Basic Introduction to SIL Assessment using Layers of Protection Analysis (LOPA)

Fayyaz Moazzam
Principal Consultant
PetroRisk Middle East, Abu Dhabi, United Arab Emirates
T. + 97126778792 M. +971561273688 F. +97126778795
fayyaz.moazzam@petrorisk.com
www.petrorisk.com

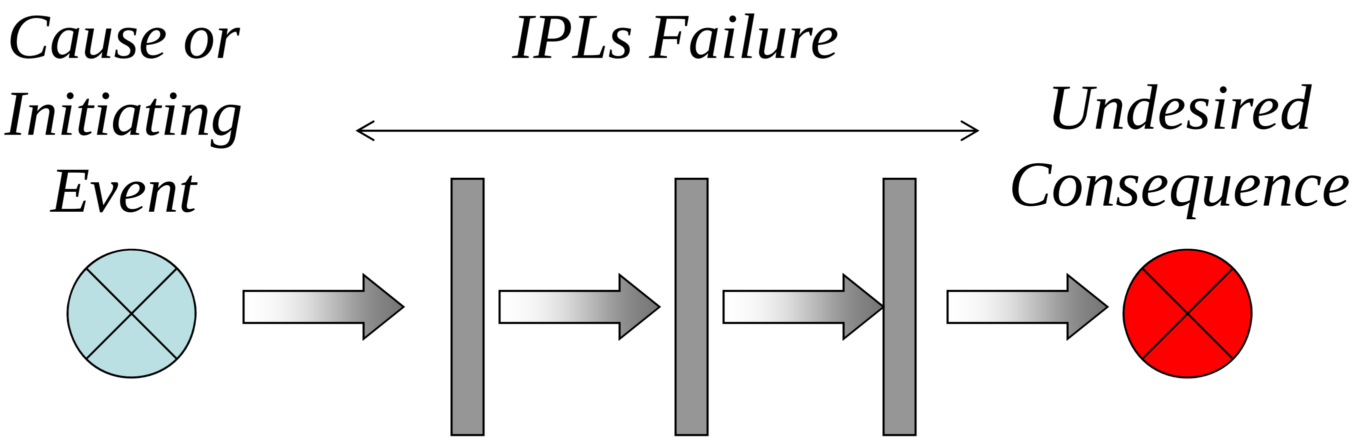
What is LOPA?

- Evaluate risks in ***orders of magnitude*** of selected accident ***scenarios***
- Builds on the information developed in ***qualitative hazard evaluation*** e.g. HAZOP

Main Questions

- LOPA helps to answer the following questions:
  - What's the ***likelihood*** of undesired events / scenarios ?
  - What's the ***risk*** associated with the scenarios?
  - Are there ***sufficient risk mitigation measures***?

Basic Principle



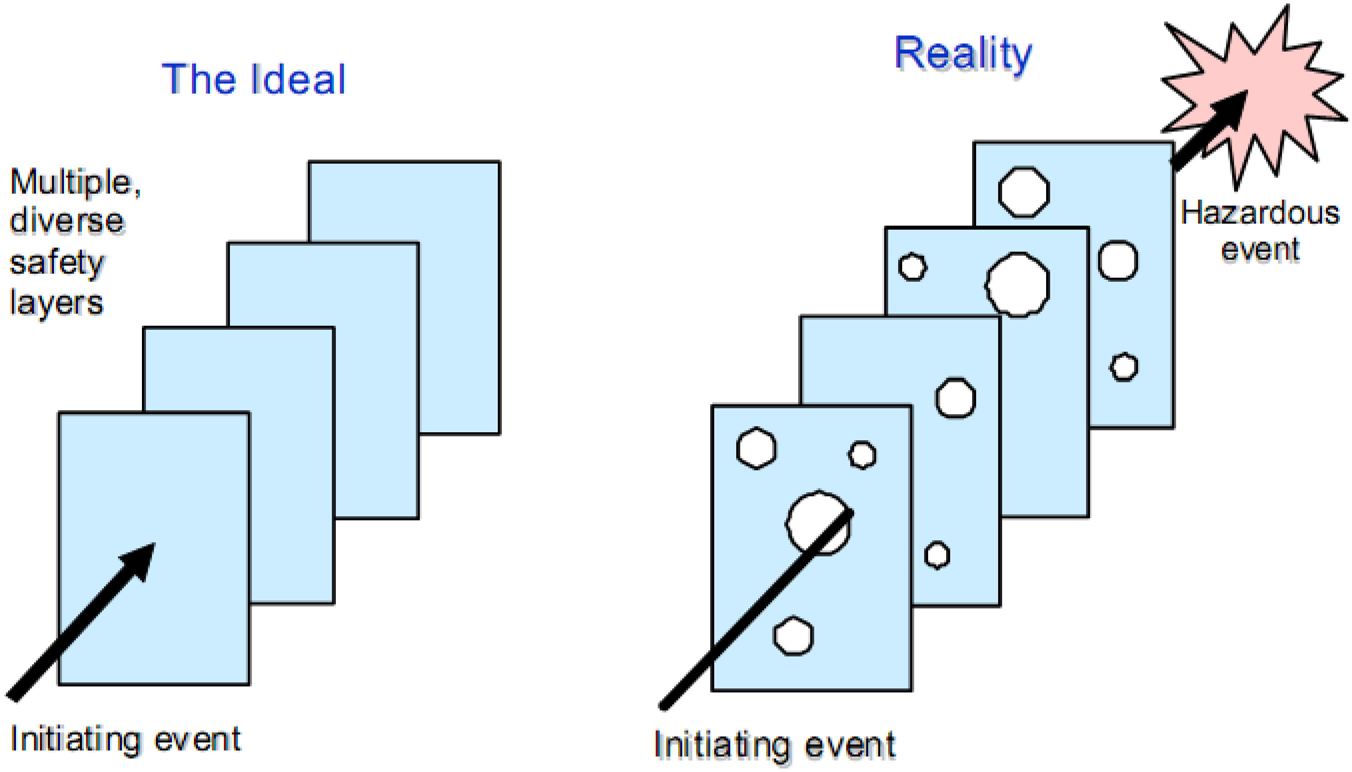
Cause or Initiating Event

IPLs Failure

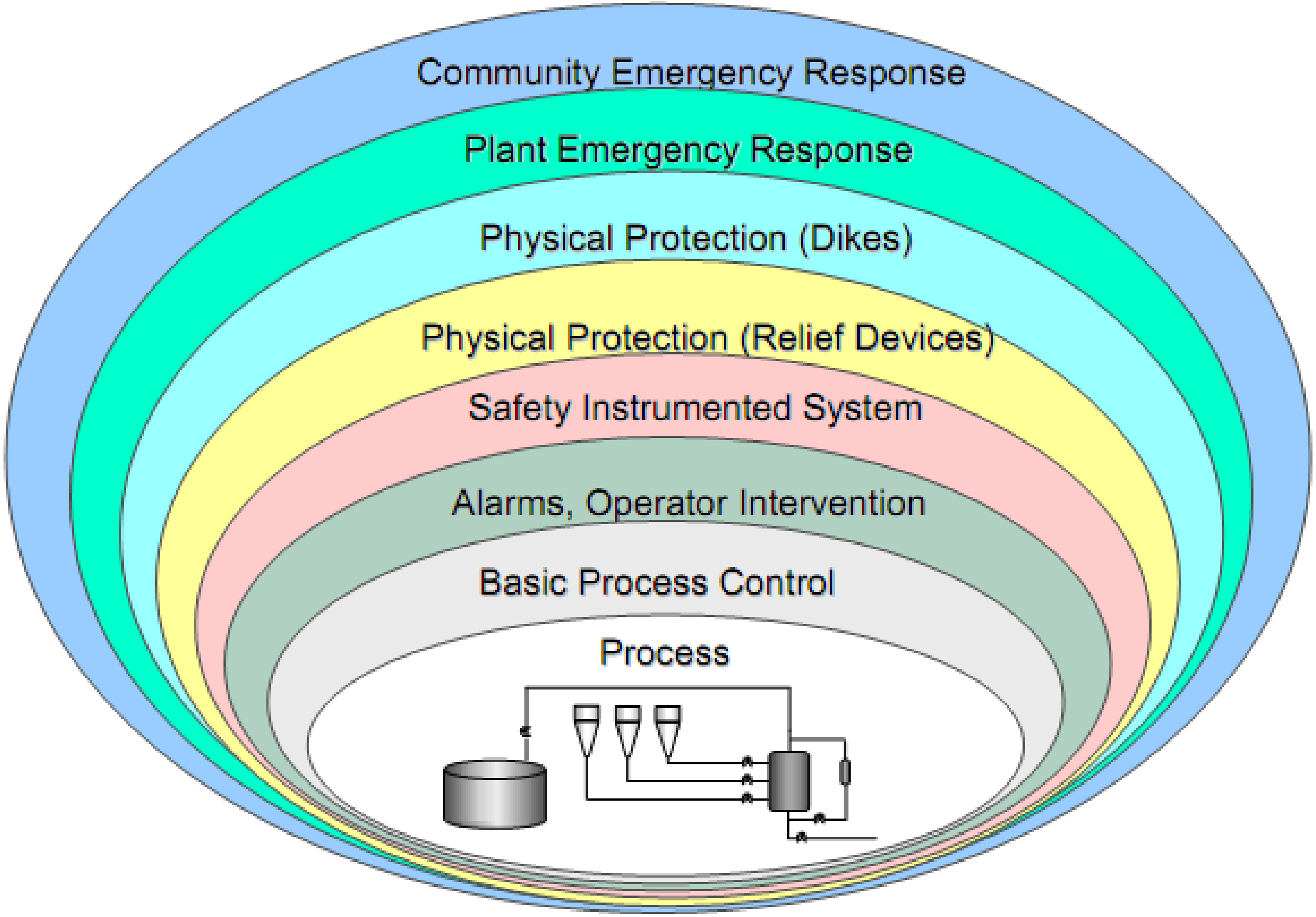
Undesired Consequence

Independent Protection Layer (IPL)
Safeguard capable of preventing a scenario from proceeding to its undesired consequence.

Protection Layers
The Ideal & Reality



Concept of Layers of Protection



Community Emergency Response

Plant Emergency Response

Physical Protection (Dikes)

Physical Protection (Relief Devices)

