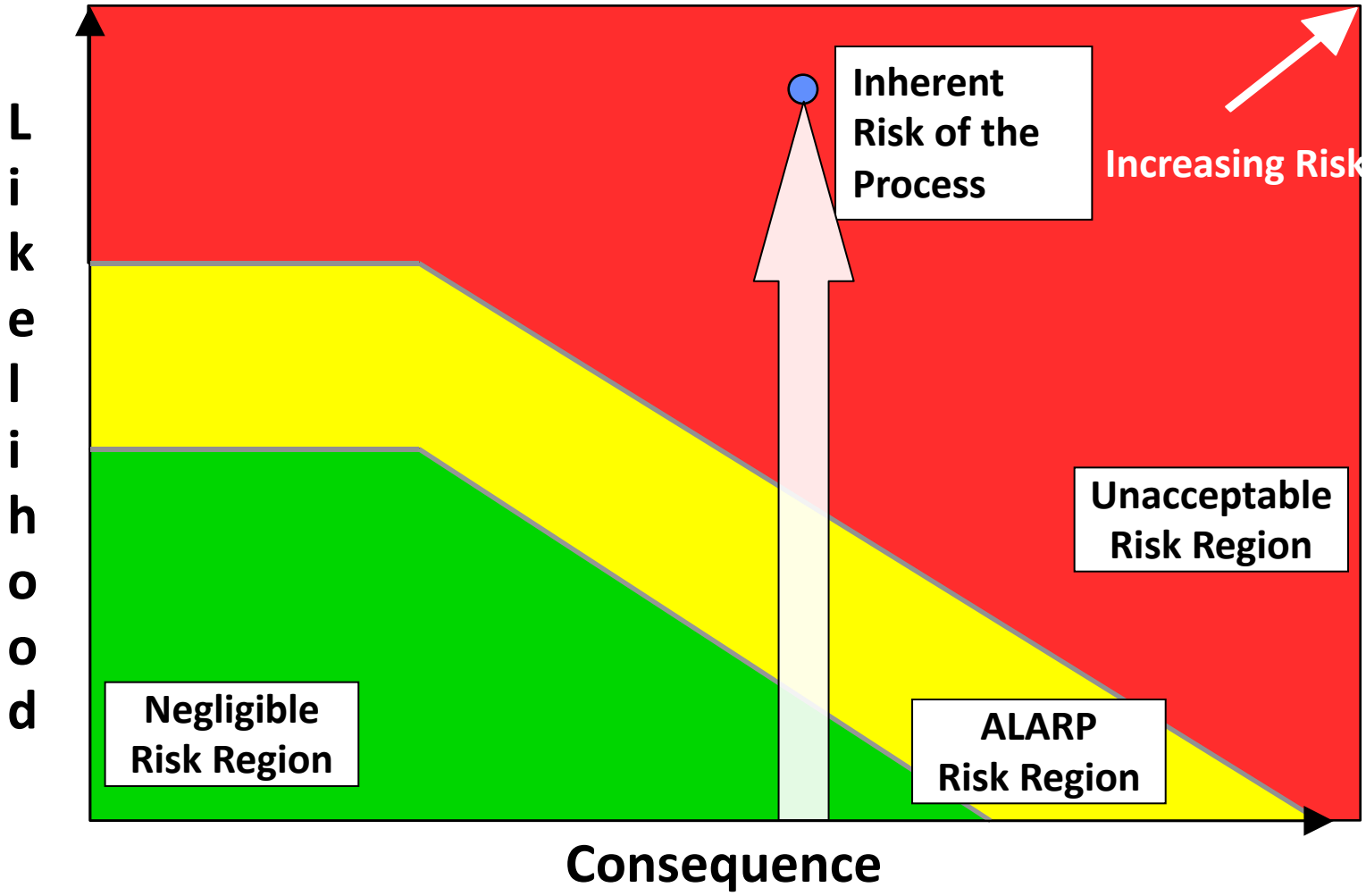
Typical SIL 1 Design



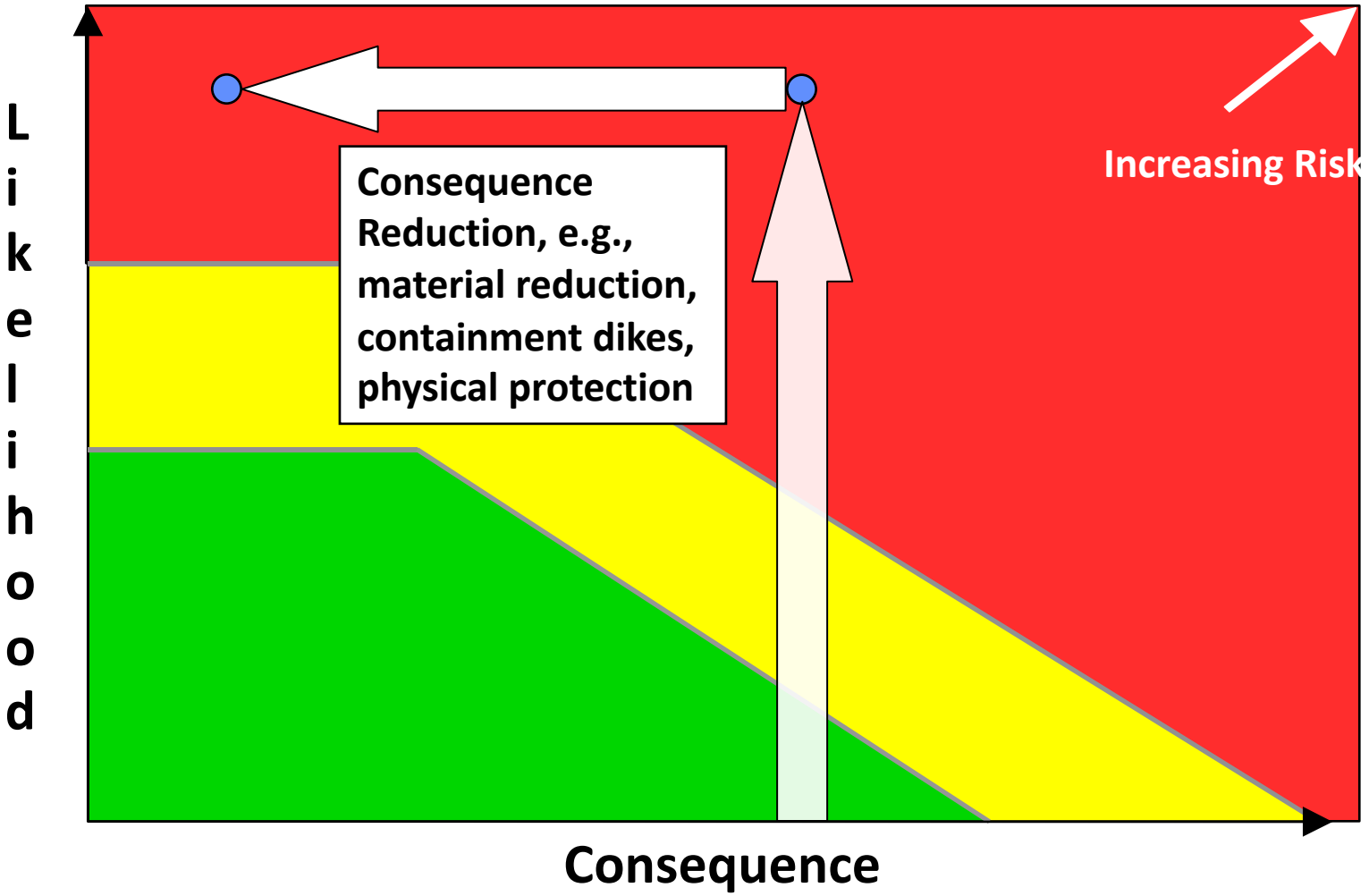
Typical SIL 2 Design



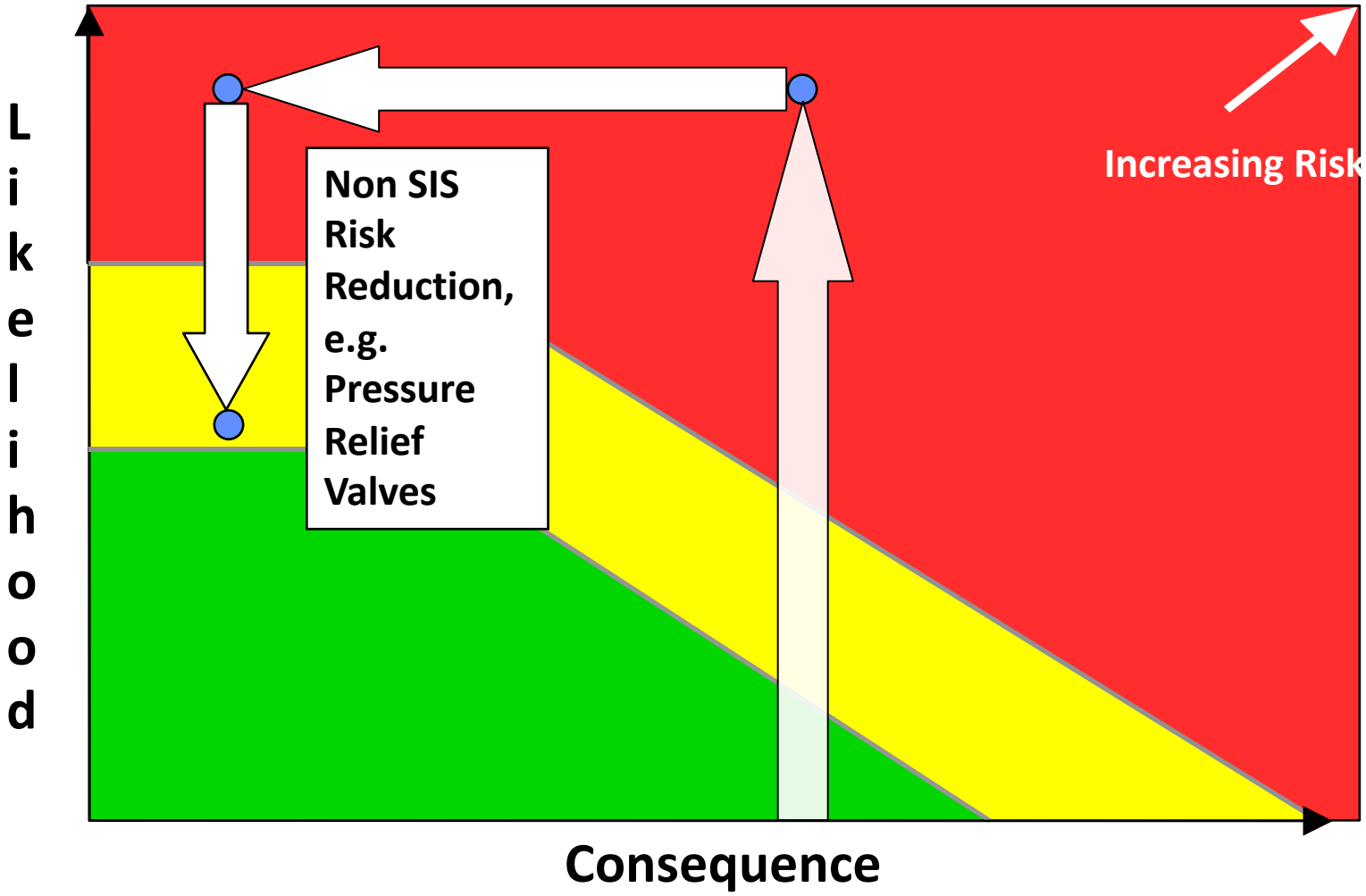
