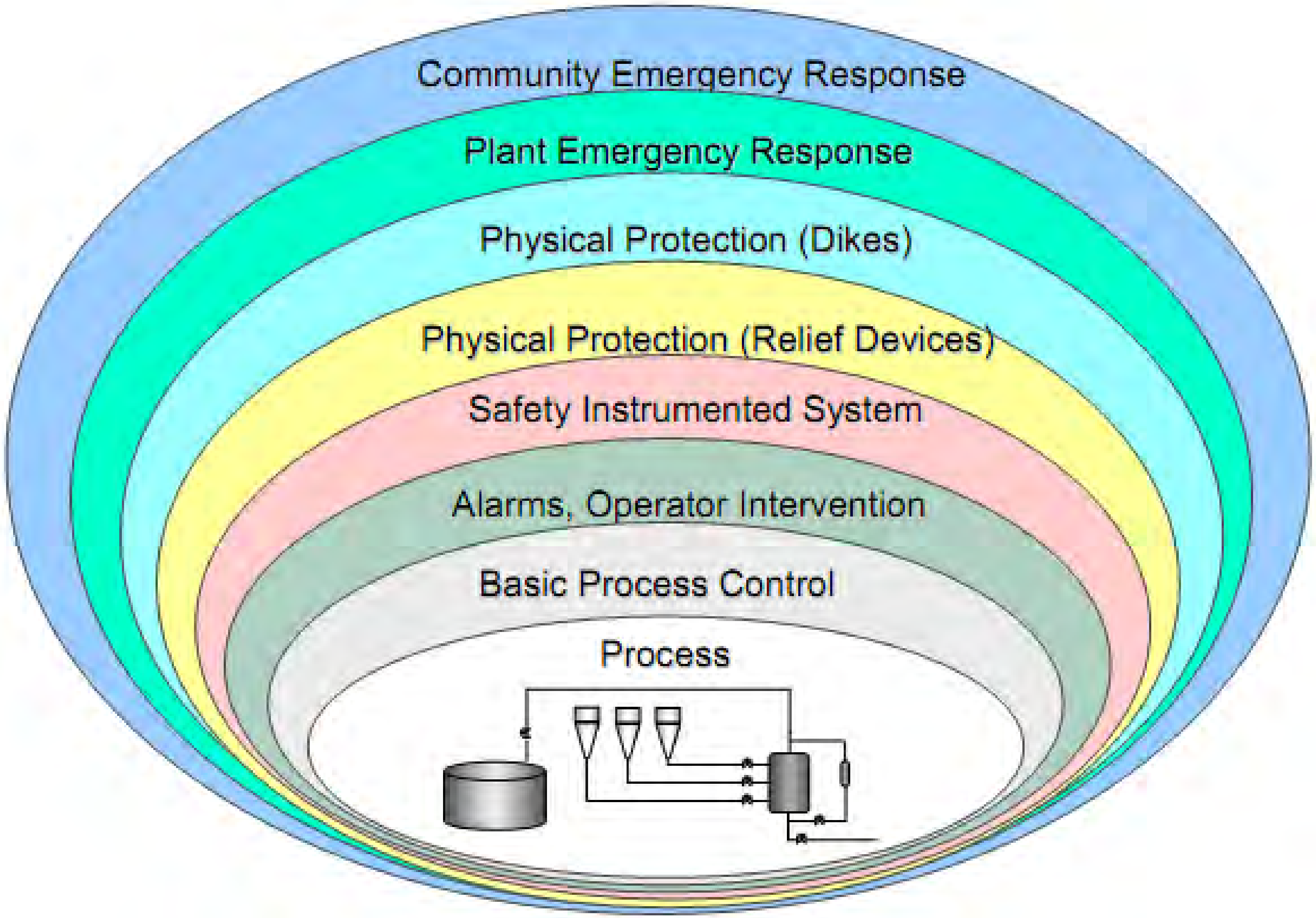
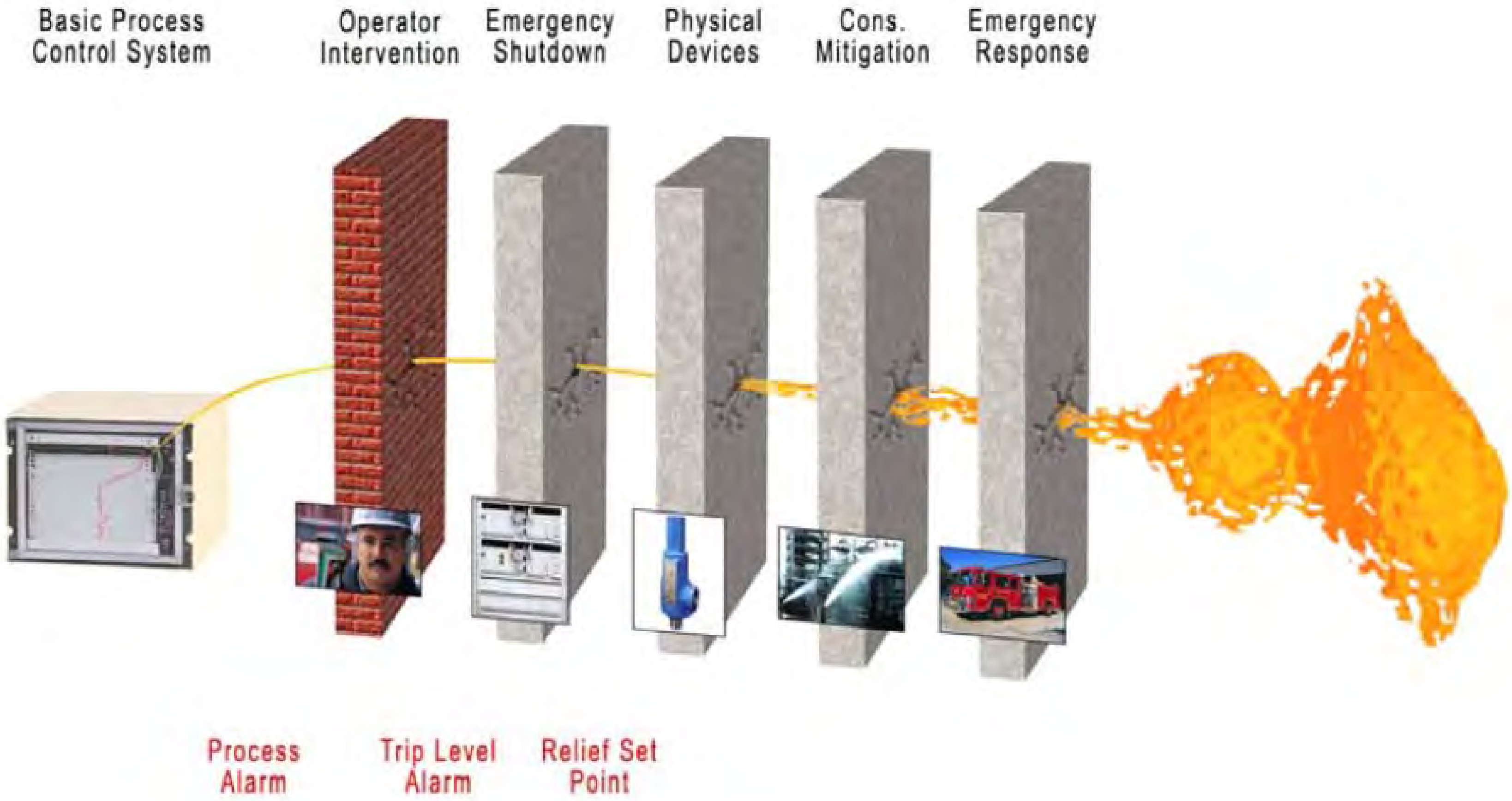
Basic Introduction
to
SIL Assessment
using
Layers of Protection Analysis (LOPA)

Fayyaz Moazzam
Principal Consultant
Petrorisk Middle East, Abu Dhabi, United Arab Emirates
M. +971 56 127 3688
fayyaz.moazzam@petrorisk.com
www.petrorisk.com

Concept of Layers of Protection



Concept of Layers of Protection



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.