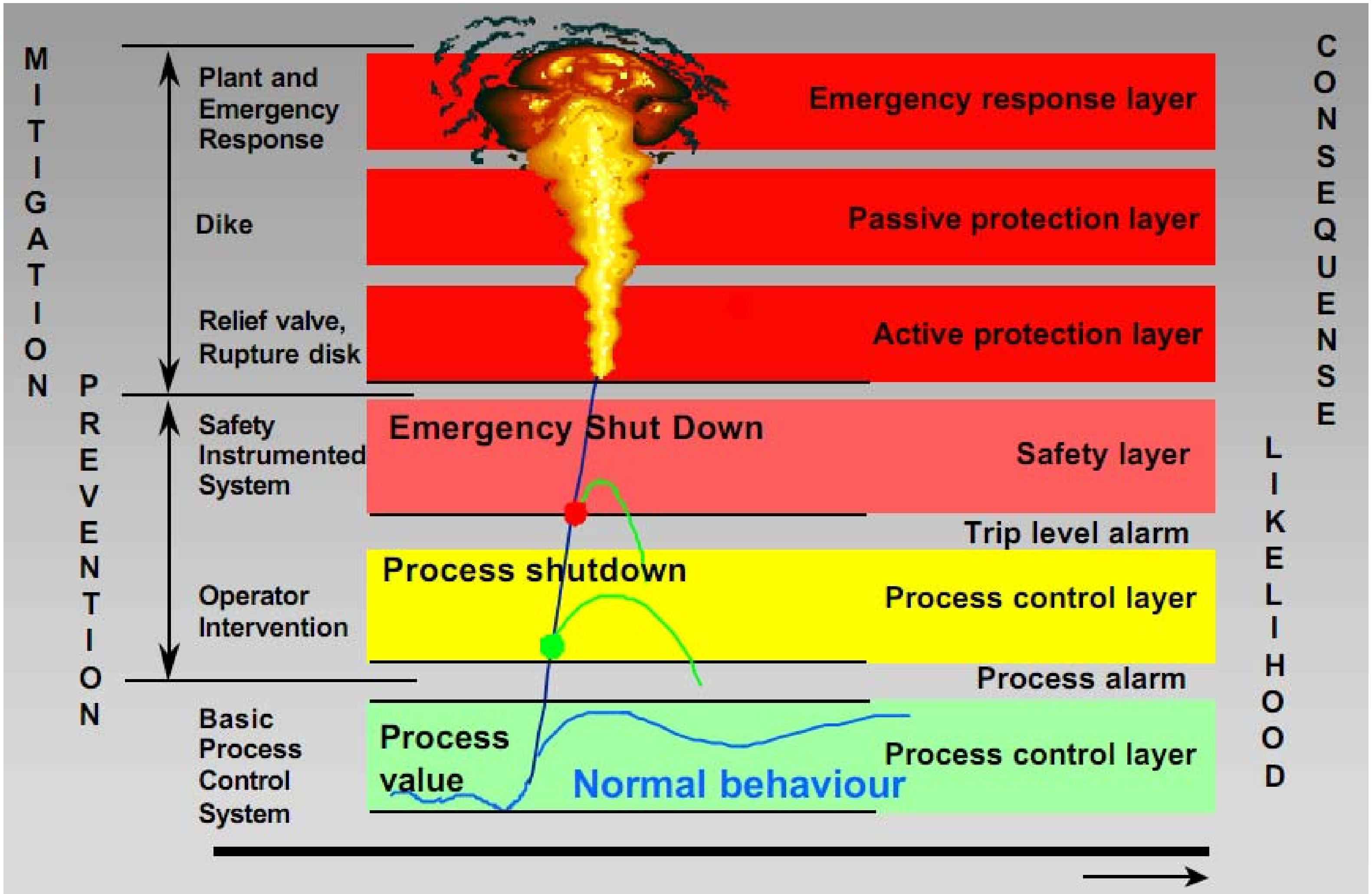
Safety Instrumented System

Alarms, Operator Intervention

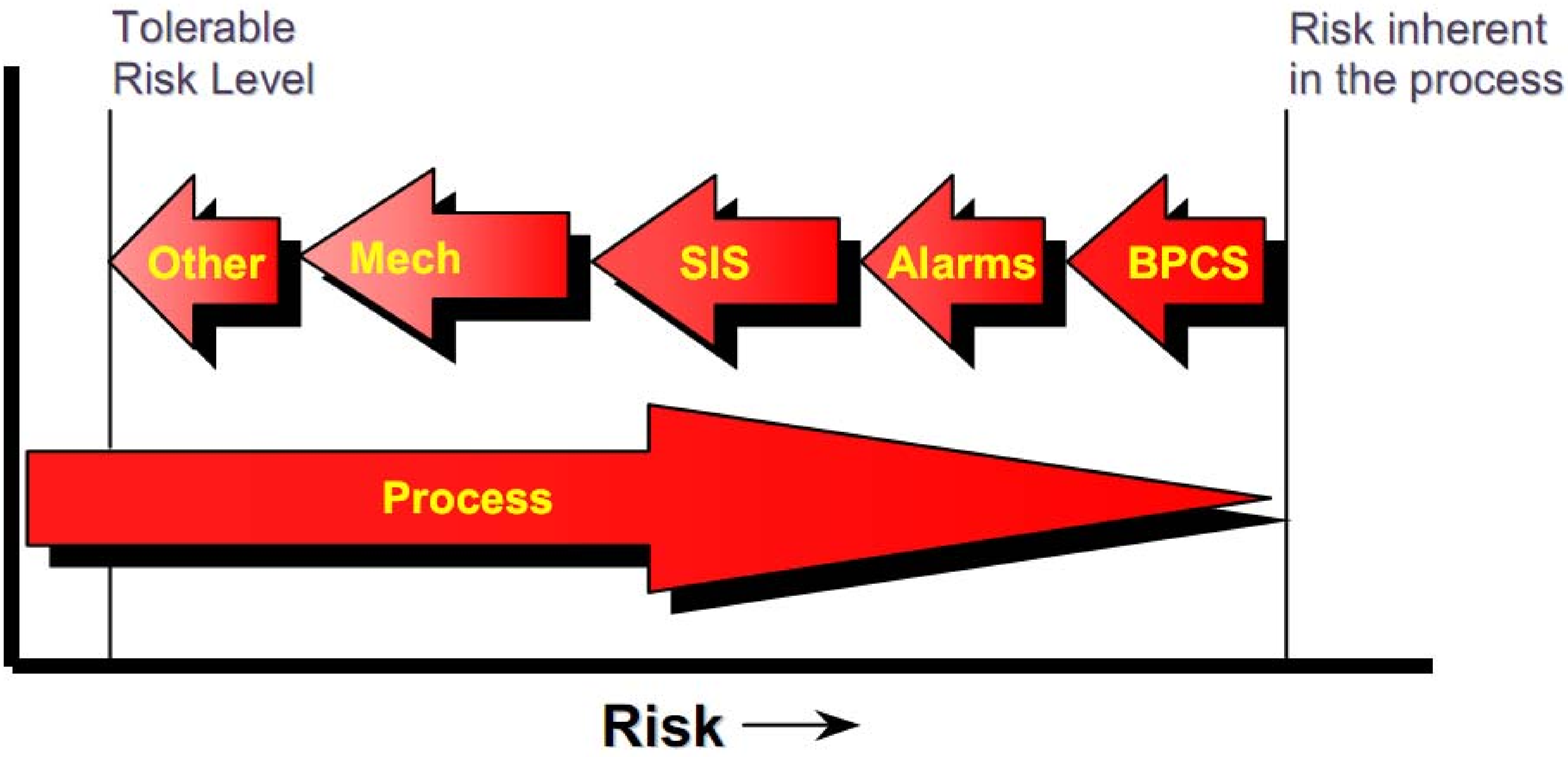
Basic Process Control

Process

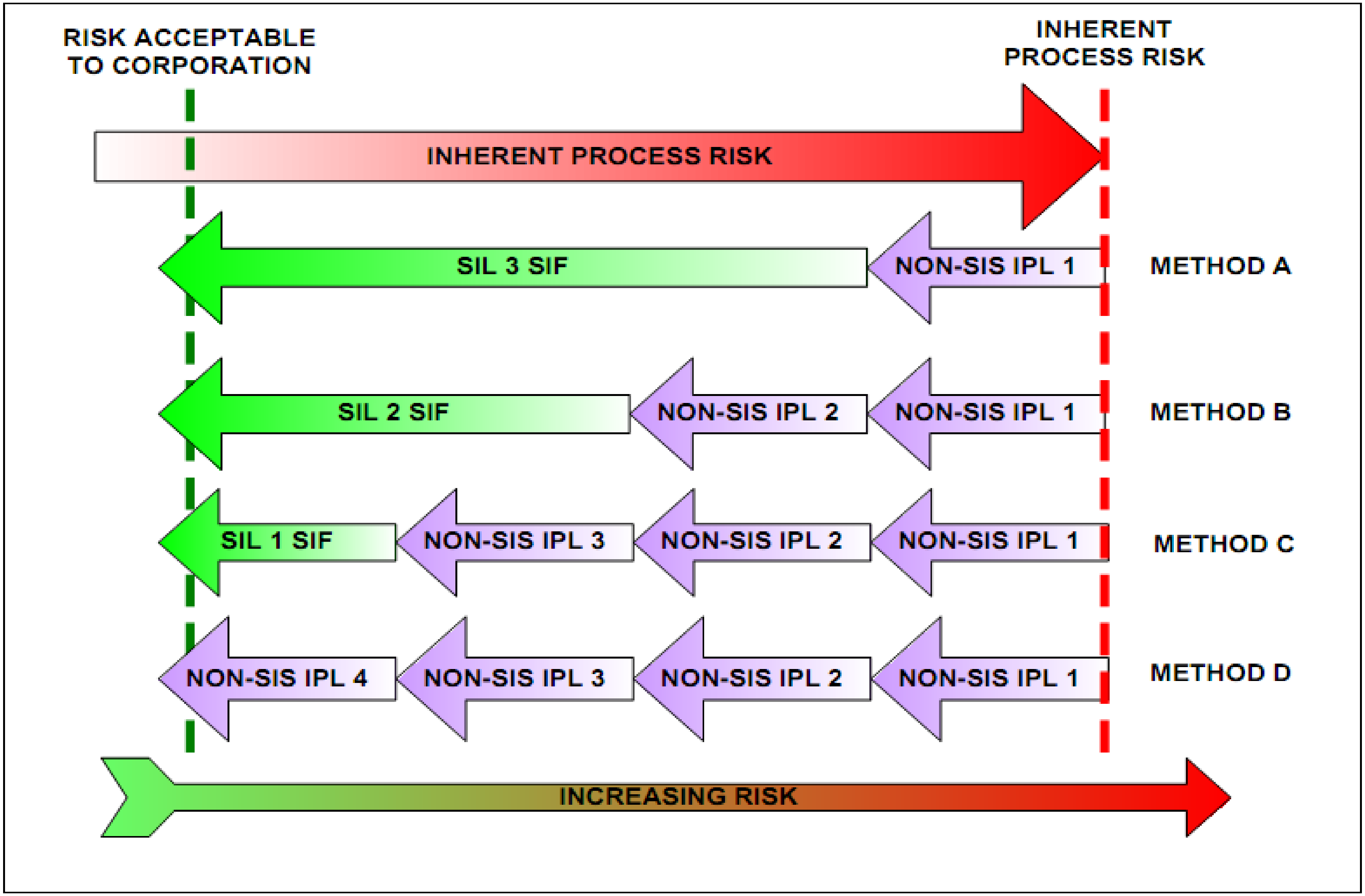
Concept of Layers of Protection



Reducing Risk with Multiple Protection Layers



Risk Reduction Using non-SIS IPLs and SIFs



PETRORISK
MIDDLE EAST – ABU DHABI

What is ***scenario*** ?

Cause + ***Consequence*** = ***Scenario***

LOPA is limited to evaluating ***a single cause-consequence pair*** as a scenario

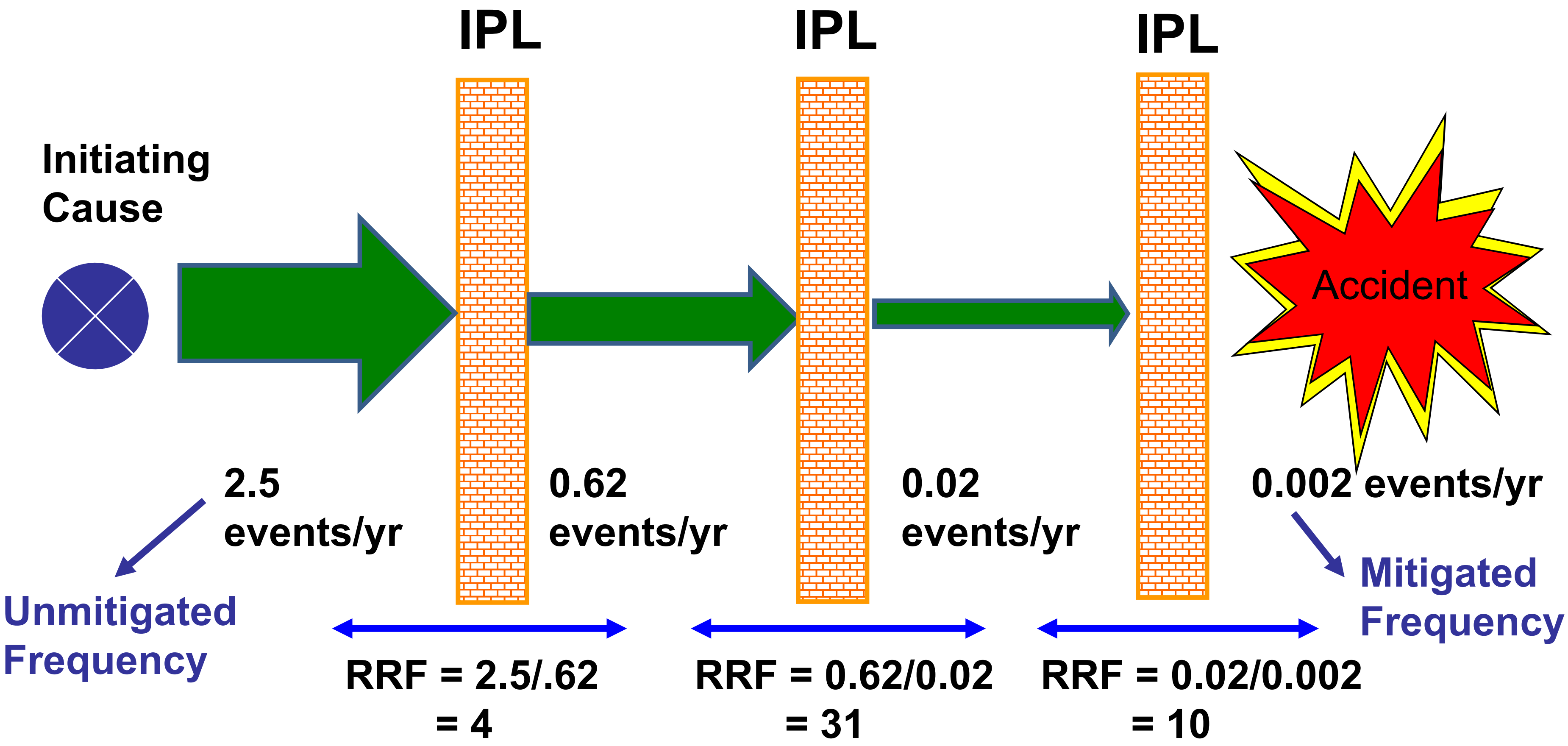
LOPA Five Basic Steps

1. Scenarios identification.
2. Identify the ***initiating event*** of the scenario and determine the initiating event frequency (events per year).
3. Identify the ***IPLs*** and estimate the ***probability of failure on demand*** of each IPL.
4. Estimate the risk of scenario.
5. Compare the calculated risk with the company's tolerable risk criteria

Independent Protection Layers

- All IPLs are safeguards, but **not** all safeguards are IPLs.
- An IPL has two main characteristics:
  - How ***effective*** is the IPL in preventing the scenario from resulting to the undesired consequence?
  - Is the IPL ***independent*** of the initiating event and the other IPLs?