Risk Reduction Process – Inherent Risk



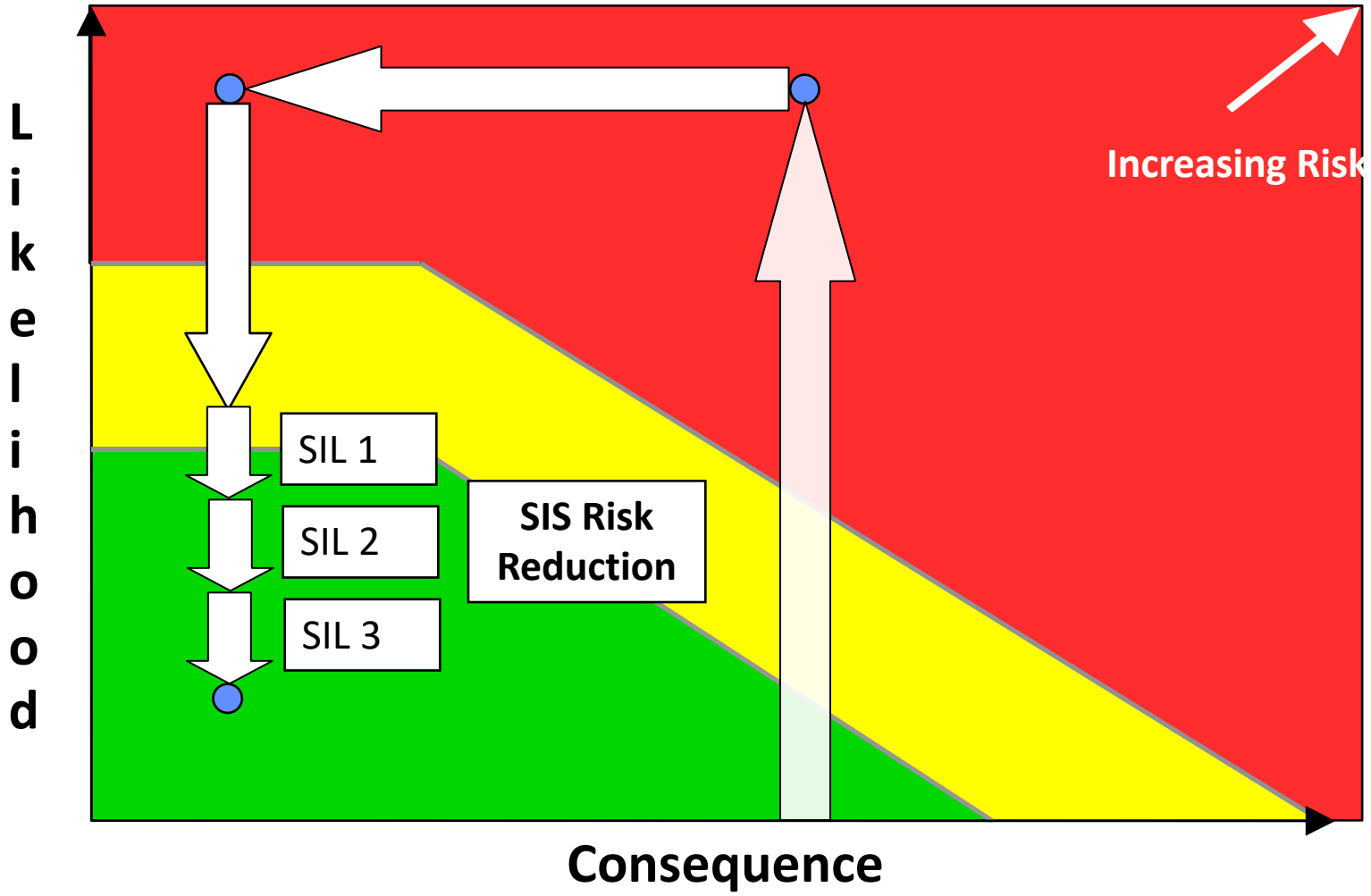
Risk Reduction – Consequence Reduction



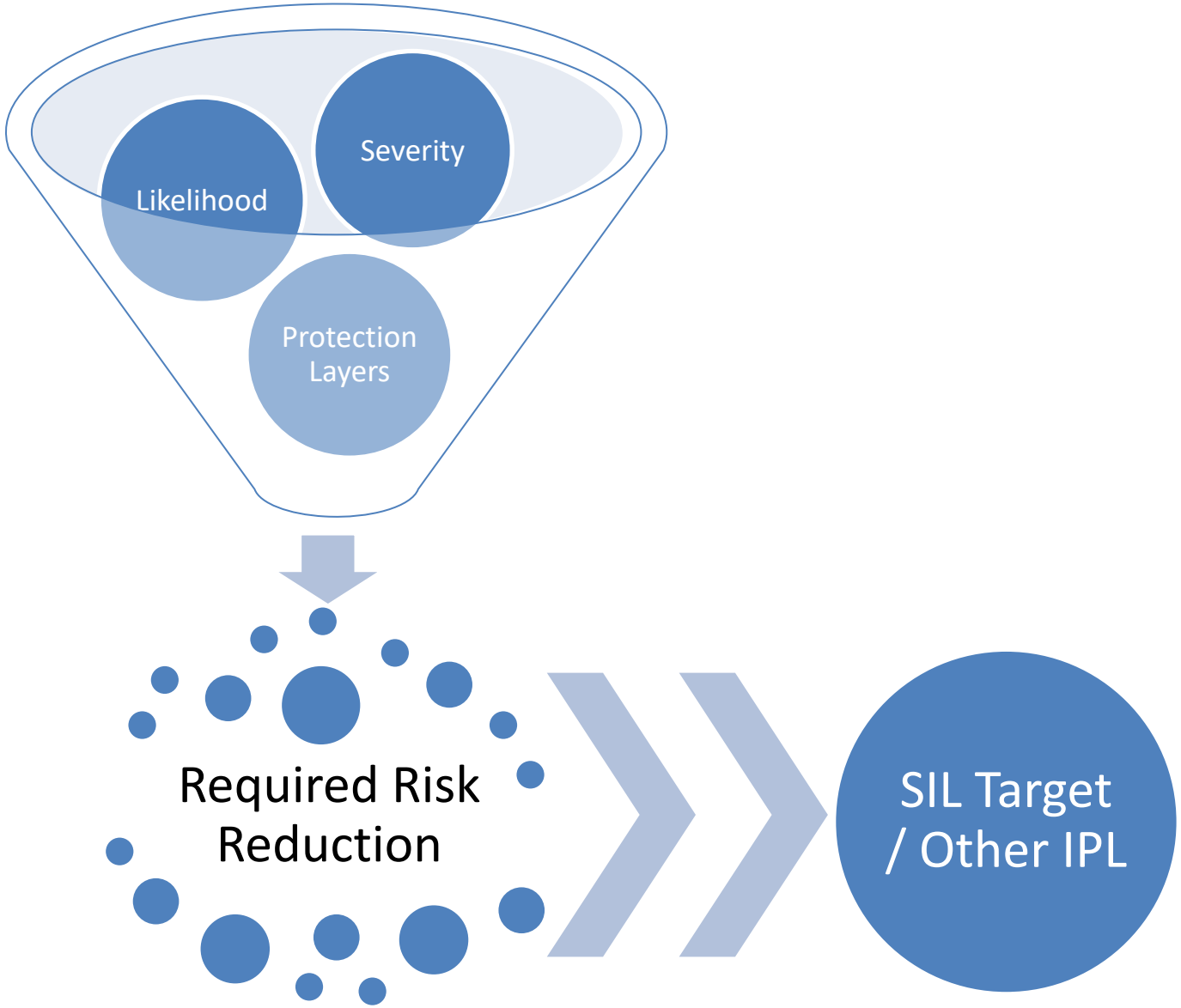