PETRORISK
MIDDLE EAST LIMITED - ABU DHABI

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*

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).

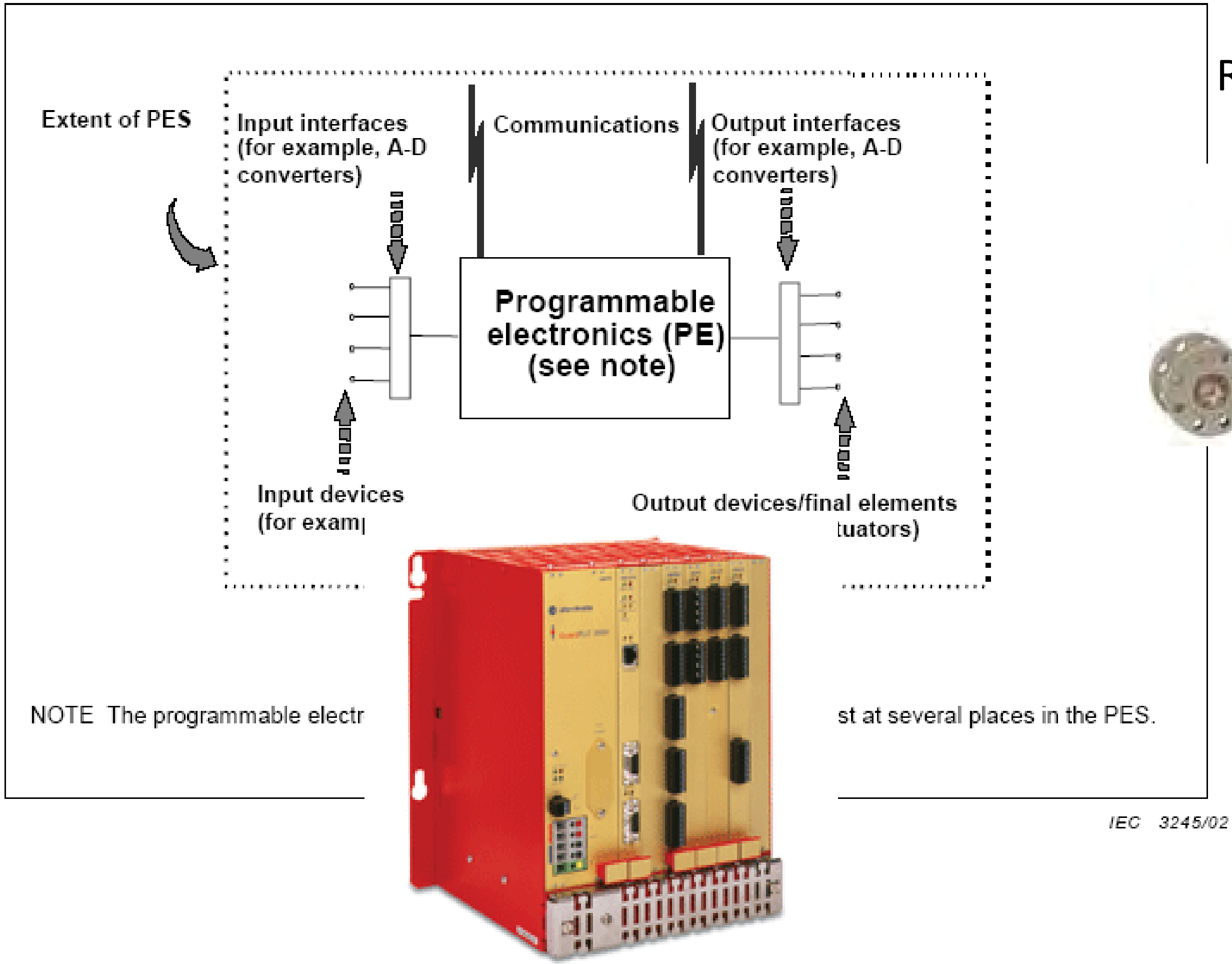
A SIS is much like a basic process control system (BPCS) but a SIS operates in a completely different mode and unique design and maintenance, or mechanical integrity requirements are needed.

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)