Basic Principle



IPL

IPL

IPL

Initiating Cause

Accident

2.5 events/yr

0.62 events/yr

0.02 events/yr

0.002 events/yr

Unmitigated Frequency

Mitigated Frequency

RRF = 2.5/.62 = 4

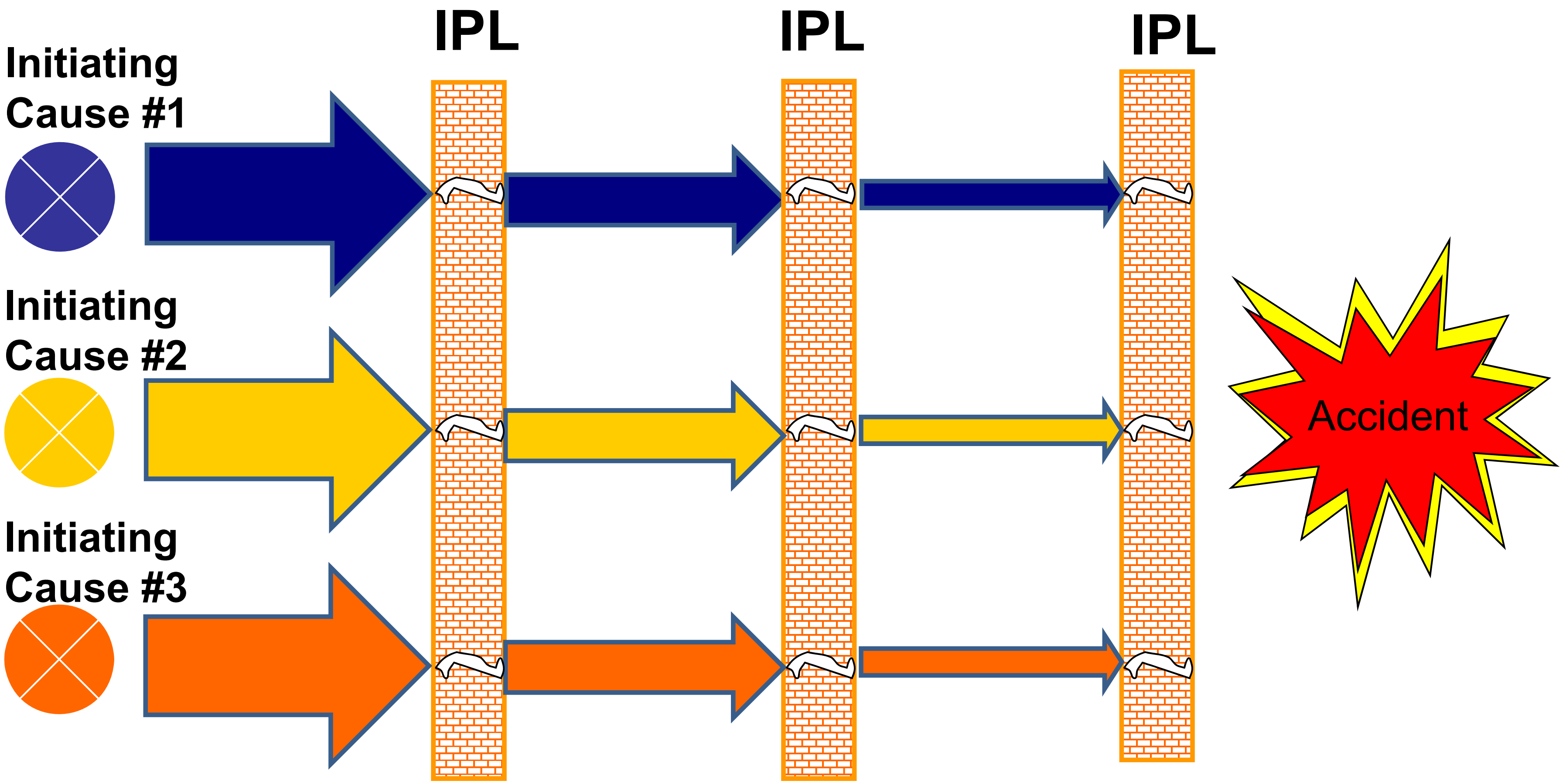
RRF = 0.62/0.02 = 31

RRF = 0.02/0.002 = 10

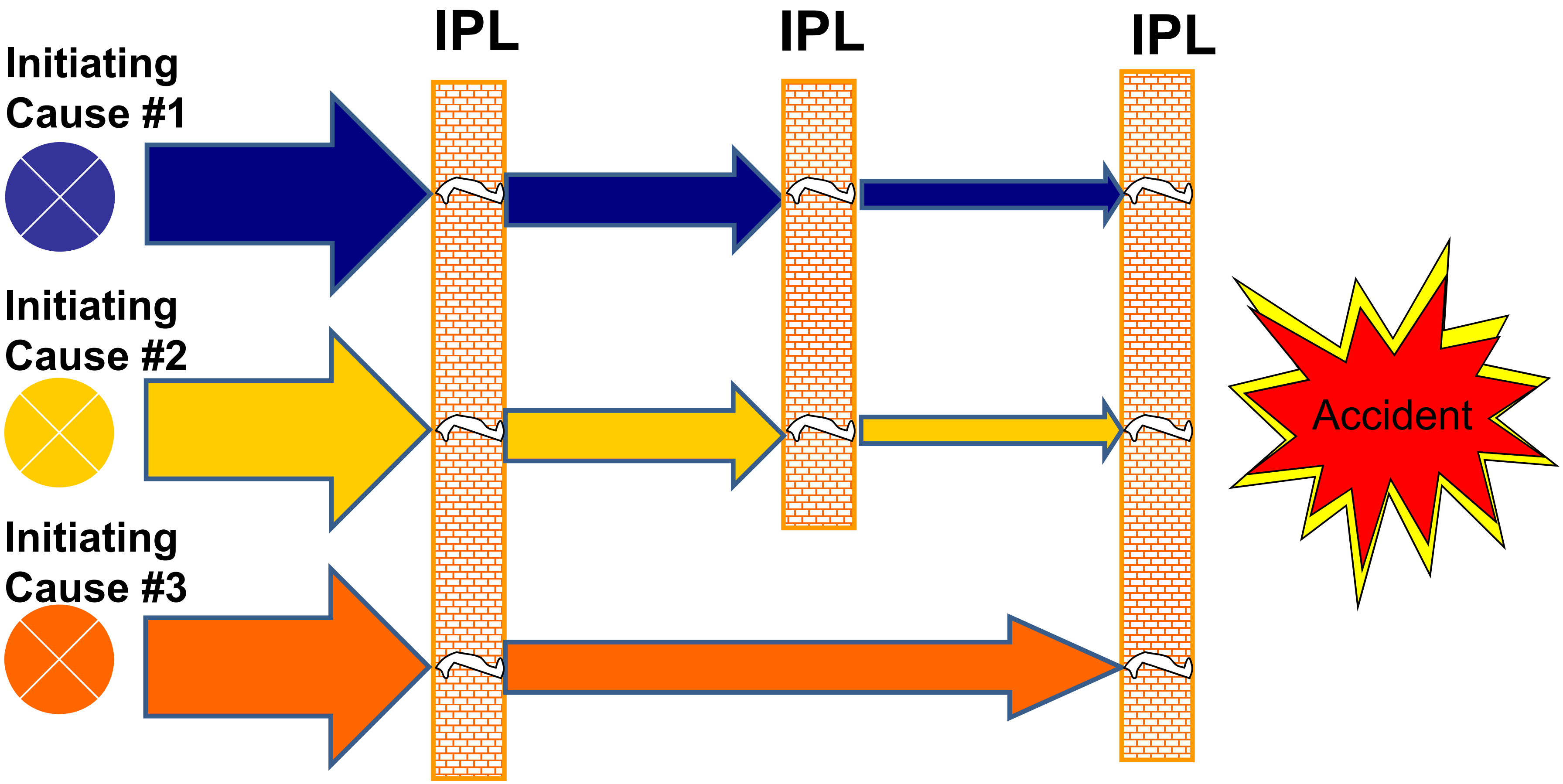
IPL – Independent Protection Layer

RRF – Risk Reduction Factor

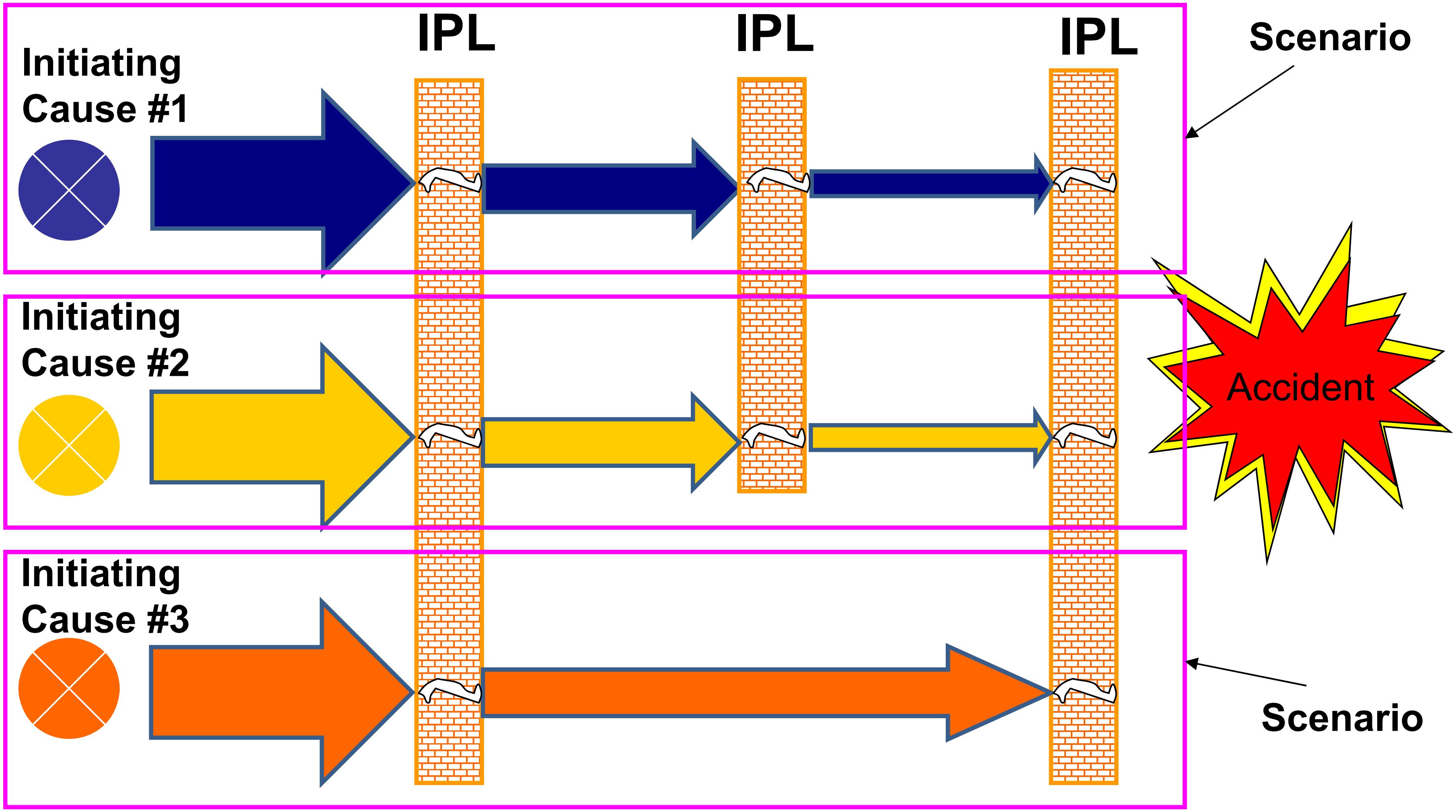
Basic Principle



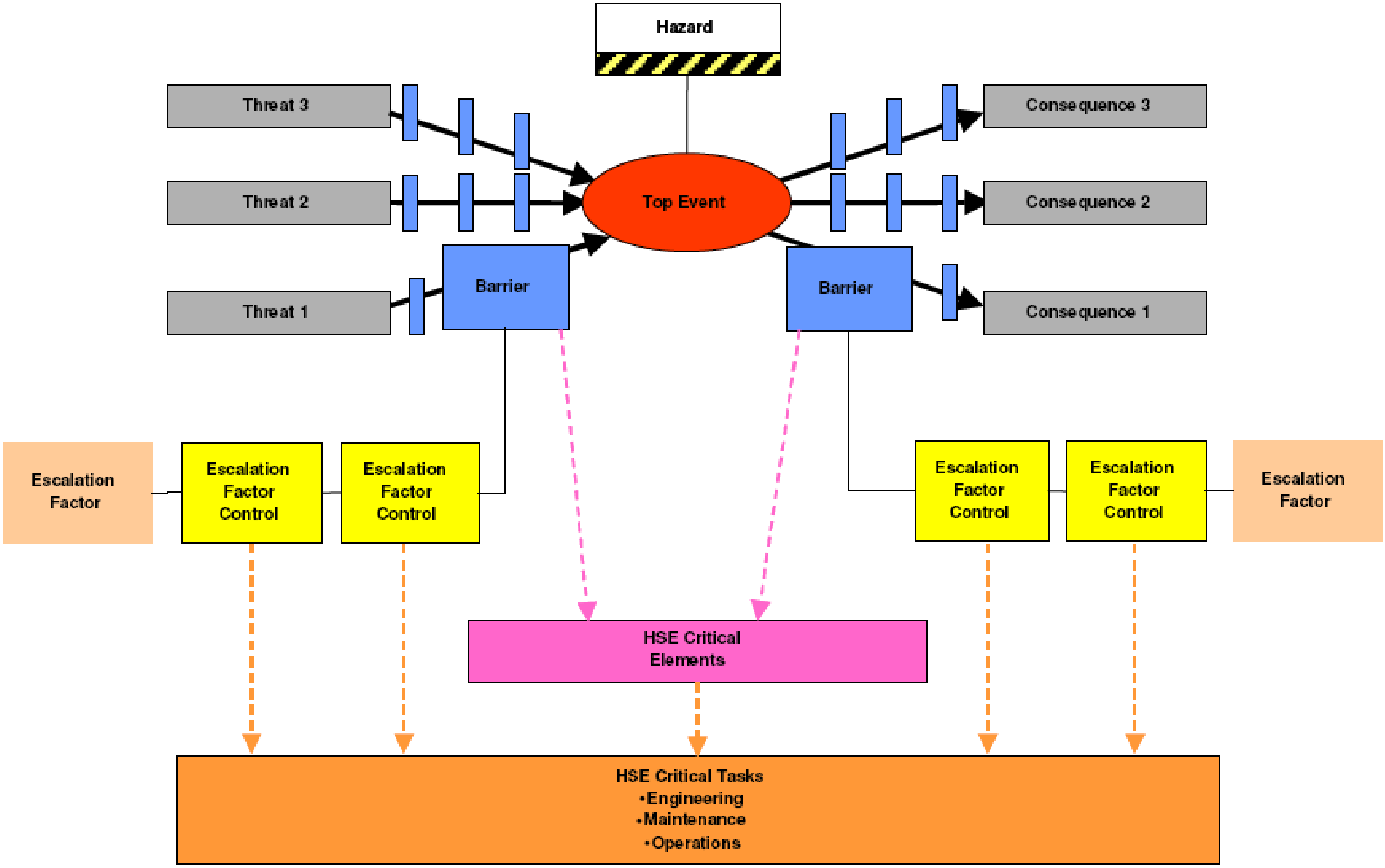
Basic Principle



Basic Principle



Preventive & Mitigative Layers



Hazard

Threat 3

Threat 2

Threat 1

Top Event

Barrier

Barrier

Consequence 3

Consequence 2

Consequence 1

Escalation Factor

Escalation Factor Control

Escalation Factor Control

Escalation Factor Control

Escalation Factor Control

Escalation Factor

HSE Critical Elements

HSE Critical Tasks
- Engineering
- Maintenance
- Operations

PETRORISK MIDDLE EAST – ABU DHABI

No.	Initiating Event	Consequence			
		P	E	A	R
1	Flange leakage, HP Gas, High H2S, Manned Area	✓			
2	Major Crude Oil leakage from sub-sea pipeline		✓	✓	✓
3	Water carryover into HP Air Compressor leading to compressor damage			✓	
4	Over-pressurization & rupture of Gaseous Nitrogen Storage Vessel	✓		✓	