Non-SIS Likelihood Reduction



SIS Risk Reduction

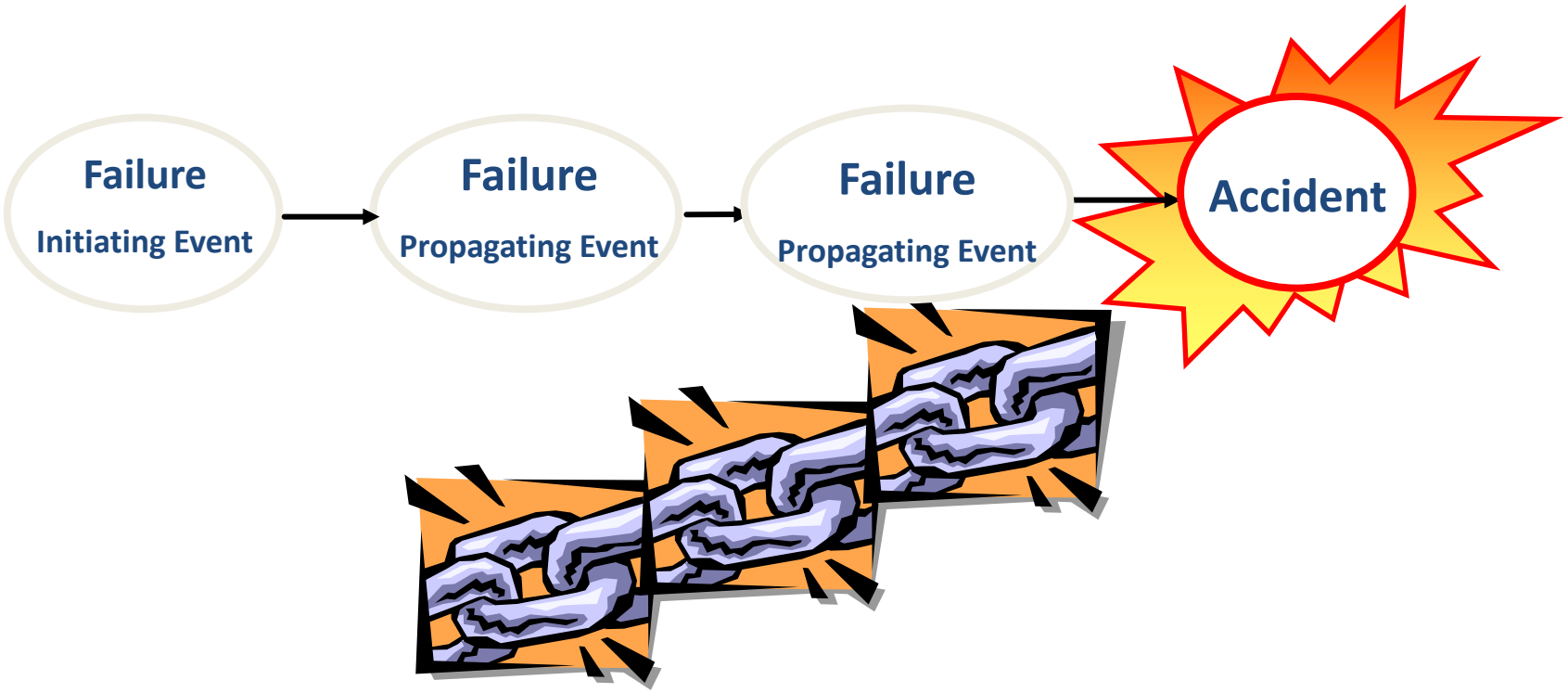


Layer of Protection Analysis