Safety Instrumented System

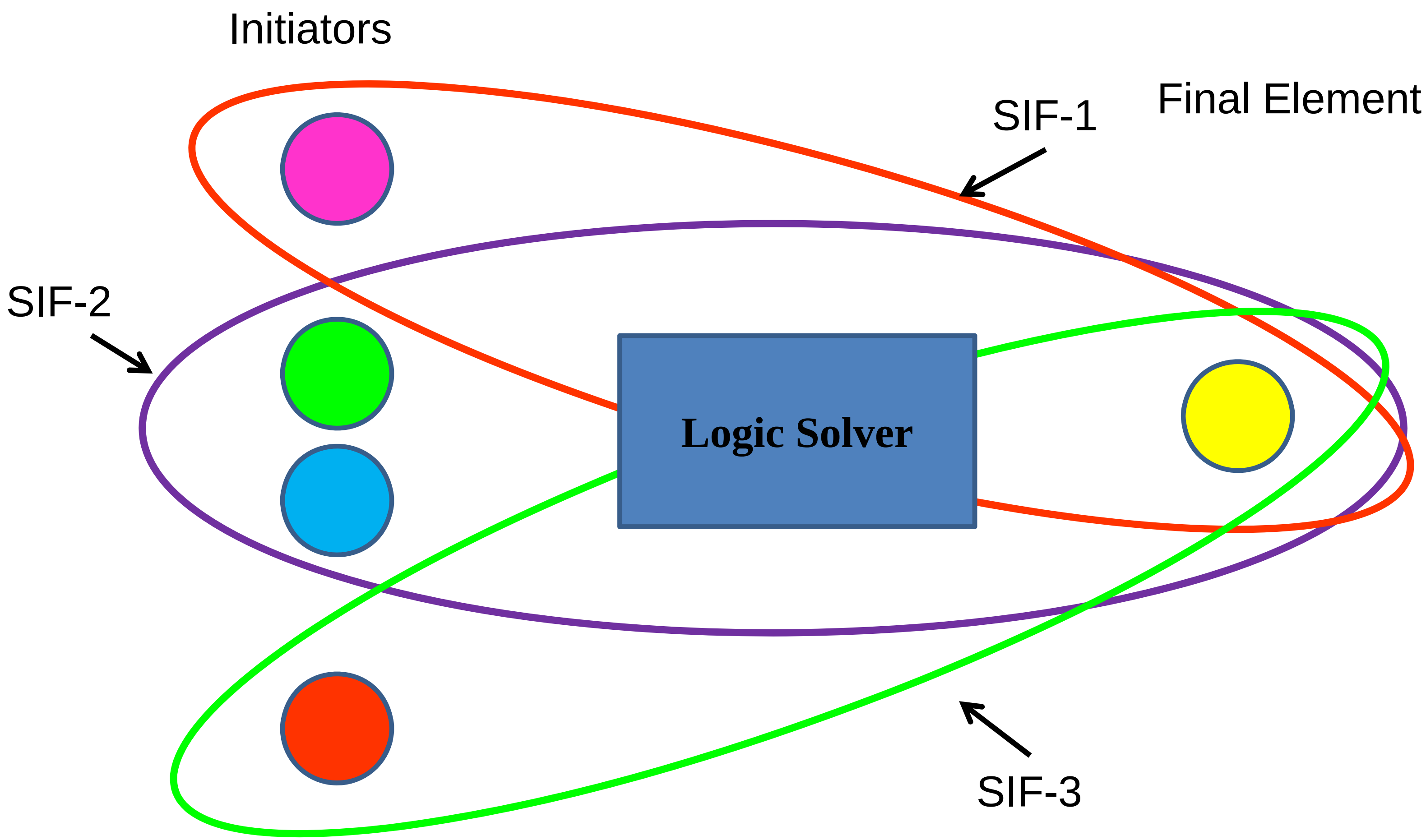
Measure



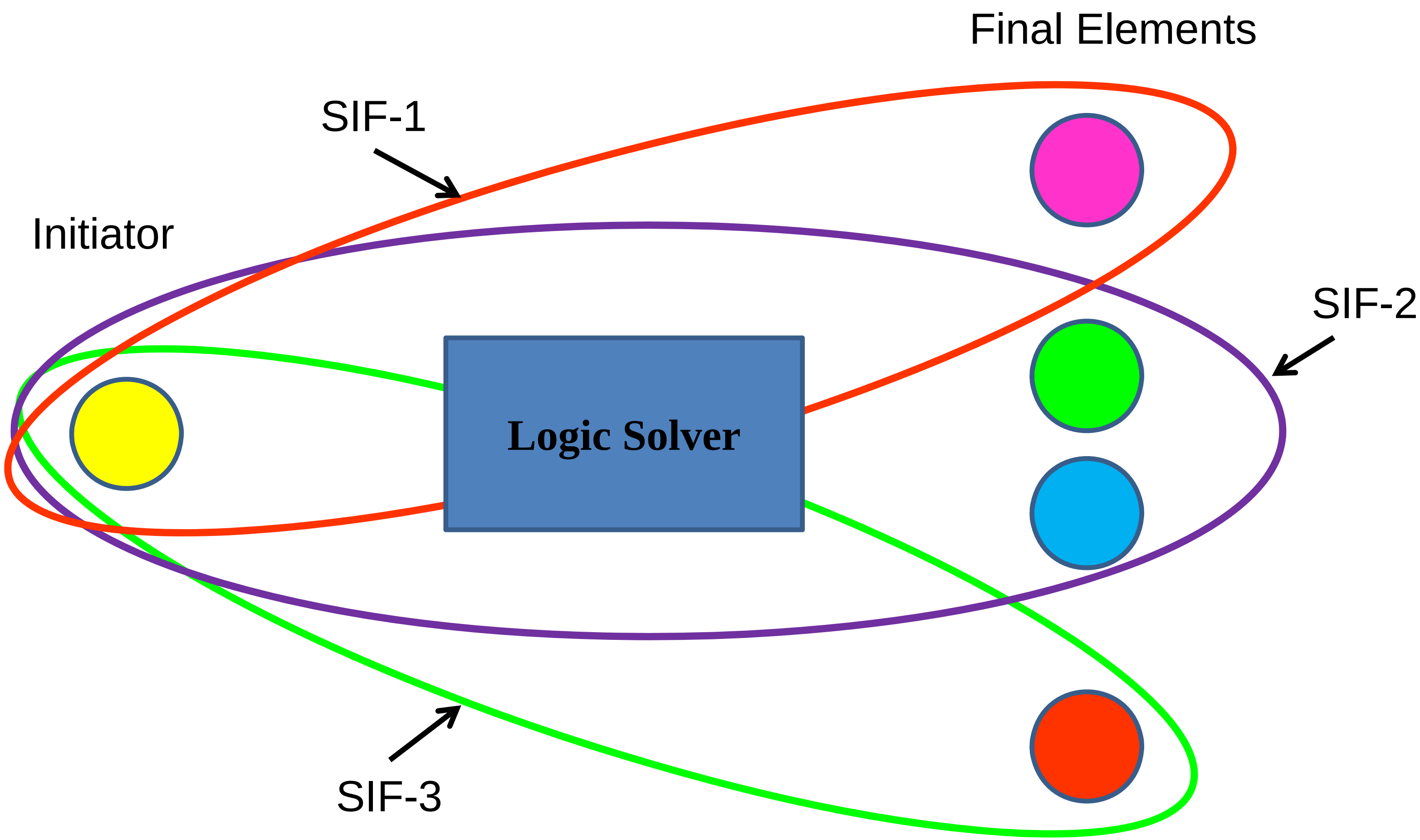
Response

Think

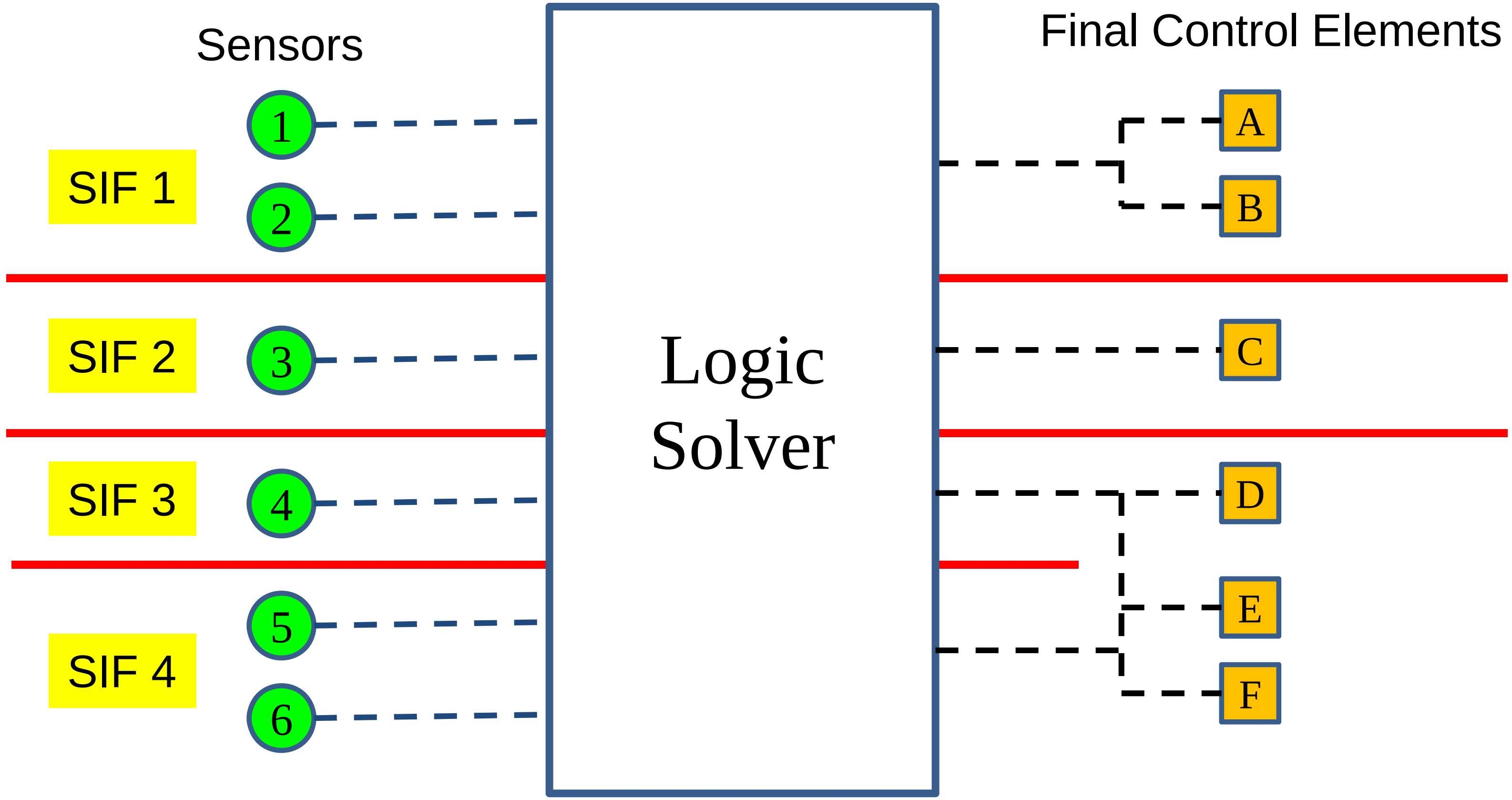
Multiple Initiators tripping one Final Element