5	Over-pressurization & rupture of Two Phase Separator handling Hydrocarbons leading to fire.	✓		✓	
6	Loss of lube oil to HP Compressor bearings			✓	

Personnel Safety

Environmental

Asset

Reputation

PETRORISK
MIDDLE EAST – ABU DHABI

Multiple Initiating Events

Accidents often have multiple potential triggers that can propagate to an unwanted accident.

Example

Gas Fired boiler's loss of flame without isolating the fuel supply can result in vapour cloud explosion.

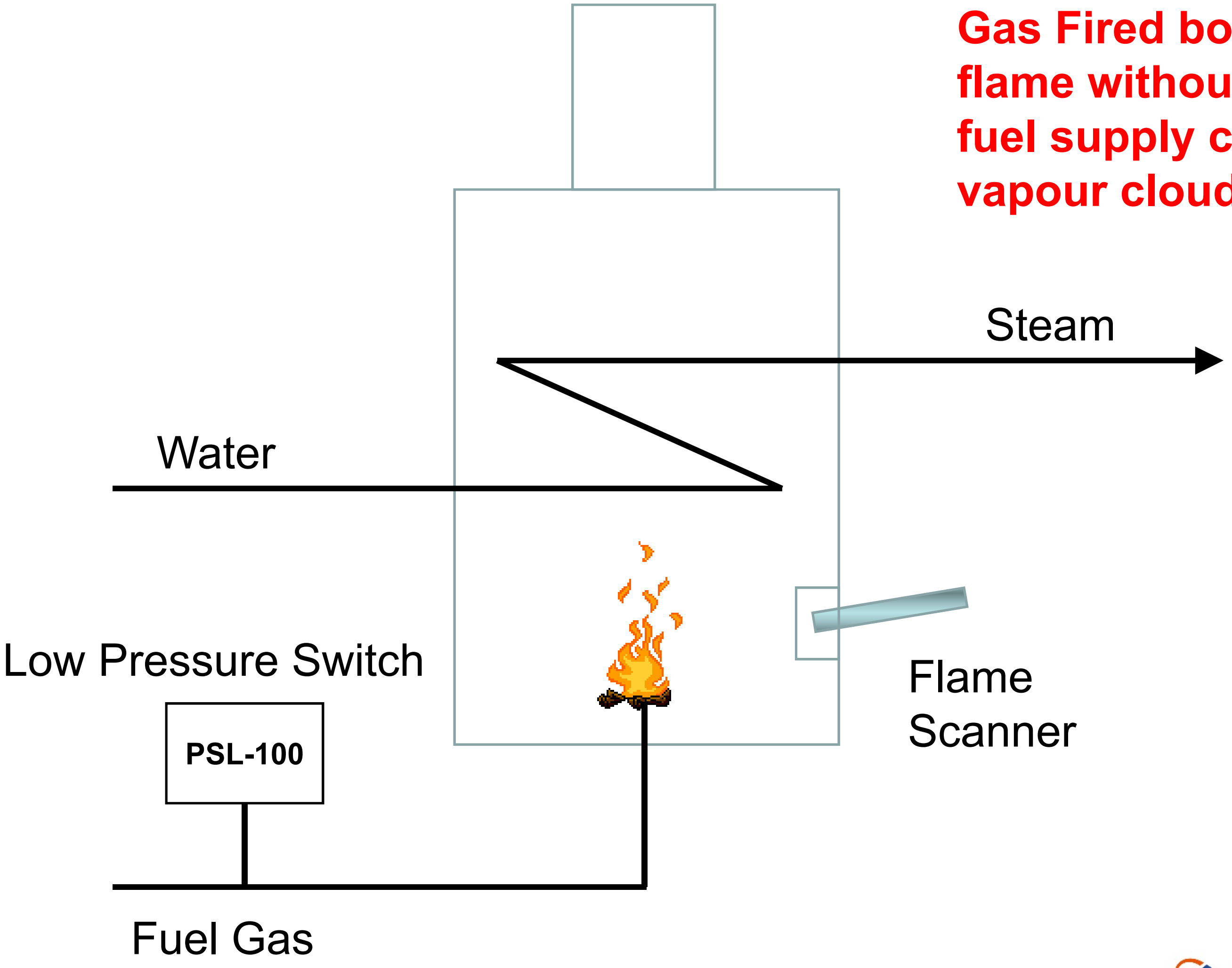
Initiating Events:

1. **A momentary drop in fuel gas pressure**
2. **A momentary high pressure spike**
3. **A slug of condensate in the fuel line**
4. **Incorrect air fuel ratio**

Multiple Initiating Events & IPLs

Example – Gas Fired Boiler

Gas Fired boiler's loss of flame without isolating the fuel supply can result in vapour cloud explosion.



Multiple Initiating Events

Example – Gas Fired Boiler

Accidents often have multiple potential triggers that can propagate to an unwanted accident.

Example

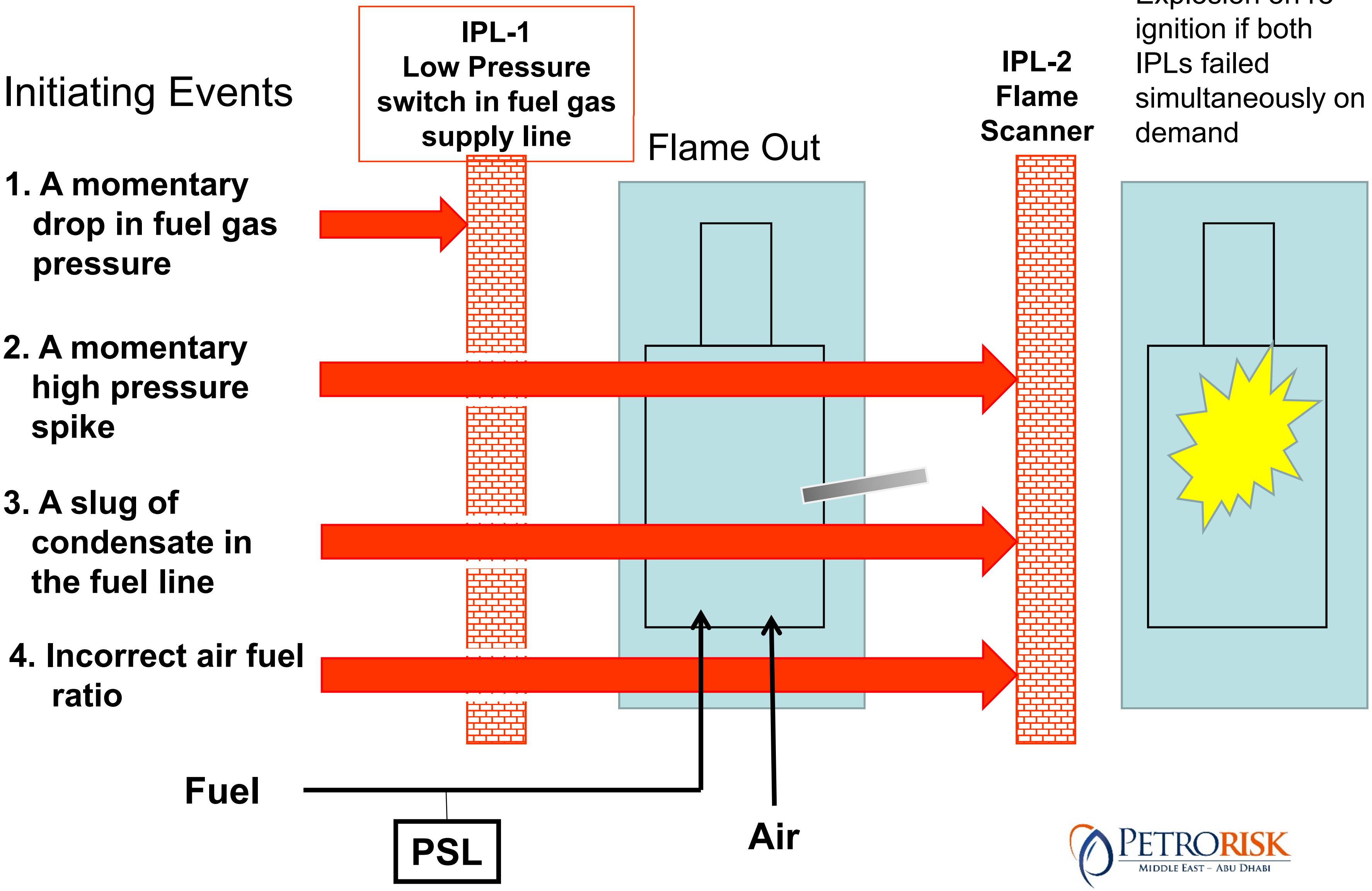
Gas Fired boiler's loss of flame without isolating the fuel supply can result in vapour cloud explosion.