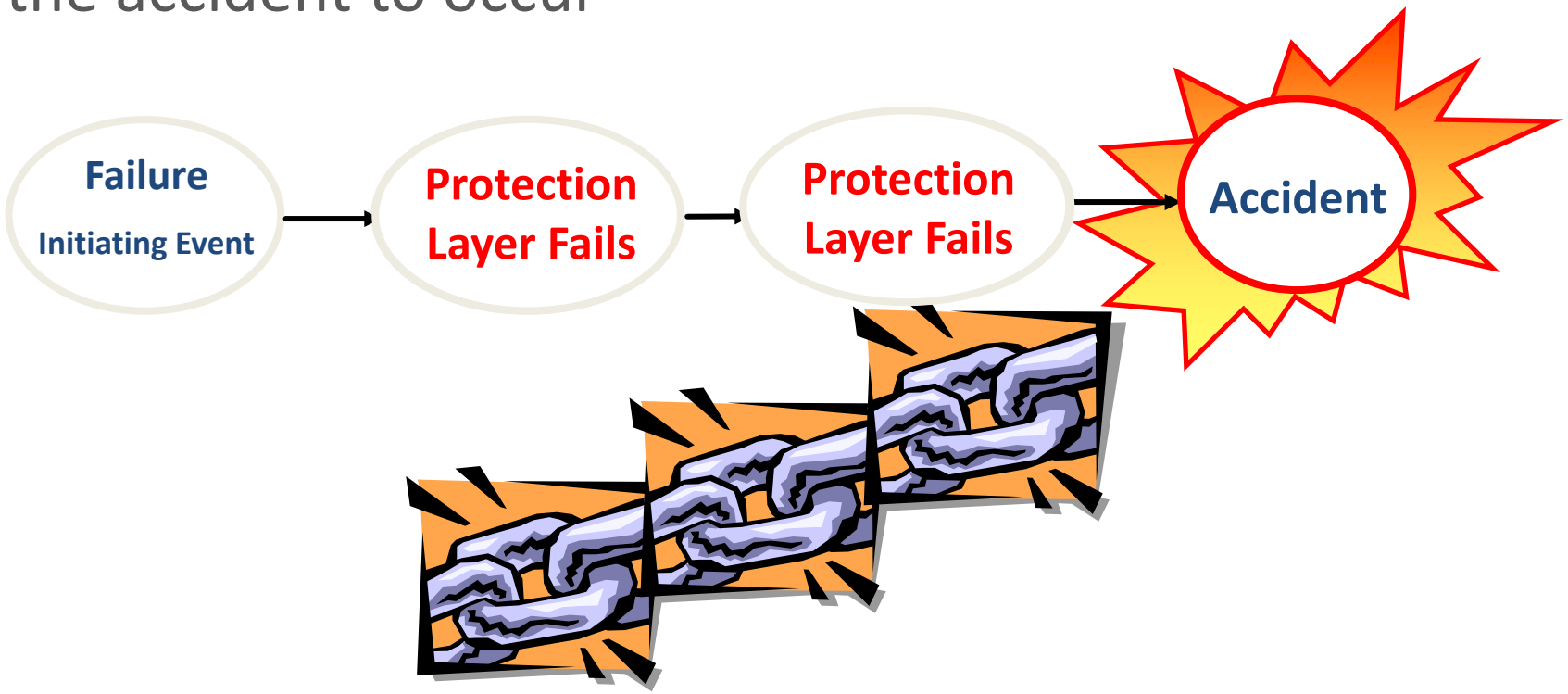
Accident Causation Model

- Assumption #1: Most major accidents happen because multiple failures occur; starting with an *initiating event*