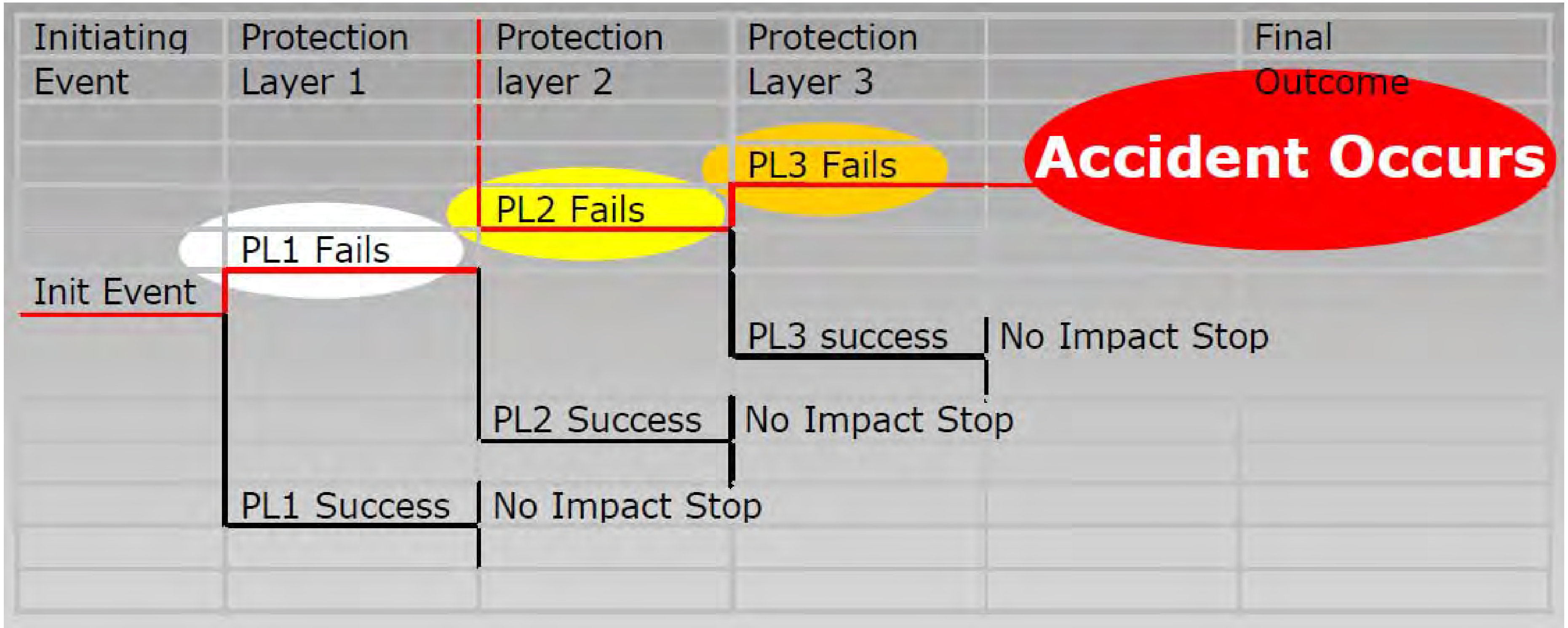
One Initiator tripping multiple Final Elements



Overall Safety Instrumented System showing SIFs



Assigning the SIL with Layer of Protection Analysis (LOPA)

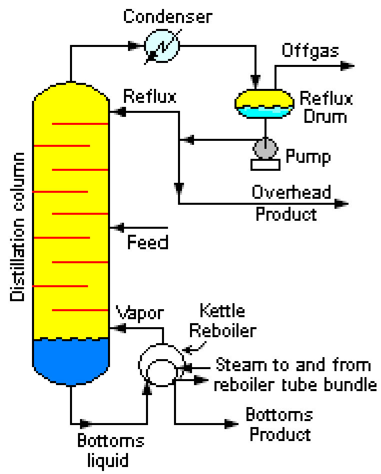


LOPA Example

An accident whose consequence is fire due to distillation column rupture with a root cause of loss of cooling water

The following layers of protection exist:

- Process designed to withstand loss of cooling water
- The operator responds to alarms and stops the process
- The column has a pressure relief valve
- Sources of ignition are controlled in the process area



PETRORISK MIDDLE EAST LIMITED – ABU DHABI

LOPA Example

Quantify the accident likelihood

– Cooling water failure likelihood is 4 per year

– Protection Layer PFD are:
  - Process design inadequate – PFD = 0.004
  - Operator response failure – PFD = 0.15
  - Relief valve failure – PFD = 0.1
  - Ignition source contacted – PFD = 0.3

LOPA Example

LOPA Solution

INIT EVENT	PL #1	PL #2	PL#3	PL#4	OUTCOME
Loss of	Process	Operator	Pressure	No	Fire
Cooling Water	Design	Response	Relief Valve	Ignition	
				0.3	1.8E-04
			0.1		Fire
		0.15			
	0.01				
4 /year					
					No Event

$$L = 4\ /year * 0.01 * 0.15 * 0.1 * 0.3 = 1.8 \times 10^{-4}/year$$

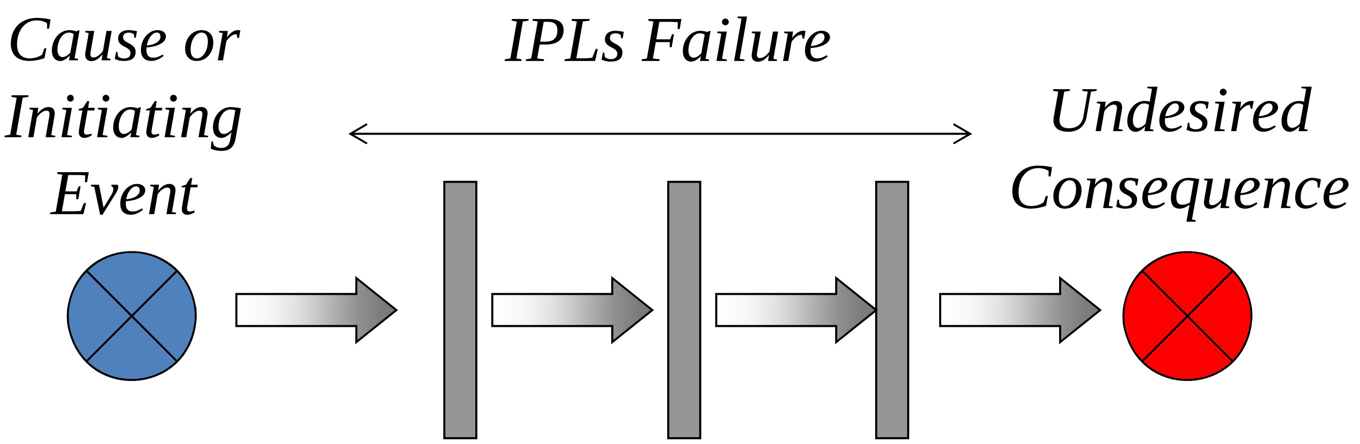
What is LOPA?

- 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



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

What is ***scenario*** ?