Initiating Events:

1. **A momentary drop in fuel gas pressure**
2. **A momentary high pressure spike**
3. **A slug of condensate in the fuel line**
4. **Incorrect air fuel ratio**

Effective & Non-Effective IPLs

Example – Gas Fired Boiler



Initiating Events

1. **A momentary drop in fuel gas pressure**
2. **A momentary high pressure spike**
3. **A slug of condensate in the fuel line**
4. **Incorrect air fuel ratio**

IPL-1
Low Pressure switch in fuel gas supply line

Flame Out

IPL-2
Flame Scanner

Explosion on re-ignition if both IPLs failed simultaneously on demand

Fuel

PSL

Air

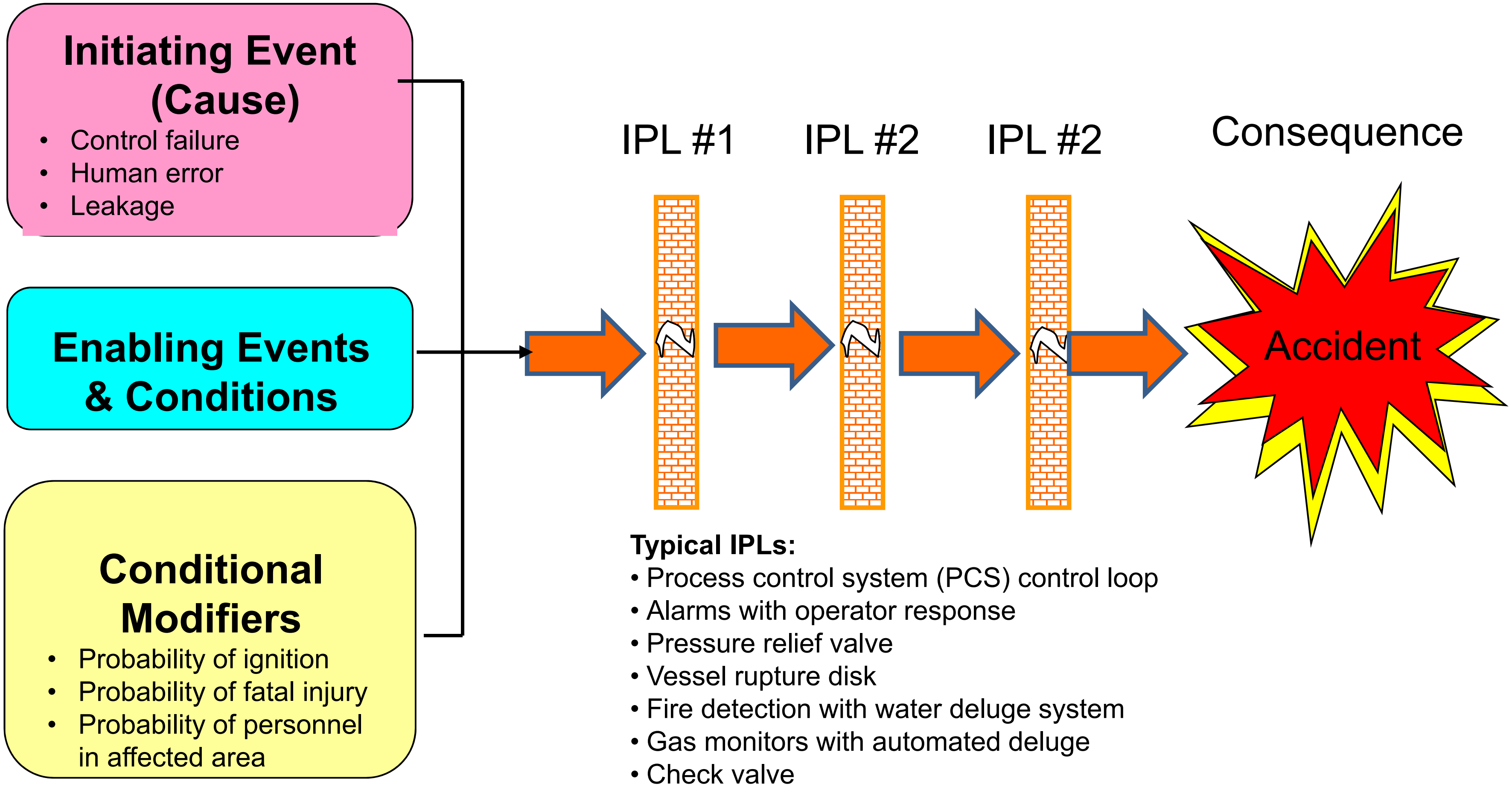
PETRORISK
MIDDLE EAST – ABU DHABI

Effective & Non-Effective IPLs

Example – Gas Fired Boiler

	IPL - 1	IPL-2
Initiating Event	**Low Pressure Switch on Fuel Supply Line**	**Flame Scanner**
A momentary drop in fuel gas pressure	Effective	Effective
A momentary high pressure spike	**Ineffective**	Effective
A pocket of inert gas in the fuel line	**Ineffective**	Effective
Incorrect air fuel ratio	**Ineffective**	Effective

Components in a Scenario



Initiating Event (Cause)

- Control failure
- Human error
- Leakage

Enabling Events & Conditions

Conditional Modifiers

- Probability of ignition
- Probability of fatal injury
- Probability of personnel in affected area

Typical IPLs:

- Process control system (PCS) control loop
- Alarms with operator response
- Pressure relief valve
- Vessel rupture disk
- Fire detection with water deluge system
- Gas monitors with automated deluge
- Check valve
- Flame arrestor
- Vacuum breaker
- Restrictive orifice
- Safety instrumented function (SIF)
- Process Design

PETRORISK
MIDDLE EAST – ABU DHABI

Initiating events

- An initiating event starts the chain-of-events that leads to an accident
- Initiating events can be the failure of a piece of equipment or an operator error

Examples:

- Failure of a cooling water pump
- Starting the wrong pump
- Inadvertent closure of a valve
- Pipe leakage

Initiating Events

Types of Initiating Events:

- ***External events***
  - Earthquakes, tornadoes, hurricanes, or floods
  - Major accidents in adjacent facilities
  - Mechanical impact by motor vehicles
- ***Equipment failures***
  - Component failures in control systems
  - Corrosion
  - Vibration
- ***Human failures***
  - Operational error
  - Maintenance error

Inappropriate Initiating Event

Examples of inappropriate initiating events:

- Inadequate operator training / certification
- Inadequate test and inspection
- Unavailability of protective devices such as safety valves or over-speed trips
- Unclear or imprecise operating procedures

Initiating Events Frequency Estimation

Failure Rate Data Sources:

- Industry Data (e.g. OREDA, IEEE, CCPS, AIChE)
- Company Experience
- Vendor Data
- Third Parties (EXIDA, TUV etc.)

Initiating Events Frequency / Failure Rate Data Estimation

Choosing failure rate data

- It is a **Judgment Call**
- Some considerations:
  - Type of services (clean / dirty ?)
  - Failure mode
  - Environment
  - Past history
  - Process experience
  - Sources of data

Initiating Event Frequency

- If initiating event frequency data is not available then it can be estimated using Fault Tree Analysis.

Initiating Events Frequency Estimation

Example

Corporate records indicate 8 Compressor tripping in the last 10 years in a plant with 6 industrial Process Gas Compressors. What is the compressor tripping event rate?

$$\text{Event Frequency} = \frac{\text{Number of Events}}{\text{Time in Operation}}$$

$$\text{Boiler explosion event rate} = \frac{\text{8 trips}}{\text{6 Compressors x 10 years}}$$

= 0.13 tripings per year per compressor

Initiating Events Frequency Estimation

Example
A plant has 157 relief valves which are tested annually. Over a 5 year period 3 valves failed to pass the function test. What is the failure rate for this plant's relief valves?

$$\text{Event Frequency} = \frac{\text{Number of Events}}{\text{Time in Operation}}$$

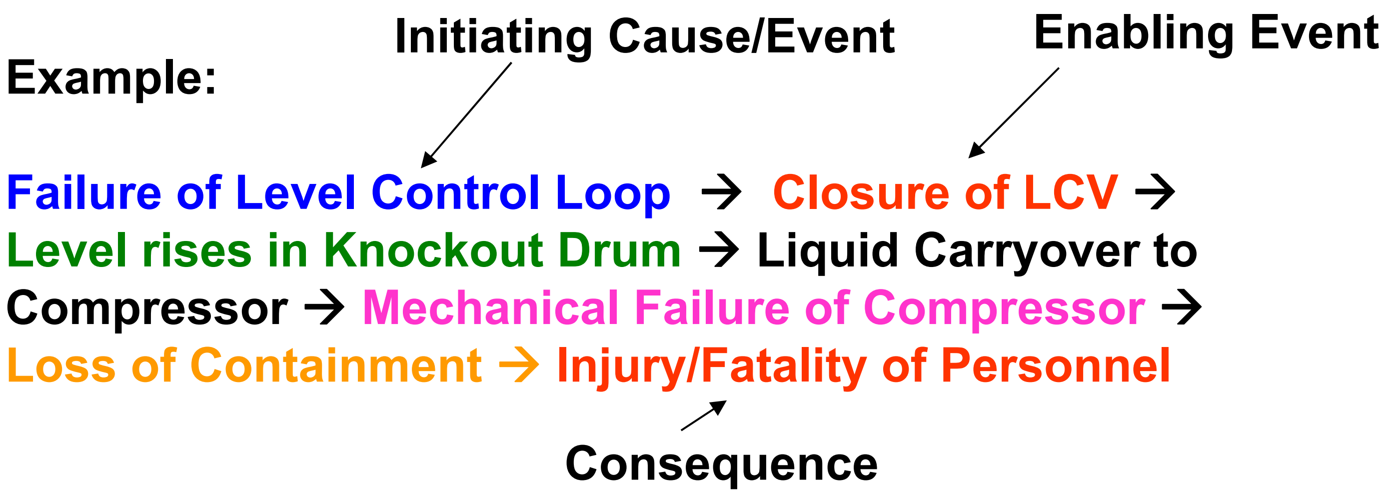
$$\text{Failure Rate for Relief Valve} = \frac{\text{3 function test failures}}{\text{157 valves x 5 years}}$$

$$= \text{0.0038 failures per year per valve}$$

PETRORISK
MIDDLE EAST – ABU DHABI

Enabling Events / Conditions

- Do **not** directly cause the scenario
- Used when the mechanism between the **initiating event** and the **consequences** need to be clarified.



Example:

Initiating Cause/Event

Enabling Event

Failure of Level Control Loop → Closure of LCV → Level rises in Knockout Drum → Liquid Carryover to Compressor → Mechanical Failure of Compressor → Loss of Containment → Injury/Fatality of Personnel

Consequence

Conditional Modifiers

- Probability of ignition
- Probability of fatal injury
- Probability of personnel in affected area

Conditional Modifiers

Probability of Ignition

- Chemical’s reactivity
- Volatility
- Auto-ignition temperature
- Potential sources of ignition that are present

Conditional Modifiers

Probability of Personnel in the Area

- Location of the process unit;
- The fraction of time plant personnel (e.g. personnel from operation, engineering and maintenance) spent in the vicinity

Conditional Modifiers

Probability of Injury

- Personnel training on handling accident scenario
- The ease of recognize a hazardous situation exists in the exposure area
- Alarm sirens and lights
- Escape time
- Accident scenario training to personnel

Independent Protection Layers

- All IPLs are safeguards, but **not** all safeguards are IPLs.
- An IPL has two main characteristics:
  - How ***effective*** is the IPL in preventing the scenario from resulting to the undesired consequence?
  - Is the IPL ***independent*** of the initiating event and the other IPLs?

Independent Protection Layers

Typical layers of protection are:

- Process Design
- Basic Process Control System (BPCS)
- Critical Alarms and Human Intervention
- Safety Instrumented System (SIS)
- Use Factor
- Physical Protection
- Post-release Protection
- Plant Emergency Response
- Community Emergency Response

Independent Protection Layers

Safeguards not usually considered IPLs

- Training and certification
- Procedures
- Normal testing and inspection
- Maintenance
- Communications
- Signs
- Fire Protection (Manual Fire Fighting etc.)
- Plant Emergency Response & Community Emergency Response

Characteristics of IPL

1. **Specificity:** An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (e.g., a runaway reaction, release of toxic material, a loss of containment, or a fire). Multiple causes may lead to the same hazardous event, and therefore multiple event scenarios may initiate action of one IPL.
2. **Independence:** An IPL is independent of the other protection layers associated with the identified danger.
3. **Dependability:** It can be counted on to do what it was designed to do. Both random and systematic failure modes are addressed in the design.
4. **Auditability:** It is designed to facilitate regular validation of the protective functions. Functional testing and maintenance of the safety system is necessary.