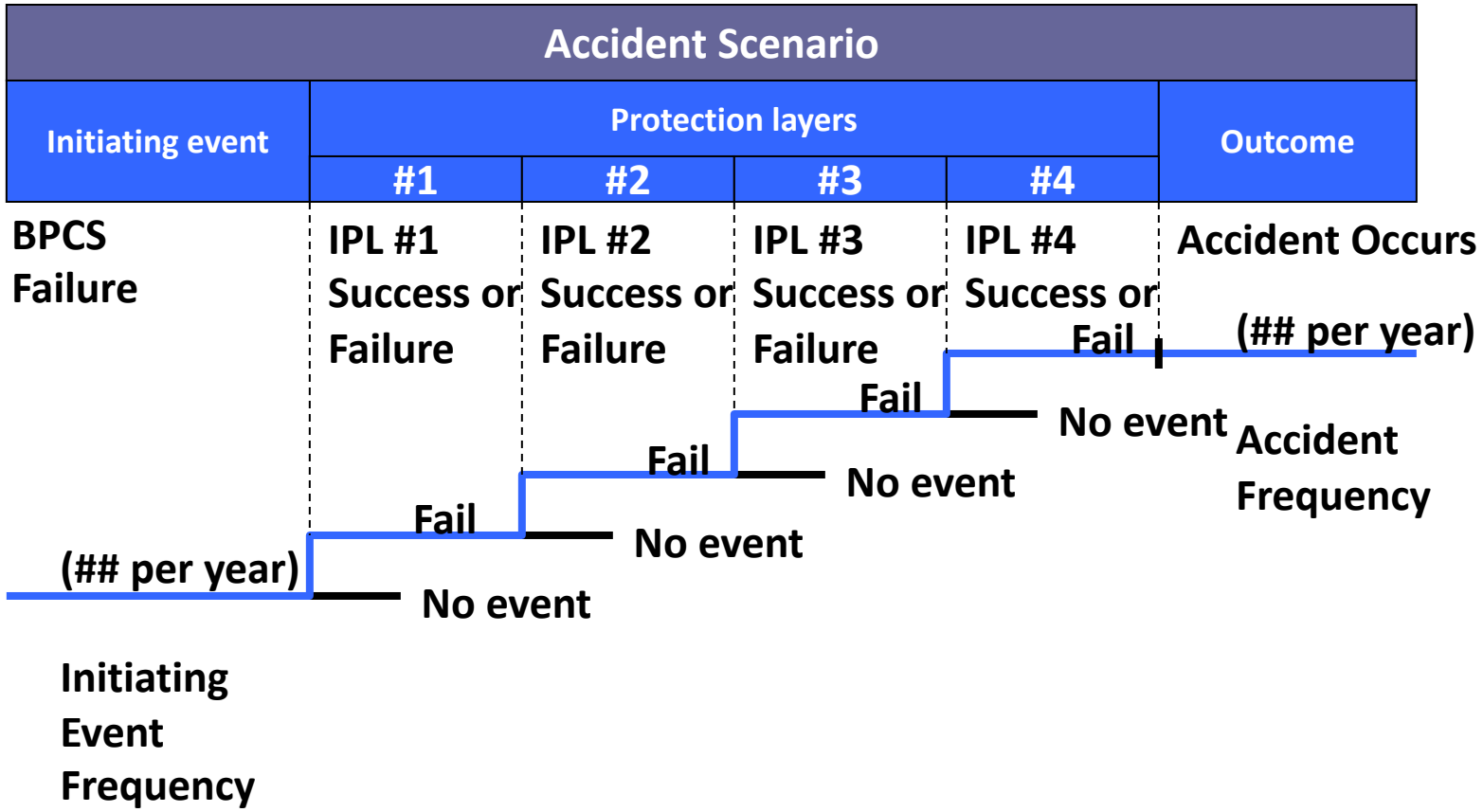


Accident Causation Model with IPL

- Assumption #2: If an Independent Protection Layer (IPL) functions as intended when an initiating event occurs no accident with result; All IPLs must fail for the accident to occur

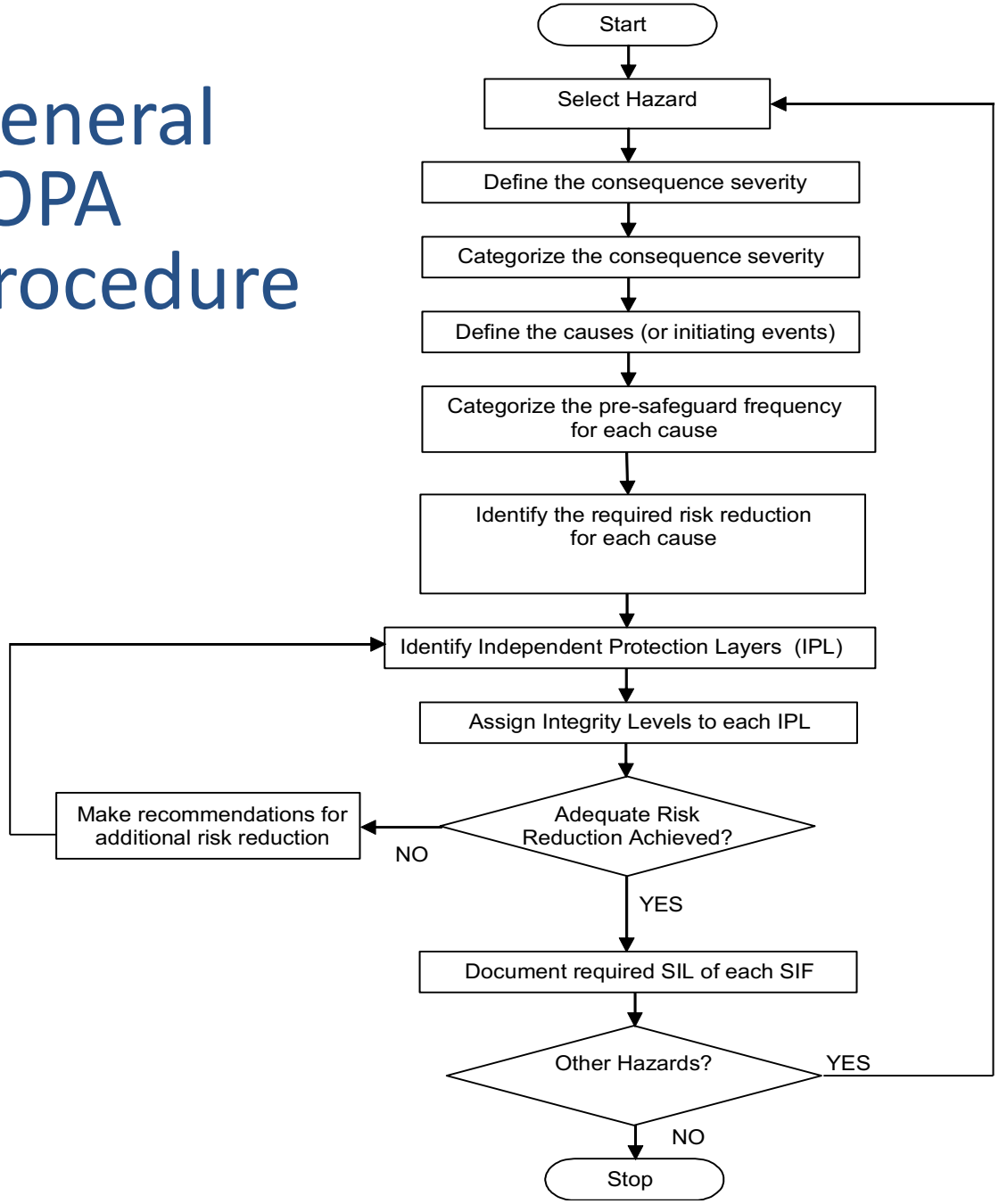


LOPA Math – “Simplified Event Tree”



Logical ‘AND’
Probability Multiplication

General LOPA Procedure



Risk Tolerance Guidelines - Explicit

Code	Category	Description	TMEL
5	Very High	Multiple Fatalities	1E-6
4	High	Single Fatality	1E-5
3	Moderate	Severe Injury (Extended Hospitalization, Dismemberment)	1E-4
2	Low	Lost Time Injury Not Requiring Extended Hospitalization	1E-3
1	Very Low	Minory Injury – First Aid	1E-2
0	None	No significant safety consequences	N/A