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

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

LOPA Five Basic Steps

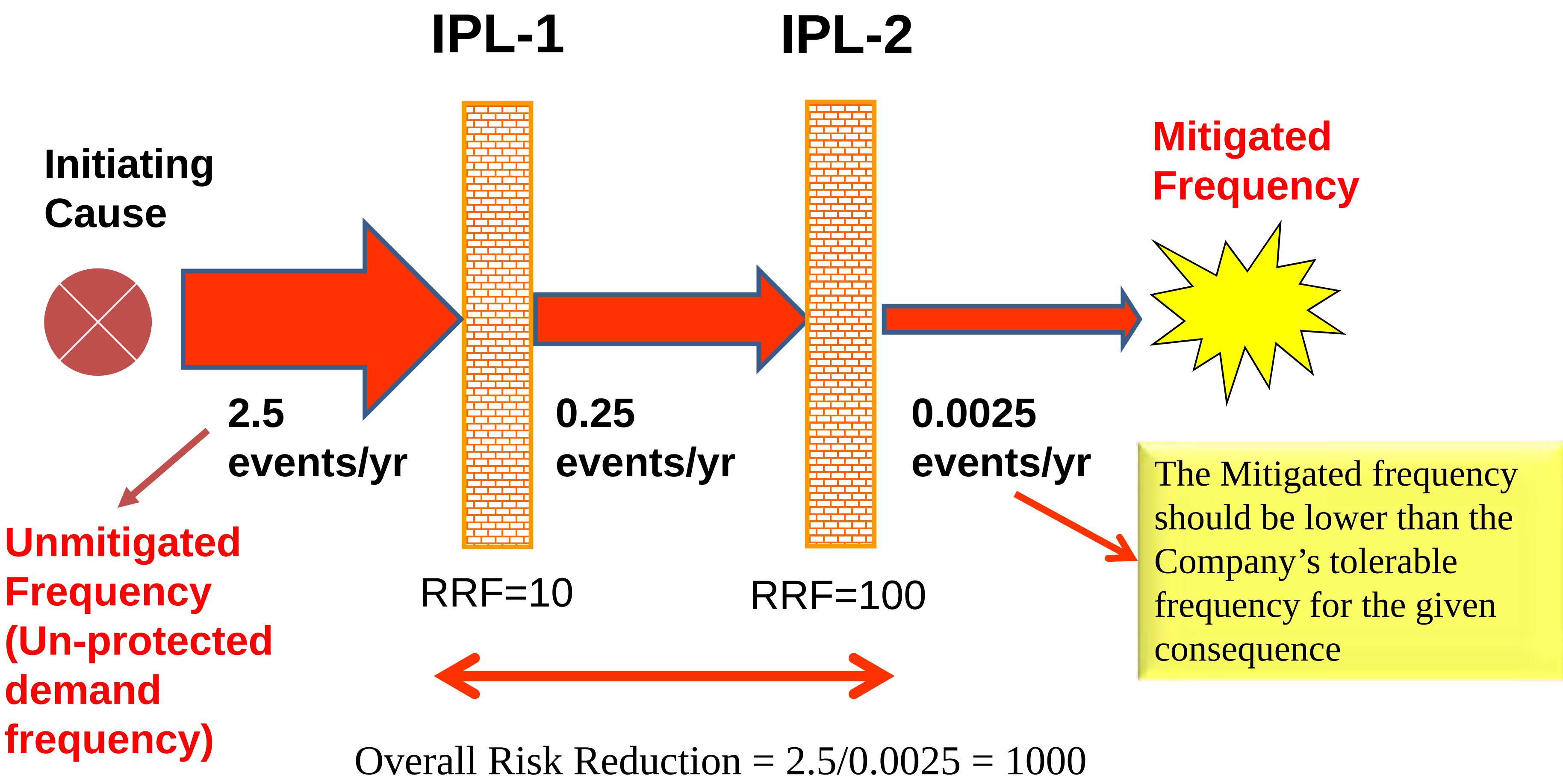
1. Scenarios identification.
2. Identify the ***initiating event*** of the scenario and determine the initiating event frequency (events per year).
3. Identify the ***IPLs*** and estimate the ***probability of failure on demand*** of each IPL.
4. Estimate the risk of scenario.
5. Compare the calculated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

PETRORISK
MIDDLE EAST LIMITED – ABU DHABI

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?