Use of Failure Rate Data

Component Failure Data

- Data sources:
  - Guidelines for Process Equipment Reliability Data, CCPS (1986)
  - Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Stations. IEEE (1984)
  - OREDA (Offshore Reliability Data)
  - Layer of Protection Analysis – Simplified Process Risk Assessment, CCPS, 2001

Use of Failure Rate Data

Human Error Rates

- Data sources:
  - Inherently Safer Chemical Processes: A life Cycle Approach , CCPS (1996)
  - Handbook of human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Swain, A.D., and H.E. Guttman, (1983)

Safety Instrumented Function (SIF)

- Instrumented loops that address a **specific** risk
- It intends to achieve or maintain a safe state for the **specific hazardous event**.
- A SIS may contain one or many SIFs and each is assigned a **Safety Integrity Level (SIL)**.
- As well, a SIF may be accomplished by more than one SIS.

Examples of SIFs in Process Industry

- Flame failure in the furnace initiates fuel gas ESDVs to close
- High level in the vessel initiates Compressor shut down
- Loss of cooling water to reactor stops the feed and depressurizes the reactor

Safety Instrumented System (SIS)

A safety instrumented system (SIS) is a combination of sensors, logic solvers and final elements that performs one or more safety instrumented functions (SIFs).

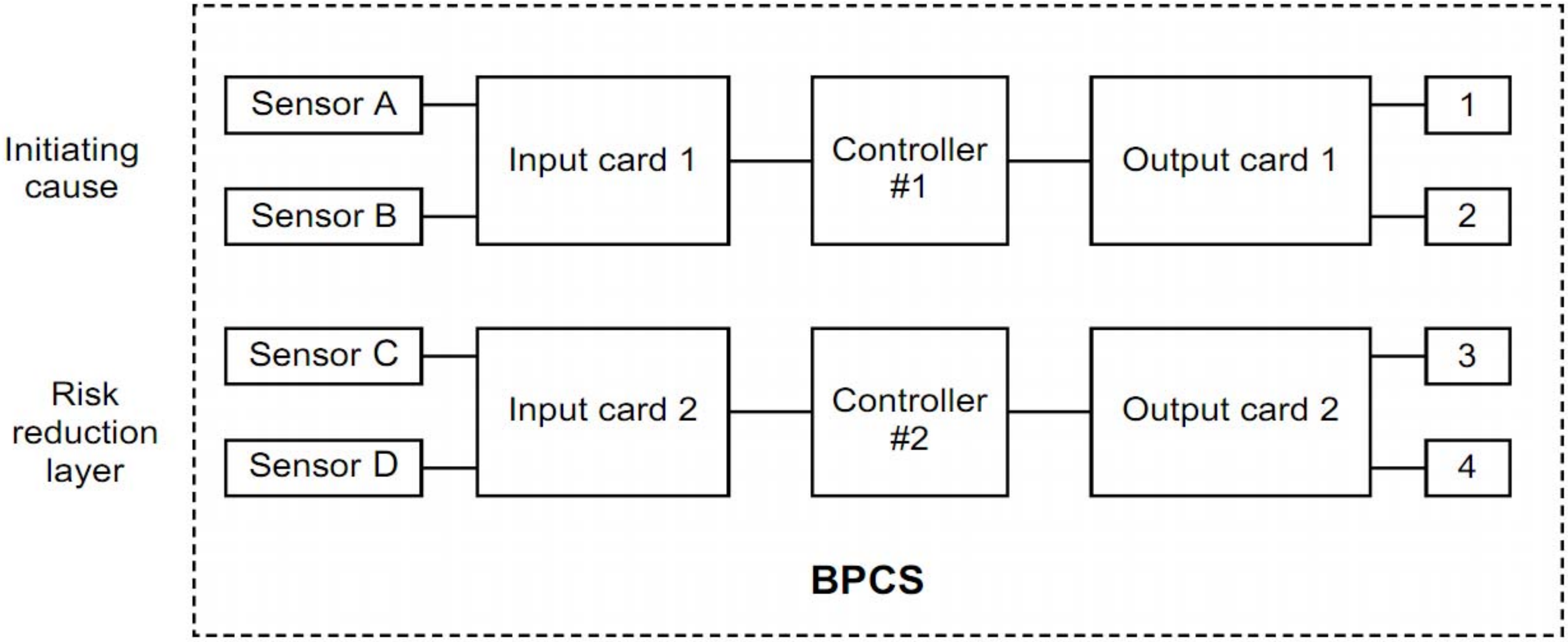
Safety Instrumented Functions

- Specific **single** set of actions and the corresponding equipment needed to identify a **single** emergency and act to bring the system to a safe state.
- SIL is assigned to each SIF based on required risk reduction
- Different from a SIS, which can encompass multiple functions and act in multiple ways to prevent multiple harmful outcomes
  - SIS may have multiple SIF with different individual SIL, so *it is incorrect and ambiguous to define a SIL for an entire safety instrumented system*

Safety Instrumented System

- Functionally SIS are independent from the BPCS
- Reliability of SIS is defined in terms of its Probability of Failure on Demand (PFD) and Safety Integrity Level (SIL)