TMEL – Target Maximum Event Likelihood

Risk Tolerance Guidelines - Implicit

5	0	3	4	5	6	7
4	0	2	3	4	5	6
3	0	1	2	3	4	5
2	0	0	1	2	3	4
1	0	0	0	1	2	3
Sev / Freq	0	1	2	3	4	5

Code	Category	Description
5	Very High	Multiple Fatalities
4	High	Single Fatality
3	Moderate	Severe Injury
2	Low	Lost Time Injury
1	Very Low	Minory Injury – First Aid
0	None	No significant safety consequences

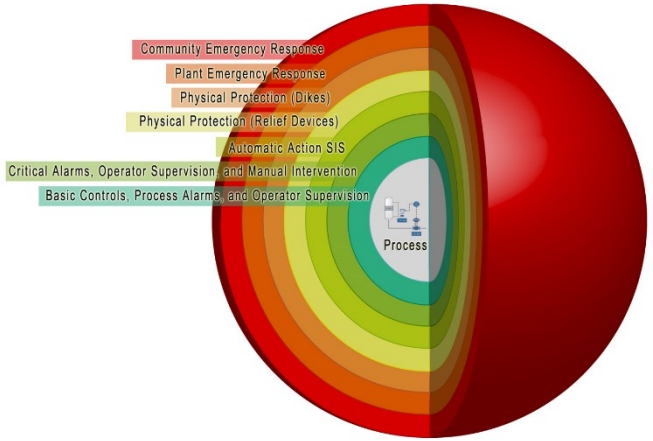
Code	Likelihood	Period
5	Very Frequent	0.1 years
4	Frequent	1 year
3	Occasional	10 years
2	Unlikely	100 years
1	Very Unlikely	1,000 years
0	None	N/A

Initiating Events - Typical

Initiating Event	Recurrance	Frequency
Basic Process Control Loop Failure	1/10 year	10^{-1}
Human Error (once per month opportunity)	1/10 year	10^{-1}
Human Error (one per day opportunity)	1 / year	1
Pump Failure	1/10 year	10^{-1}
Compressor Failure	1/10 year	10^{-1}
Other Initiating Events – Develop Using Experience of Team		

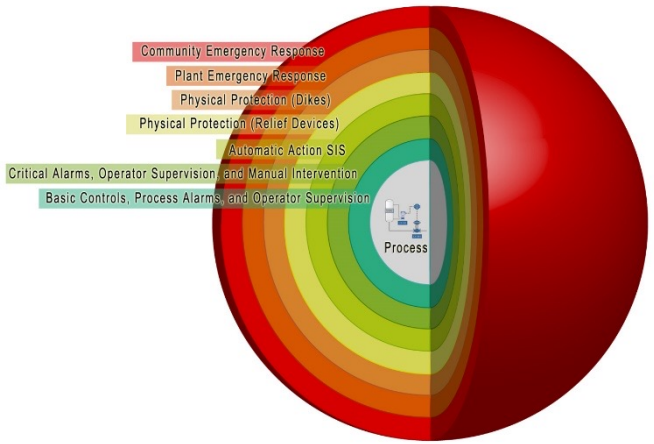
IPL Requirements

- Independent Protection Layers (IPL) are limited to safeguards have the following characteristics
  - Specificity
    - Specifically designed to prevent the Hazard Identified
  - Independence
    - From cause (initiating event) and other IPL
  - Dependability
    - Each provides at least one order of magnitude of risk reduction
  - Auditability
    - Can be tracked



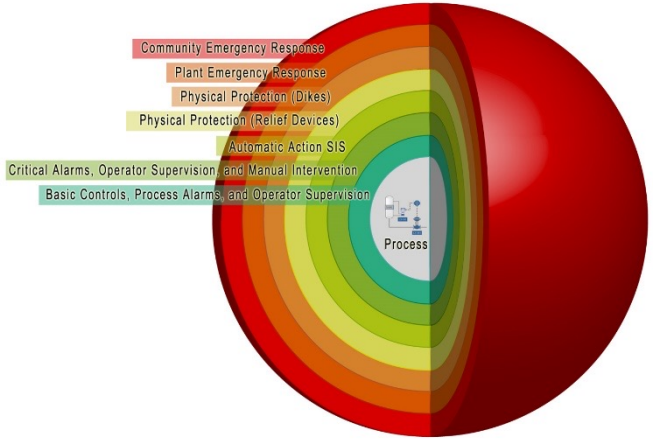
Typical IPL Usage Rules

- IPLs don’t prevent initiating events from occurring
- IPLs do function once the initiating event has already occurred
- If a BPCS control loop failure was the initiating event, don’t use equipment from a failed BPCS loop to justify IPL credit
- Don’t use training or preventive maintenance as an IPL
- Don’t take credit for the operator more than once
- Don’t identify the SIS for more than one IPL



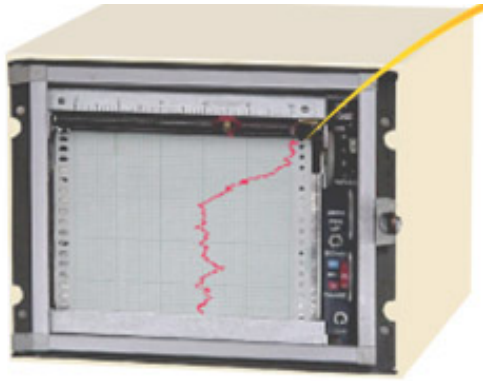
Commonly Used IPLs – Operator Intervention

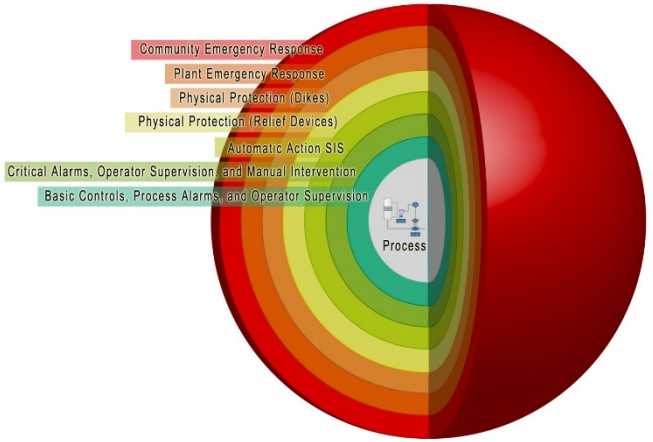
- Operator Intervention
  - Based on annunciated alarm, not just an indication
  - Continuously manned alarm location
  - Procedures and training for proper alarm response
  - Adequate response time available (~20 minutes) before hazardous condition results