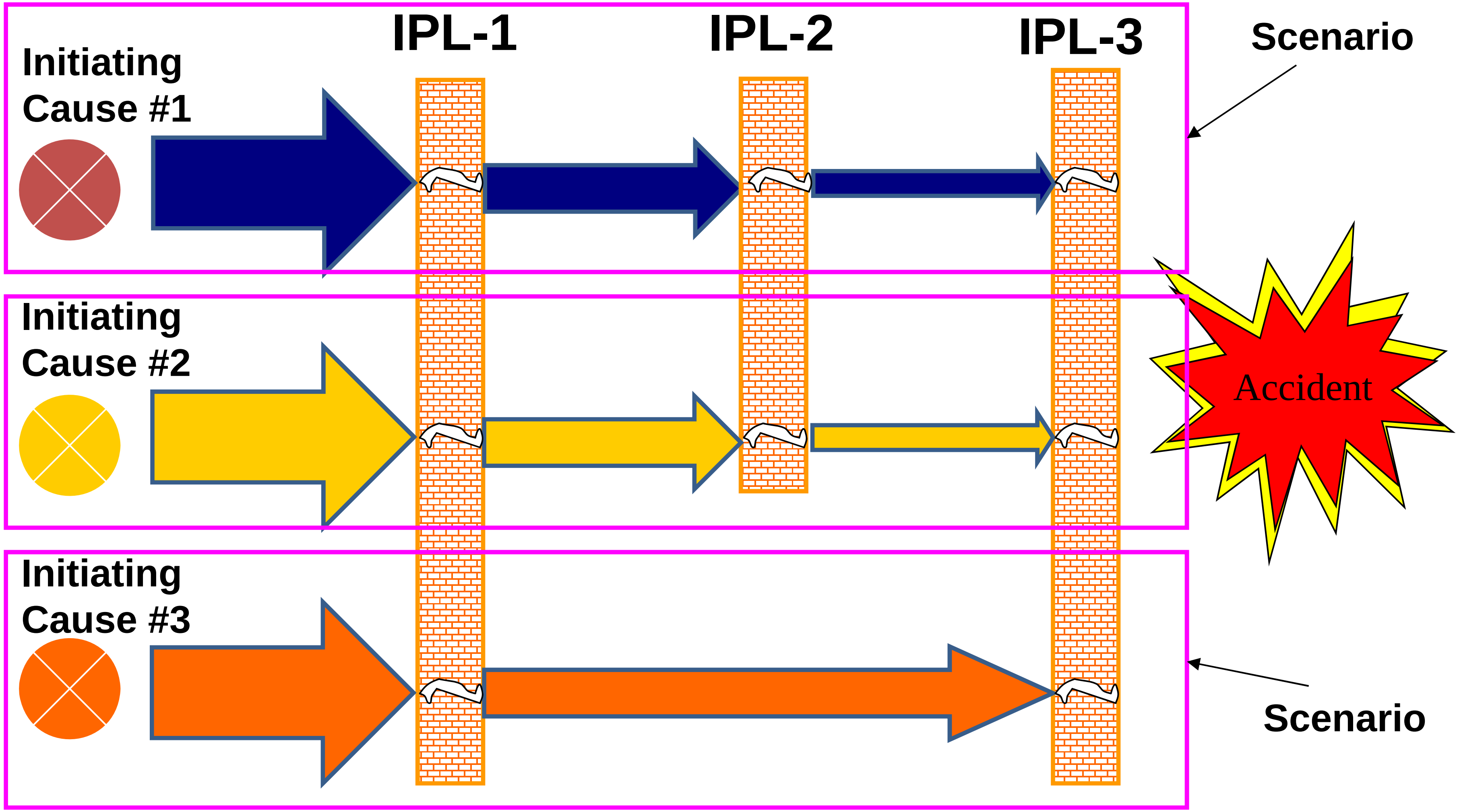
Basic Principle



IPL – Independent Protection Layer

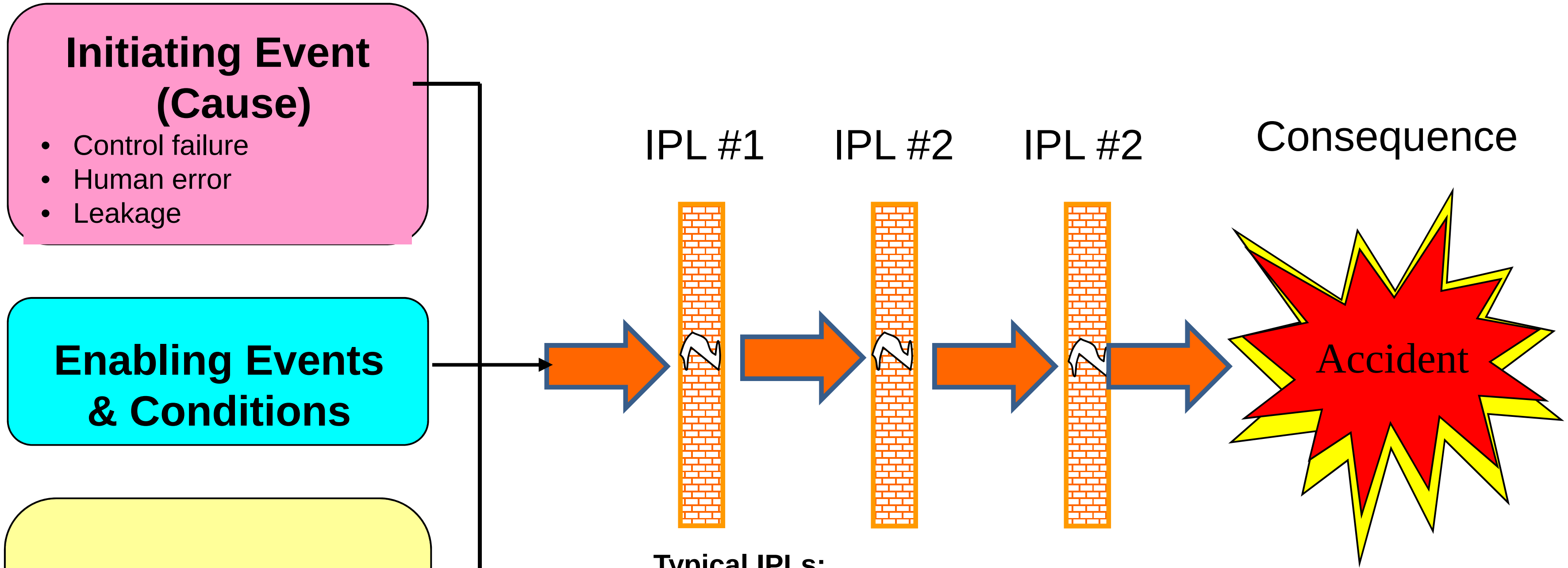
RRF – Risk Reduction Factor

Basic Principle



PETRORISK
MIDDLE EAST LIMITED – ABU DHABI

Components in a Scenario



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 LIMITED – ABU DHABI

Failures in Safety Instrumented System

Random Failures

A failure occurring at a random time, which results from one or more of degradation mechanisms.

Systematic Failures

A failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors.

Common cause Failures

The failure two or more units in a redundant system due to a common stress

Random Hardware Failures

A spontaneous failure of a hardware component at any given time

- Permanent – exist until repaired
- Dynamic – exists only under certain circumstances

IEC-61508 Approach

- Proactive measures to control systematic failures
- Hardware reliability study (PFDavg)

Common Cause Failures

The failure two or more units in a redundant system due to a common stress

Common Cause Failures are due to:

- Heat
- Humidity
- Chemical Corrosion
- Shock
- Vibration
- Electrical Surge
- Electrostatic Discharge
- Radio Interference
- Unexpected sequence of events
- Human Errors

Factors that affect Common Cause Failures

- Separation & Segregation (signal cables, logic subsystem channels, sensor & control elements having separate control electronics etc.)
- Diversity & redundancy (channel technology e.g. electronic & programmable electronic. MooN architecture, different sensing technologies, different designers etc.)
- Complexity, design, application, maturity & experience
- Assessment, Analysis and Feedback of data
- Procedures and Human Interface
- Competence, Training & Safety Culture
- Environmental Controls
- Environmental Testing

Systematic Failures

Examples of systematic failures:

- Safety Instrumented System design errors
- Hardware implementation errors
- Software errors
- Human interaction errors
- Hardware design errors
- Modification errors

The systematic failure rate is extremely difficult to estimate

Effective design, independent reviews, and thorough testing processes must be implemented to minimize the probability of systematic failures.

Functional Safety

A safety system is functionally safe if ….

Random, common cause and systematic failures do not lead to malfunctioning of the safety system and do not result in

- injury or death of humans
- spills to the environment
- loss of equipment or production

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

Failure Rate Data Collection and Sources

(1) Sampling

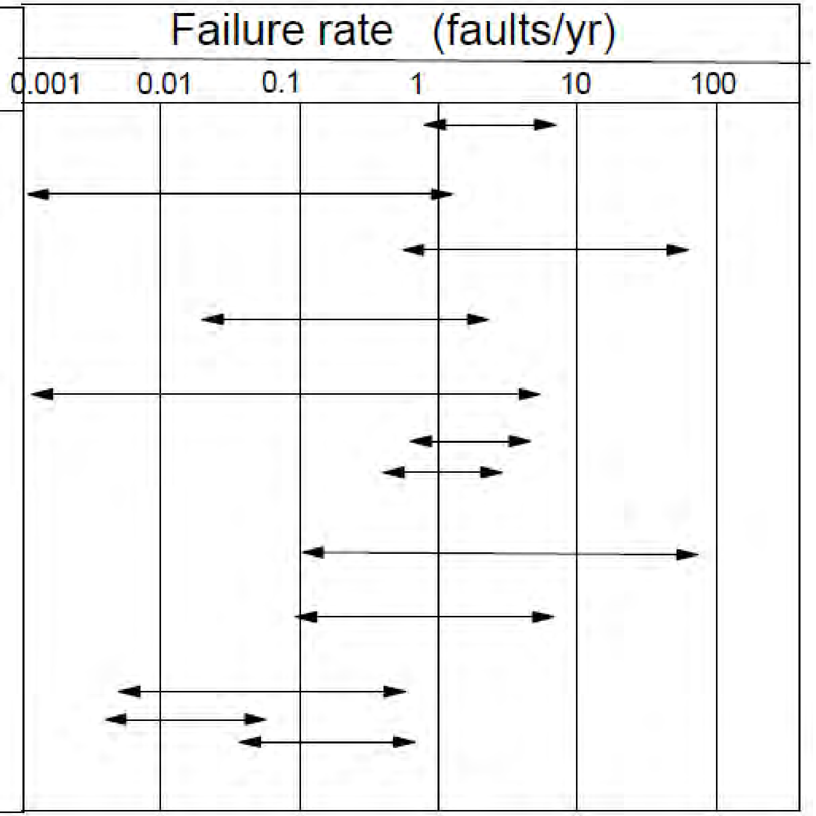
(2) Prediction

(3) Field data

Spread of Failure Rate Data

Spread of Failure Rates

Equipment	Failure mode
Boilers	All failures
Bursting discs	Spurious failure
Compressore (per casing)	All failures
Fans	All failures
Heat exchangers, coolers, etc	All failures
Instrumentation - control loop	All failures
- simple trip	All failures
Pumps - various	All failures
Turbines - various	All failures
Valves - non return	Stuck open
- pressure relief	Stuck shut (>150%)
	Lift light (<90%)



Typical Fault Rates used in The Assessment of Protective Systems

Equipment type	Total failure rates /year		
	Clean	Medium	Dirty
Temperature transmitter (electrical)	0.2	-	-
Flow element	0.1	0.2	0.4
Turbine flow element (3)	0.1	Do not use	
Flow transmitter	0.2	0.4	0.8
E/M meter	0.05	0.1	0.2
Analyser - measuring element	2.0	4.0	8.0
Pressure transmitter	0.2	0.4	0.8
Pressure switch (instrument air)	0.1	-	-
Pressure switch (process)	0.2	0.4	0.8
Level switch (float)	0.2	0.4	0.8
Radioactive level transmitter (fail high)	0.1	-	-
Radioactive level transmitter (fail low)	0.15	-	-
Radioactive level switch	0.015	-	-

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 Data

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

Frequency and Rate

Frequency is the number of times an event occurs in unit elapsed time.

Rate is the number of times an event occurs in unit working (on-line running) time.

Example – Failure Frequency

If there are two pumps A and B where each pump fails twice per year and runs all year .

Hence for each pump:
Failure frequency = failure rate = 2 /year

Frequency is the number of times an event occurs in unit elapsed time.
Rate is the number of times an event occurs in unit working (on-line running) time.

Example – Failure Frequency

Two pumps C and D; one working and one spare.

Assume each pump on average fails twice per year and runs for 50% of the time, in this case:

Failure frequency of *each* pump = 2 /year

Failure rate of *each* pump = 2 / 0.5 /year = 4/year

The failure rate is the number of times each of the pumps would fail if it ran for a full year.

Example – Failure Frequency

Pumps C and D, one running, one spare. Each pump fails suddenly twice per year. Repair takes 2 days per failure. On average each pump runs for 50% of time. How often will there be no spare pump available when the running pump fails?