Independence between Initiating Cause & IPL



Initiating cause

Sensor A

Sensor B

Input card 1

Controller #1

Output card 1

1

2

Risk reduction layer

Sensor C

Sensor D

Input card 2

Controller #2

Output card 2

3

4

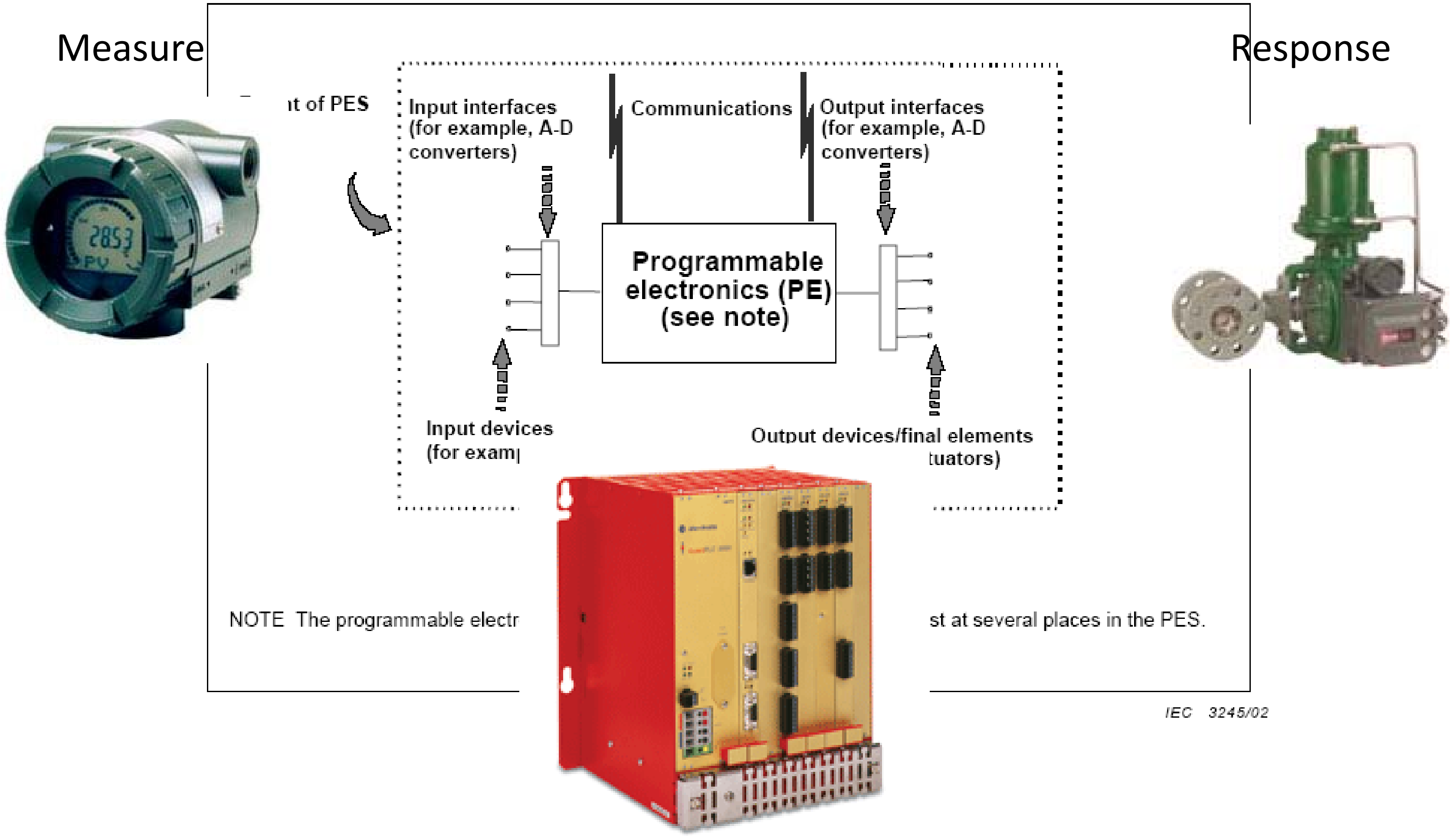
BPCS

Figure 2 – BPCS function and initiating cause independence illustration

Safety Instrumented System

Measure

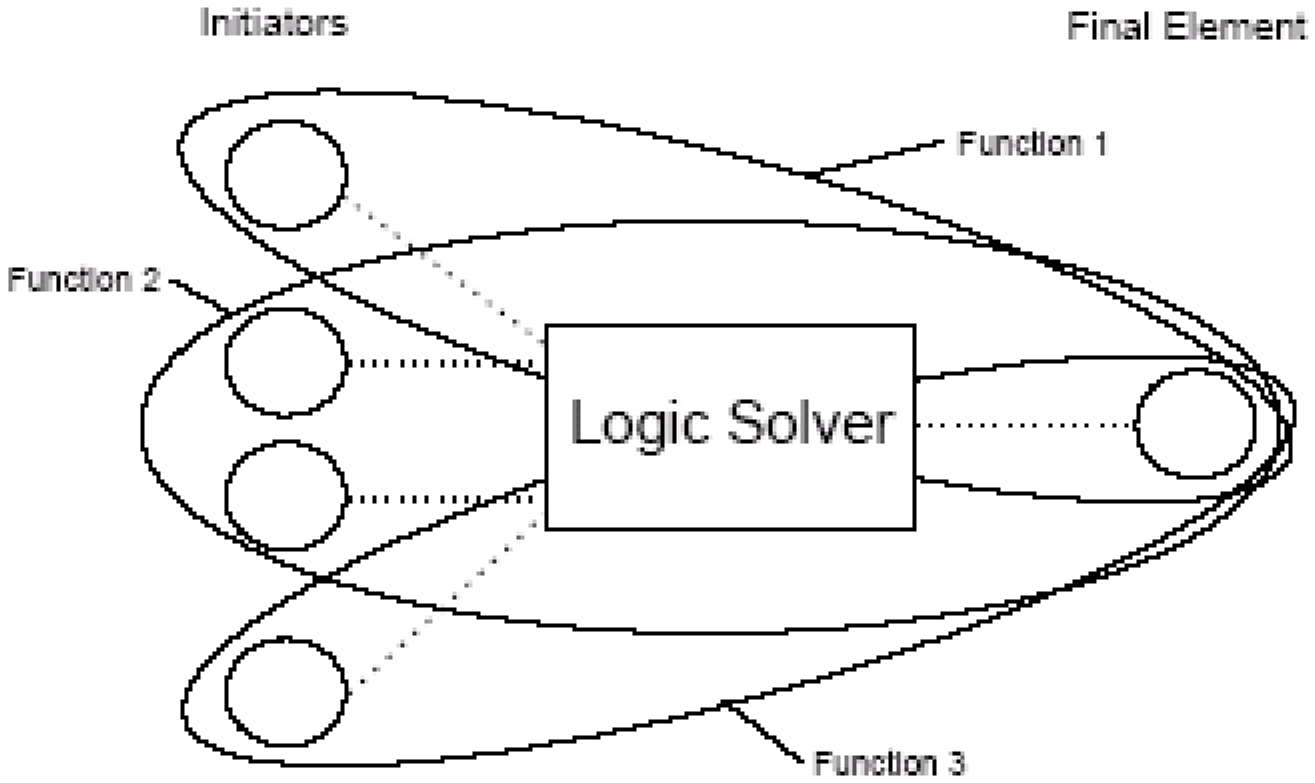
Response



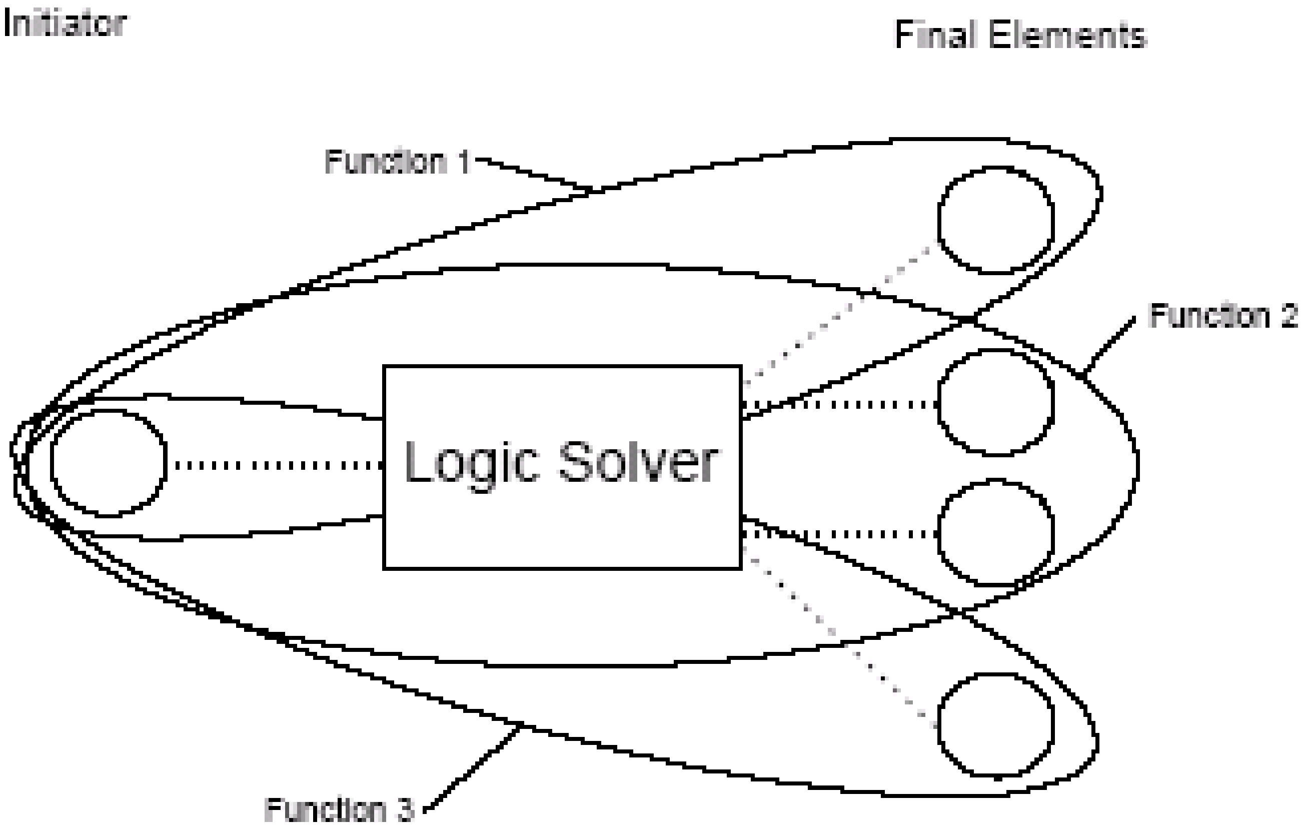
Think

PETRORISK
MIDDLE EAST – ABU DHABI

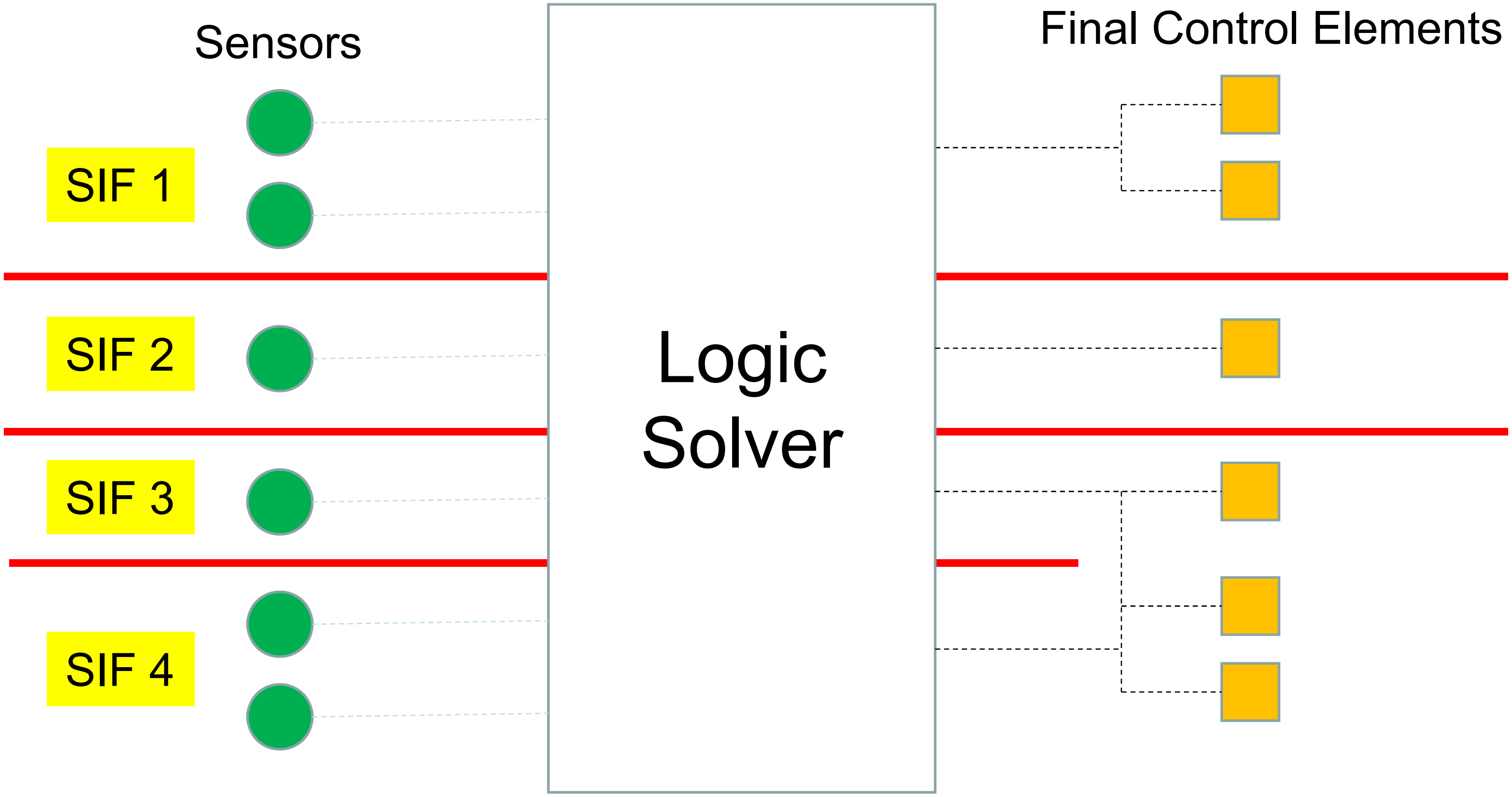
Multiple Initiators tripping one Final Element



One Initiator tripping multiple Final Elements



Overall Safety Instrumented System showing SIFs



PETRORISK
MIDDLE EAST – ABU DHABI

Understanding Safety Integrity Level (SIL)

- **What does SIL mean?**
  - **S**afety **I**ntegrity **L**evel
  - A measure of **probability to fail on demand (PFD)** of the SIS.
  - It is statistical representation of the integrity of the SIS when a process **demand** occurs.
  - A **demand** occurs whenever the process reaches the trip condition and causes the SIS to take action.

SIL Classification

SIL	Probability Category
1	1 in 10 to 1 in 100
2	1 in 100 to 1 in 1,000
3	1 in 1,000 to 1 in 10,000
4	1 in 10,000 to 1 in 100,000

1 in 10 means, the function will fail once in a total of 10 process demands

1 in 1000 means, the function will fail once in a total of 1000 process demands

SIL Classification

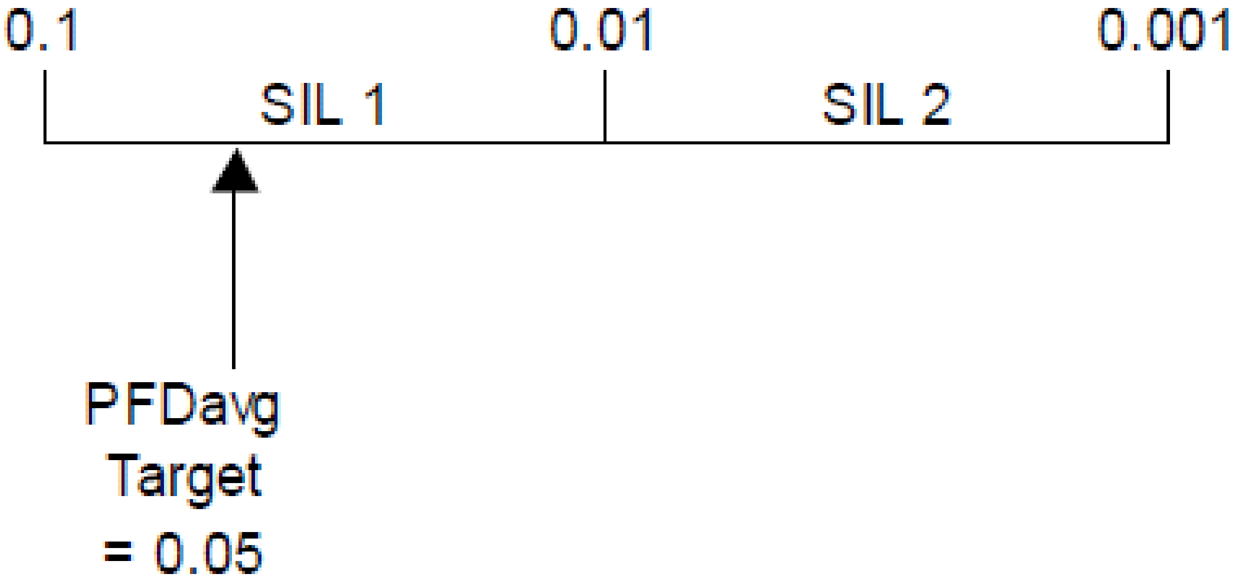
Safety Integrity Levels

SIL Level	**Probability of failure on demand (Demand Mode of Operation)**		**Risk Reduction Factor**
SIL 4	>=10^{-5} to <10^{-4}	>=0.00001 to <0.0001	100000 to 10000
SIL 3	>=10^{-4} to <10^{-3}	>=0.0001 to <0.001	10000 to 1000
SIL 2	>=10^{-3} to <10^{-2}	>=0.001 to <0.01	1000 to 100
SIL 1	>=10^{-2} to <10^{-1}	>=0.01 to <0.1	100 to 10

PETRORISK
MIDDLE EAST – ABU DHABI

Target vs Selected SIL Rating

For example, the required risk reduction from a safety instrumented function needs a $\mathrm{PFD}_{\mathrm{avg}}$ target of 0.05



SIL Methodology

1 Identify the specific hazardous event

2 Determine the severity and target frequency

3 Identify the Initiating Causes

4 Scenario Development

5 Protective Measure Listing (IPLs)

6 Completion of LOPA standard proforma

Setting Tolerable Frequency

For example, if there are 10,000 plants in the country and the operating company accepts the risk equivalent to one catastrophic accident leading to multiple fatalities every 10 years, then the tolerable frequency of the operating company for such an accident would be:

Tolerable Frequency = 1 occurrence per 10,000 plants every 10 years
= 1 / 10,000 / 10
= 1.0E-05 occurrence per year per plant

Or probability of catastrophic accident leading to multiple fatalities per year per plant

It would be wrong to take inverse of 1.0E-05, which would be 100,000 years, and say that a plant will have catastrophic failure every 100,000 years

Frequency Calculation

For example, if the statistical data indicates that 1 out of 300 smokers die every year, then the frequency can be calculated as follows:

Frequency = 1 death per 300 smokers every year

= 1 death / 300 smokers / 1 year

= 3.3E-03 deaths per smoker per year

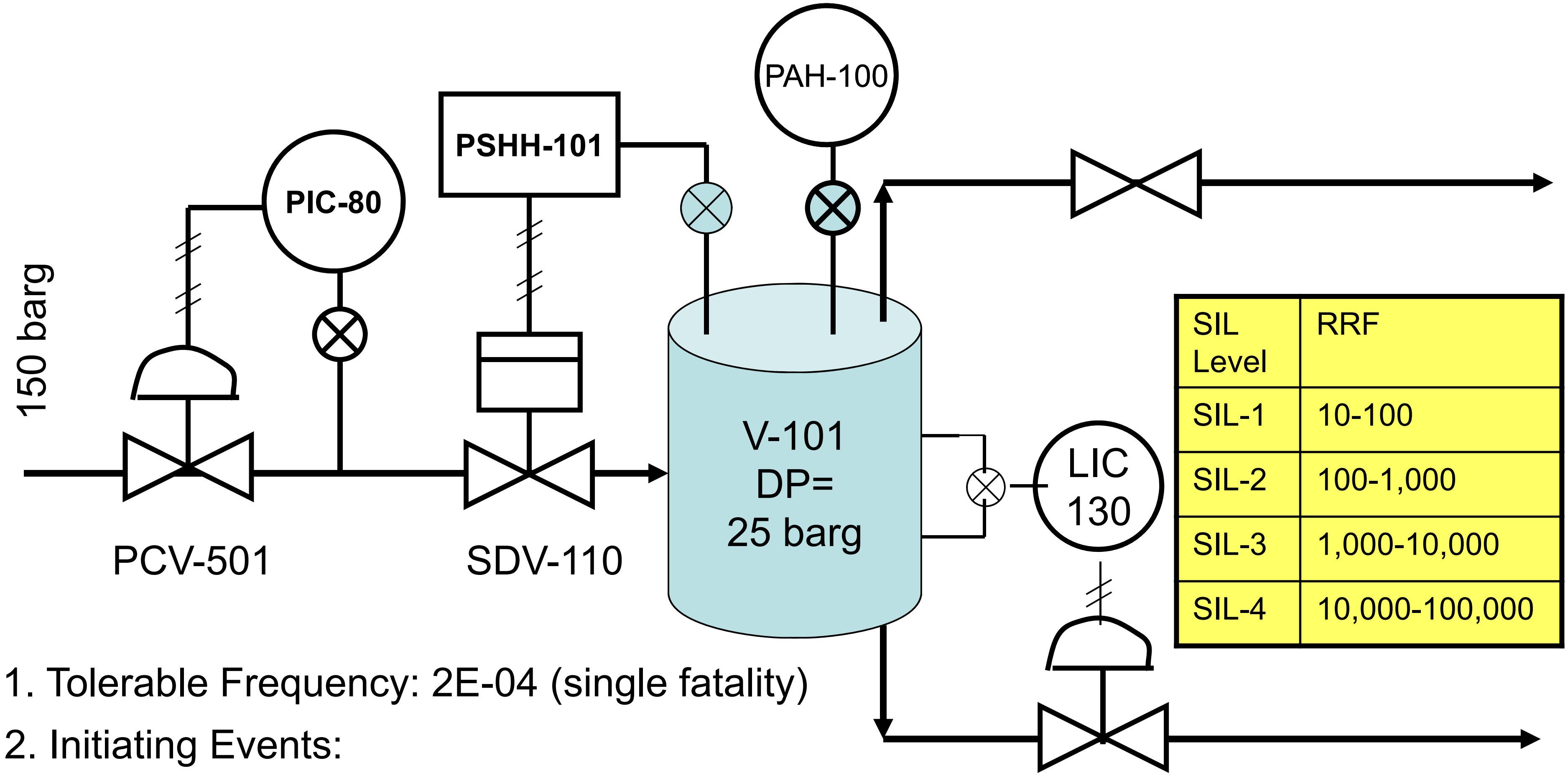
Or probability of a smoker dying per year

It would be wrong to take inverse of 3.3E-03, which would be 300 years, and say that a smoker would die every 300 years

Tolerable Frequencies

Tolerable Frequency	People	Environment	Assets	Reputation
2E-05 /yr	**Multiple fatalities or permanent disabilities**	**Massive Effect- Persistent severe environmental damage**	**Substantial or a total loss of operations (>$10,000,000)**	**Extensive adverse coverage in international media.**
2E-04 /yr	**Single fatality or permanent disability**	**Major effect- severe environmental damage**	**Partial operation loss and/or prolonged shutdown (<$10,000,000)**	**National public concern. Extensive adverse coverage in the national media.**
2E-03 /yr	**Serious injuries (lost time cases)**	**Localized effect- Limited loss of discharge of known toxicity**	**Extended plant damage and/or partial shutdown (<$500,000)**	**Regional public concern. Extensive adverse coverage in local media.**
2E-02 /yr	**Minor injuries (medical treatment cases)**	**Minor Effect Contamination**	**Moderate plant damage and/or brief operations disruption (<$100,000)**	**Some local public concern. Some local media coverage.**
2E-01 /yr	**Slight injuries (first aid cases)**	**Slight release Local Environment damage**	**Minor plant damage and no disruption to Operations (<$10,000)**	**Public awareness may exist, but there is no public concern.**

SIL Calculation

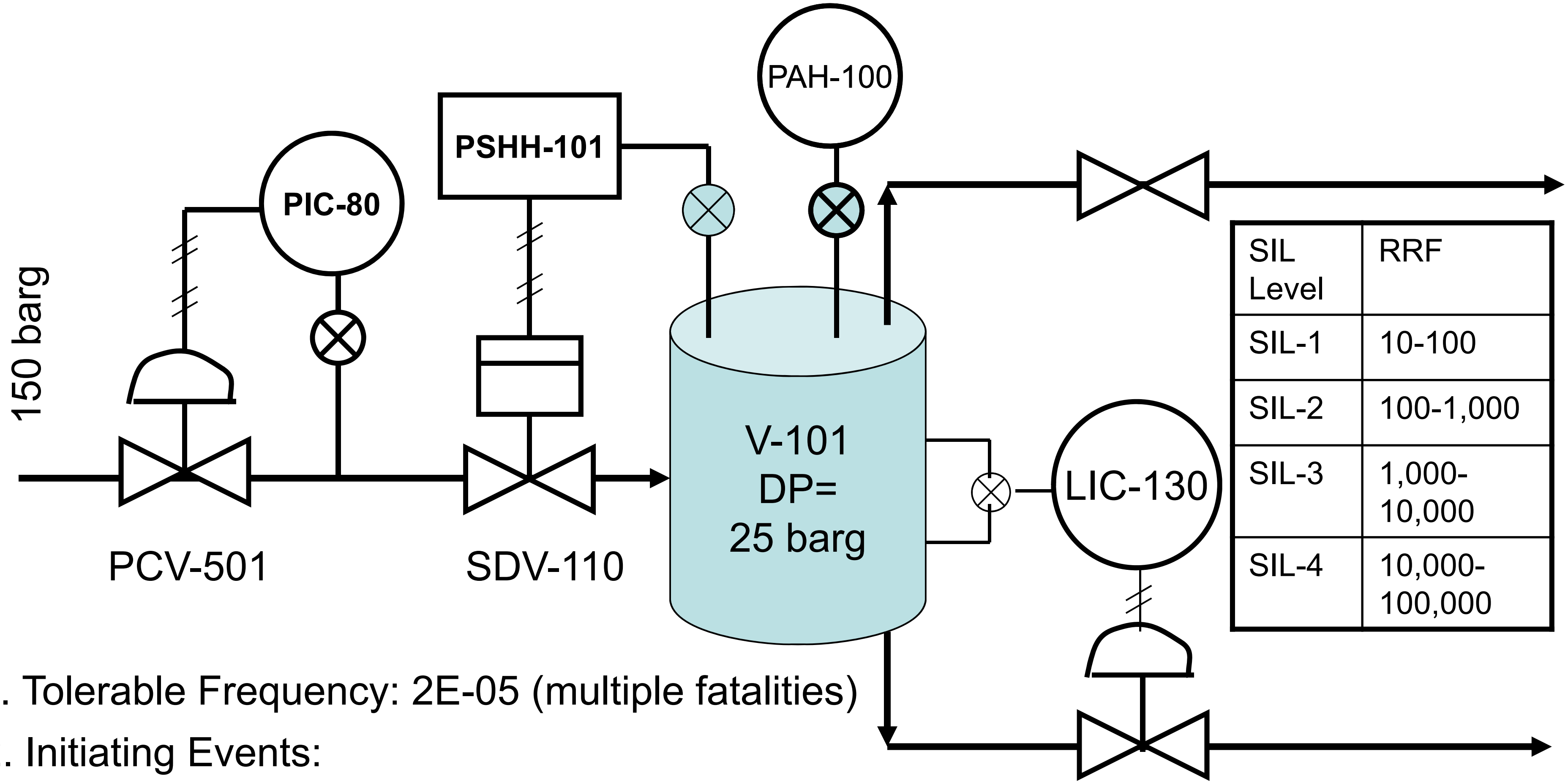


SIL Level	RRF
SIL-1	10-100
SIL-2	100-1,000
SIL-3	1,000-10,000
SIL-4	10,000-100,000

1. Tolerable Frequency: 2E-04 (single fatality)
2. Initiating Events:
   PCV-501 Fail Opened
   Initiating Event Frequency → 0.1/yr
3. Independent Protection Layers (IPLs):
   High Pressure Alarm, PAH-100
   Prob. of Failure on Demand → 0.1
4. Actual Frequency:
   0.1/yr x 0.1 = 0.01/yr
5. Risk Reduction Factor:
   =Actual Frequency / Tolerable Frequency
   =0.01/2E-04
   =50 (SIL-1)

PETRORISK
MIDDLE EAST – ABU DHABI

SIL Calculation

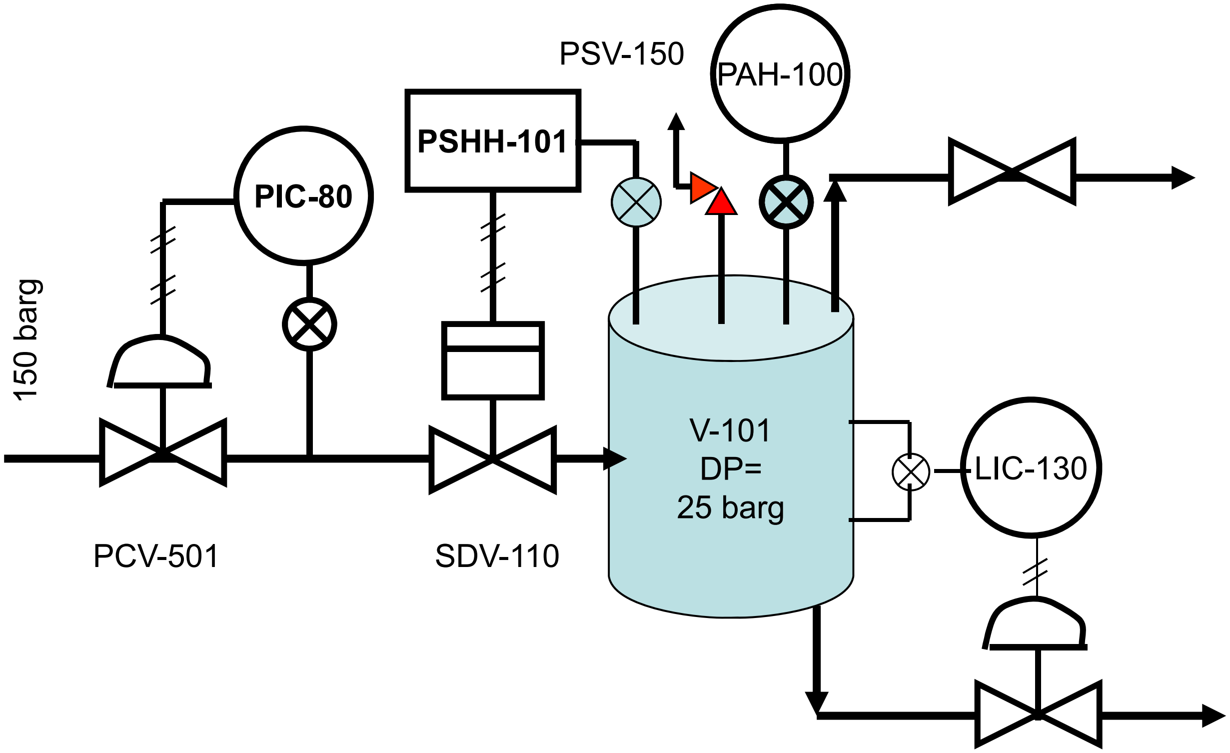


SIL Level	RRF
SIL-1	10-100
SIL-2	100-1,000
SIL-3	1,000-10,000
SIL-4	10,000-100,000

1. Tolerable Frequency: 2E-05 (multiple fatalities)
2. Initiating Events:
   PCV-501 Fail Opened
   Initiating Event Frequency → 0.1/yr
3. Independent Protection Layers (IPLs):
   High Pressure Alarm, PAH-100
   Prob. of Failure on Demand → 0.1
4. Actual Frequency:
   0.1/yr x 0.1 = 0.01/yr
5. Risk Reduction Factor:
   =Actual Frequency / Tolerable Frequency
   =0.01/2E-05
   =500 (SIL-2)

PETRORISK
MIDDLE EAST – ABU DHABI

SIL Calculation



SIL Level	RRF
SIL-1	10-100
SIL-2	100-1,000
SIL-3	1,000-10,000
SIL-4	10,000-100,000

1. Tolerable Frequency: 2E-05
   (multiple fatalities)
2. Initiating Events:
   PCV-501 Fail Opened
   Initiating Event Frequency → 0.1/yr
3. Independent Protection Layers (IPLs):
   High Pressure Alarm, PAH-100; PFDavg → 0.1
   Pressure Safety Valve, PSV-150; PFDavg → 0.01
4. Actual Frequency: 0.1/yr x 0.1 x 0.01 = 0.001/yr
   (Alarm) (PSV)
5. Risk Reduction Factor:
   =Actual Freq. / Tolerable Freq.
   =0.001/2E-05
   =50 (SIL-1)

PETRORISK
MIDDLE EAST – ABU DHABI