Commonly Used IPL – Basic Process Control

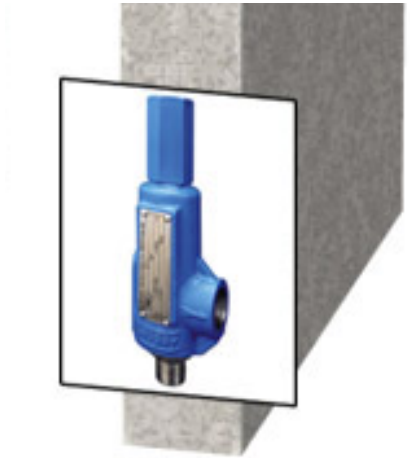
- Basic Process Control System Response
  - Continuous Control or BPCS Interlock that is independent from the initiating event
  - Completely mitigates the hazard
  - Run in automatic mode during all operational phases where a hazard could occur

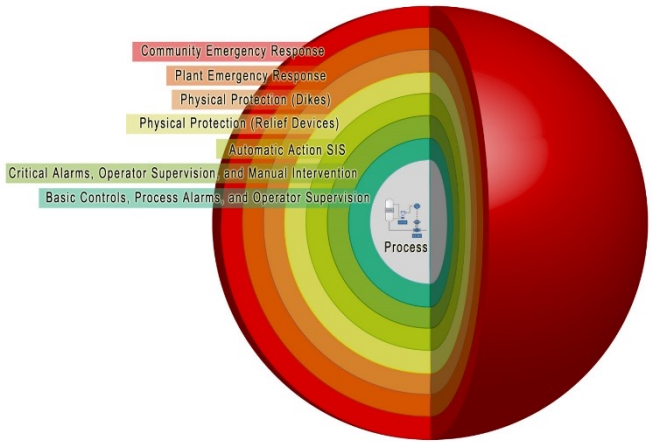




Commonly Used IPLs – Pressure Relief

- Emergency Pressure Relief System
  - Adequately sized for the identified hazard scenario
  - Subject to mechanical integrity program (i.e., tested)
  - Proven to be reliable in service based on inspection history





Credit for Layers of Protection

IPL Type	Implicit IPL Credits	Explicit IPL PFD	Explicit IPL RRF
BPCS Control Loop	1	0.1	10
Operator Response to Alarm	1	0.1	10
Relief Valve (spring loaded, clean service)	2	0.01	100
Rupture Disk (clean service)	2	0.01	100
Check Valves (dual, clean service)	1	0.1	10
SIL 1 – Safety Instrumented Function	1	0.1	10
SIL 2 – Safety Instrumented Function	2	0.01	100
SIL 3 – Safety Instrumented Function	3	0.001	1,000

PFD = Probability of Failure on Demand
RRF = Risk Reduction Factor (1/PFD)

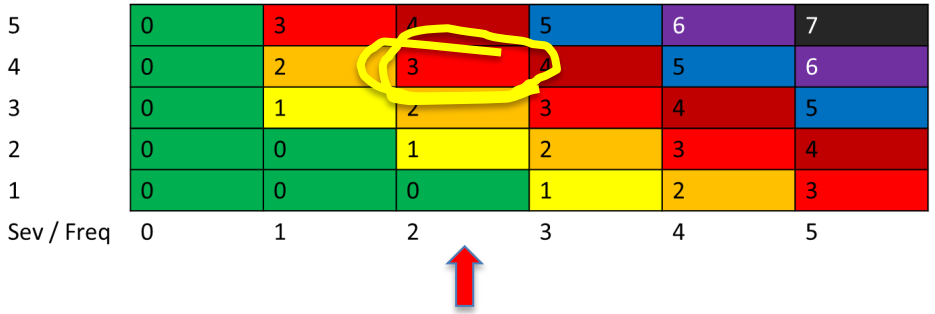
Calculating Risk Reduction – Implicit

Team Determines Consequence Category and Likelihood Category

Code	Category	Description
5	Very High	Multiple Fatalities
4	High	Single Fatality
3	Moderate	Sever Injury
2	Low	Lost Time Injury
1	Very Low	Minory Injury – First Aid
0	None	No significant safety consequences

Code	Likelihood	Period
5	Very Frequent	0.1 years
4	Frequent	1 year
3	Occasional	10 years
2	Unlikely	100 years
1	Very Unlikely	1,000 years
0	None	N/A

Use Matrix to Determine Necessary Risk Reduction



Subtract "Credits for IPL"

IPLs:		
	Check Valves	1 Credit
	Operator	1 Credit
	Total	2 Credits

Required Risk Reduction to be Allocated

3 IPL Required (from Table) – 2 IPL Existing = 1 IPL Shortfall to be Allocated

Calculating Risk Reduction - Explicit

Team Determines Consequence Category and Associated TMEL

Code	Category	Description	TMEL
5	Very High	Multiple Fatalities	1E-6
4	High	Single Fatality	1E-5
3	Moderate	Sever Injury (Extended Hospitalization, Dismemberment)	1E-4
2	Low	Lost Time Injury Not Requiring Extended Hospitalization	1E-3
1	Very Low	Minory Injury – First Aid	1E-2
0	None	No significant safety consequences	N/A

Team Identifies Initiating Event(s) and IPLs – Multiplies Frequencies and probabilities to Determine Intermediate Event Likelihood

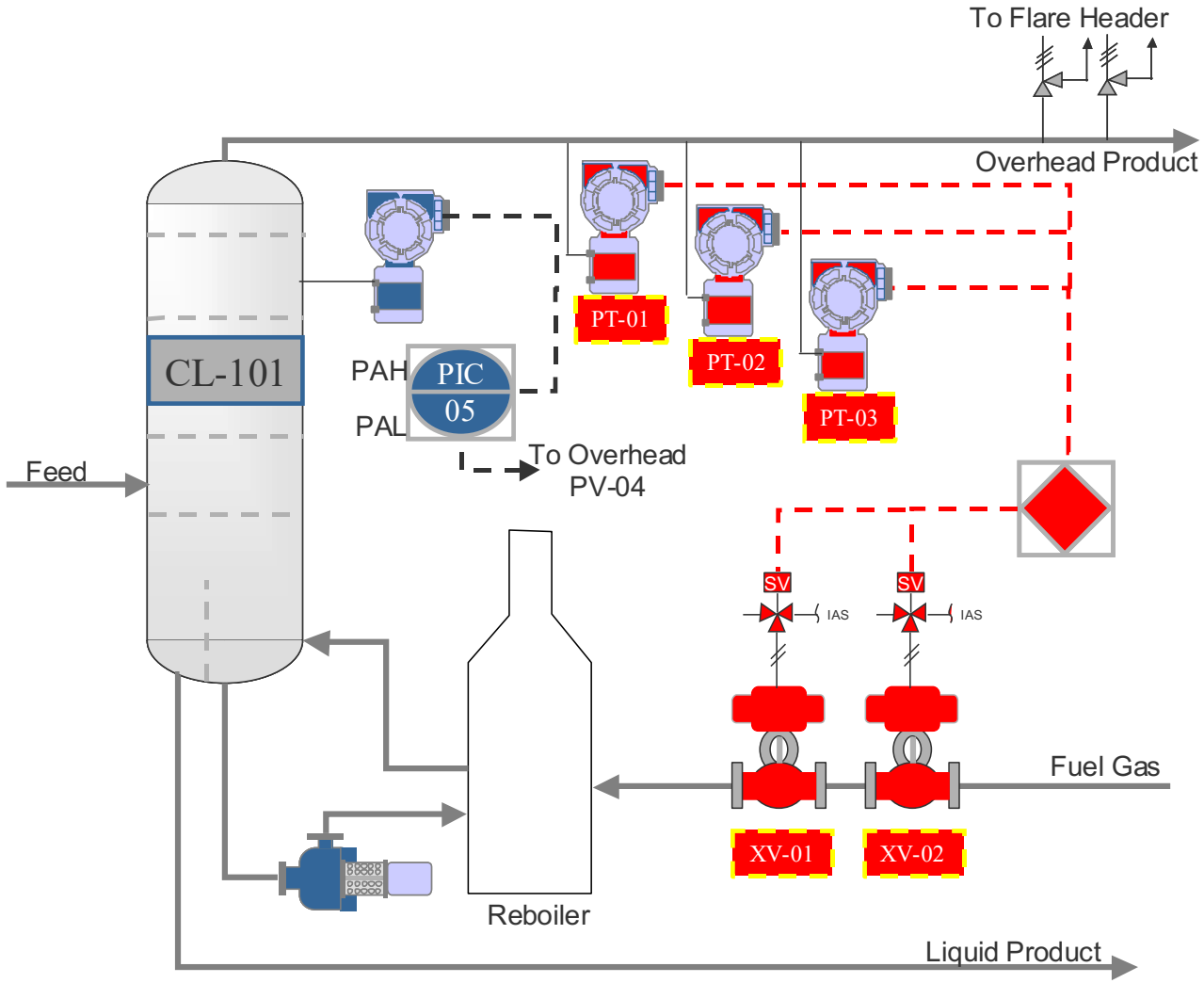
Init Evt:	BPCS Fails	0.1 /year
IPLs:	Operator	0.1
	Check Valve	0.1
Int. Evt. Likelihood		1.0E-3

Require Risk Reduction is: Intermediate Event Likelihood / TMEL

Int. Evt. Likelihood	1.0E-3
TMEL	1.0E-4

Required Risk Reduction 10

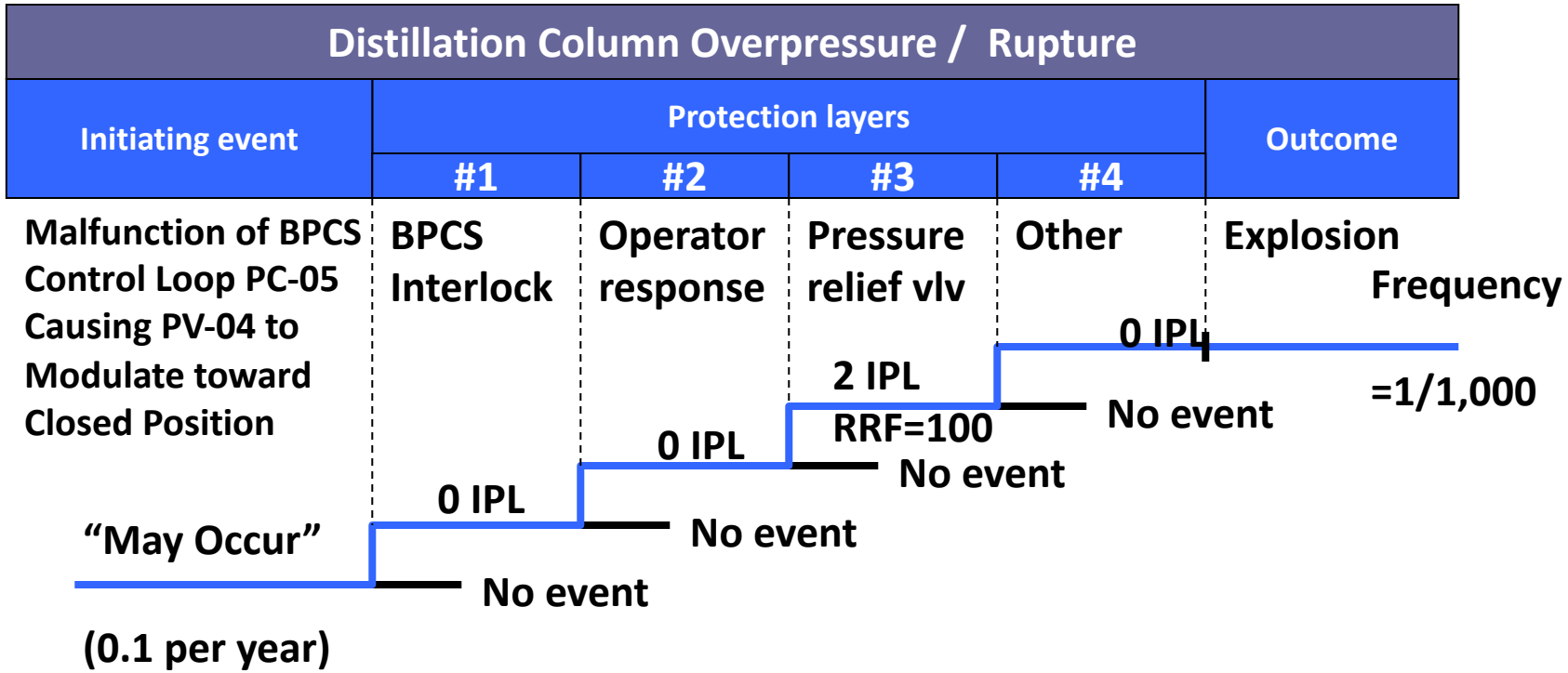
LOPA Example – Distillation Column



Proposed Safety Instrumented Function

ID	Description	Inputs	Outputs	Req. SIL	Notes
SIF -01	High-High Pressure in Column CL-101 causes shutoff of Reboiler H-100 to remove heat input to column	PT-01 PT-02 PT-03 (2oo3)	XV-01 Close XV-02 Close (1oo2)		

Example LOPA Event Tree



Example LOPA Required Risk Reduction

Code	Category	Description	TMEL
5	Very High	Multiple Fatalities	1E-6
4	High	Single Fatality	1E-5
3	Moderate	Sever Injury (Extended Hospitalization, Dismemberment)	1E-4
2	Low	Lost Time Injury Not Requiring Extended Hospitalization	1E-3
1	Very Low	Minory Injury – First Aid	1E-2
0	None	No significant safety consequences	N/A

Require Risk Reduction is:

Intermediate Event Likelihood

TMEL

Int. Evt. Likelihood	1.0E-3
TMEL	1.0E-5
Required Risk Reduction	100

Thank you for attending!

- Lecture portion completed
- Quiz to ensure retention of presented material
- Download and print course completion certificate

KENEXIS

Design for Safety, Security & Reliability

Active Contributors, Instructors, & Authors