The running pump (either C or D) fails a total of 4 times/year
There is no spare pump (either C or D) available for a total of
4 x 2 = 8 days/yr.
Hence, assuming the failures are independent and the failure rates are constant the frequency of no spare pump available when the running pump fails is given by the equation:
= (frequency of running pump failing) x (probability of no spare available)
= 4 x (8/365)
= 0.088 /year

Initiating Events Frequency Estimation from Plant Failure Data

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 events per year per compressor

PETRORISK MIDDLE EAST LIMITED - ABU DHABI

Initiating Events Frequency Estimation from Plant Failure Data

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?

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

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

= 0.0038 failures per year per valve

Mean Time To Failure – MTTF

The average successful operating time interval of a device, subsystem or system.

A module has an MTTF of 80 years for all failure modes. Assuming a constant failure rate, what is the total failure rate for all failure modes?

λ = 1 / MTTF = 1 / 80years = 0.0125 failures/year

λ = 1.43E-06 failures/hour

MTTR, Mean Time To Repair

The average successful repair time interval of a device, subsystem or system.

Mean Time Between Failures (MTBF)

The average time interval of one failure / repair cycle of a system. Applies only to repairable systems.

MTBF = MTTF + MTTR

Example:
Device reliability expressed with MTBF of 100 years
Then, failure rate = 1/100 failures per year
If a system has 300 such devices then:
= 300 x (1/100) = 3 device failures /year

Enabling Events / Conditions

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

Initiating Cause/Event **Enabling Event**

Example:

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 personnel in affected area
- Probability of fatal injury

Conditional Modifiers

Probability of Ignition

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

Take Probability of Ignition of 1.0 near furnaces, roads etc.

PETRORISK MIDDLE EAST LIMITED – ABU DHABI

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

Take Probability of Personnel Presence as 1.0 if personnel always present. For presence of 1 hr in the hazardous area per 8 hrs shift, probability of personnel presence will be 1/8=0.125

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

Take Probability of Injury as 1.0 if personnel will definitely be injured

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)
- 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)

PETRORISK MIDDLE EAST LIMITED – ABU DHABI

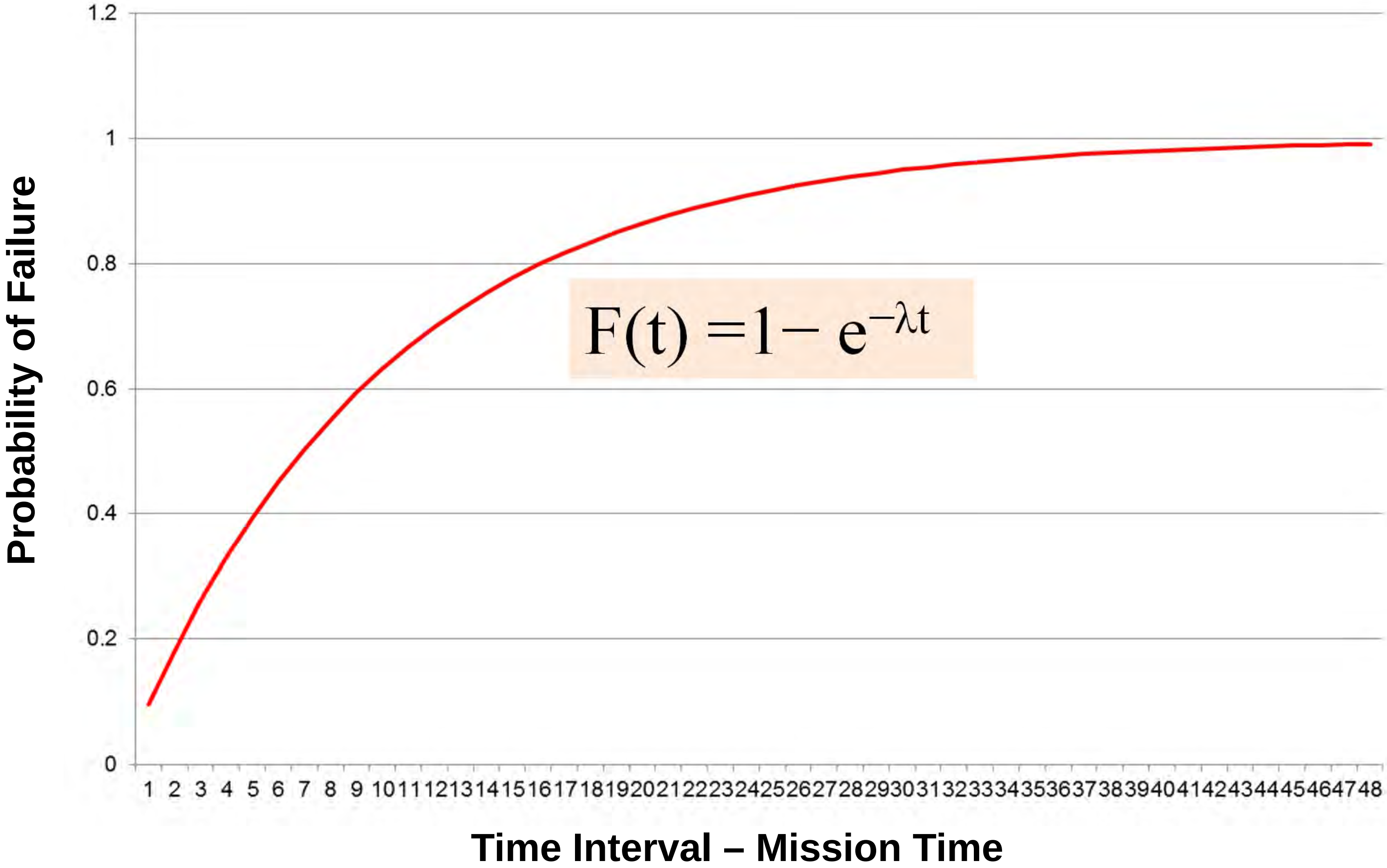
Probability of failure on demand (PFD)

When a piece of equipment or a system operates only on specific demand, the probability of failure is referred to as probability of failure on demand (PFD).

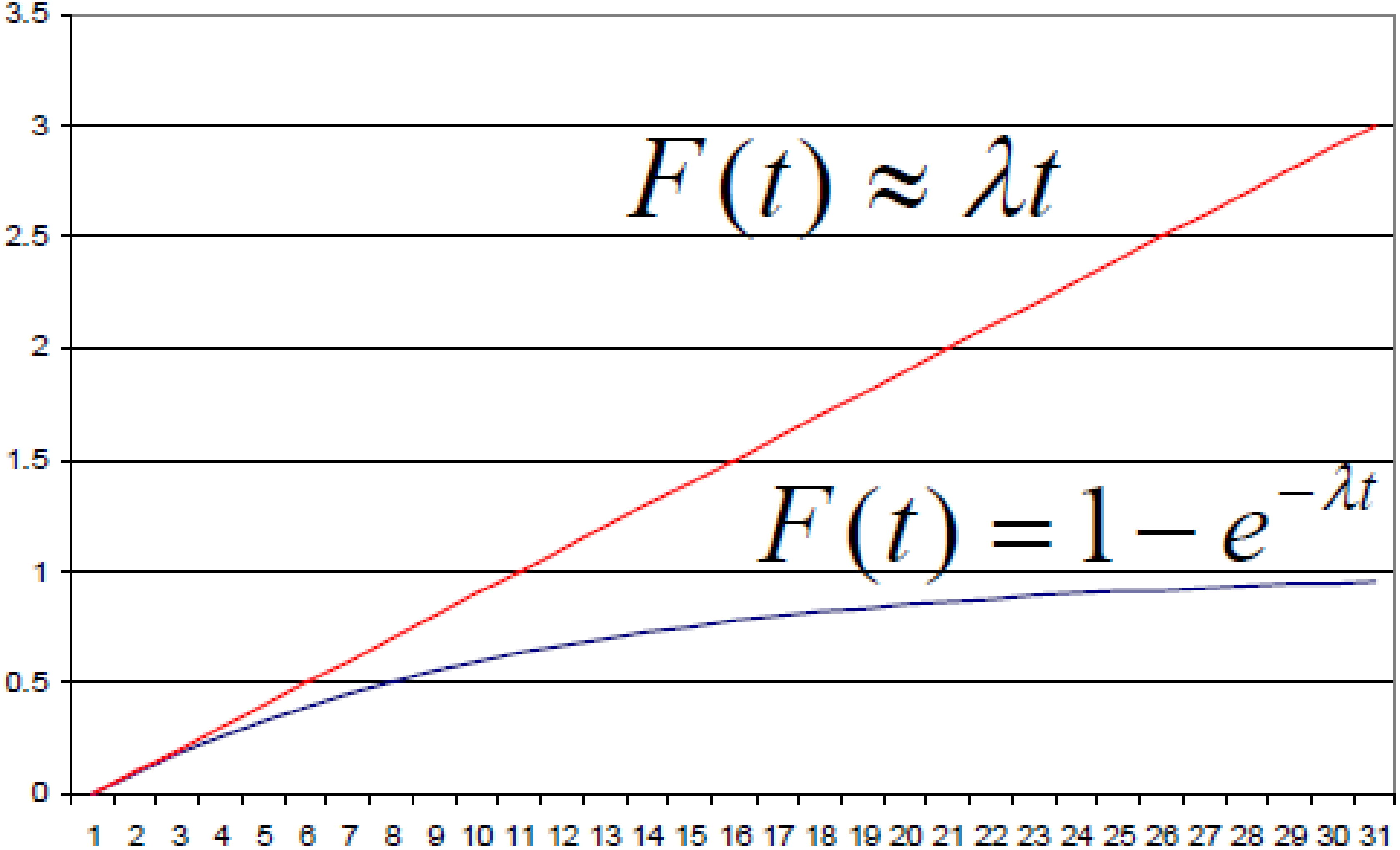
For a constant failure rate:

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

Probability of Failure

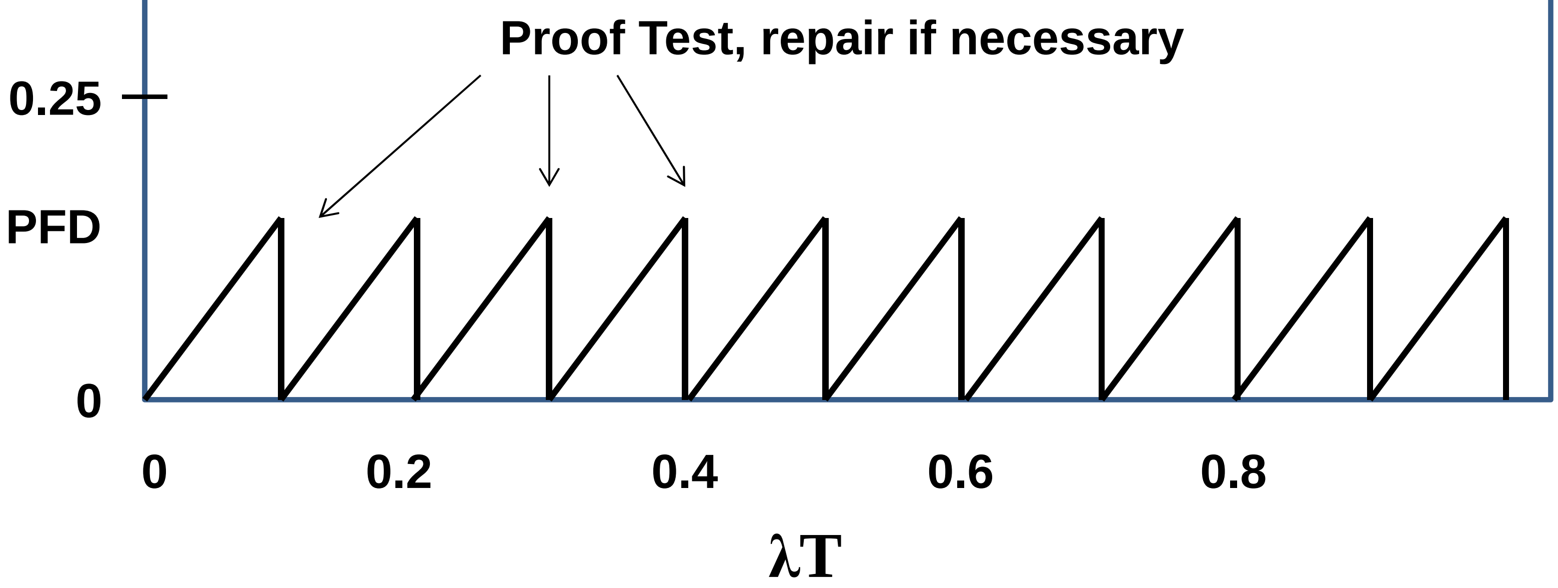


Probability of Failure on Demand



Effect of Proof Testing

Constant failure rate, working at time 0



The probability of having failed varies from 0 immediately after a proof test to λT immediately before a proof test, where T is the proof test period.

PFD Calculation

- **For protection layers that *cannot be repaired* during operation the *unreliability* function is used to calculate PFD**

- **For protection layers that are *inspected and repaired* during process operation, *unavailability* methods are used and provide an average PFD**

PETRORISK
MIDDLE EAST LIMITED – ABU DHABI

PFD - Unreliability

Given a constant failure event rate:

- **Unreliability (PFD)**
  = 1 - Exp (- failure event rate * time interval)

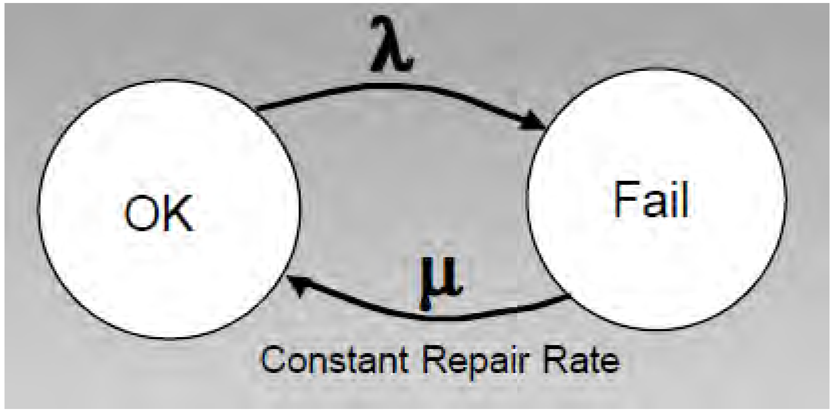
$$F(t) = 1- e^{-\lambda t}$$

(For protection layers that *cannot be repaired* during operation)

PETRORISK MIDDLE EAST LIMITED - ABU DHABI

PFD - Unavailability

MTTF = 1/λ
MTTR = 1/μ



U = μ / λ + μ

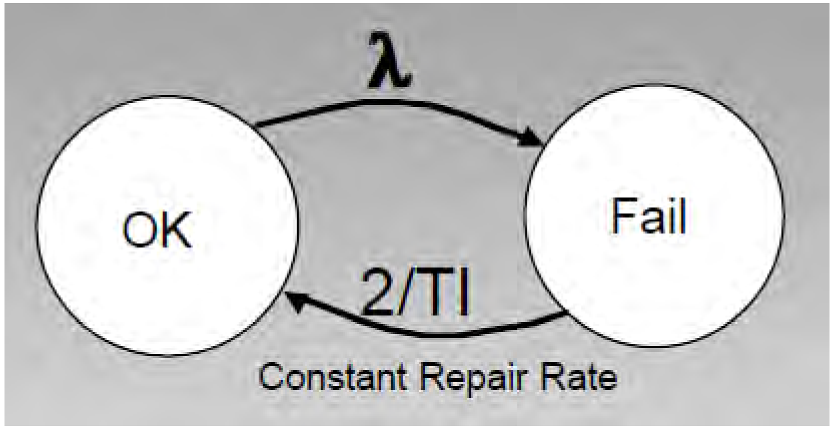
For repairable systems, the PFD is calculated using an unavailability function.

PFD - Unavailability

$U = \mu / \lambda + \mu$

$MTTF = 1/\lambda$

$MTTR = 1/\mu$



$U = PFDavg = (\lambda * TI) / 2$

PFD – Data Needed

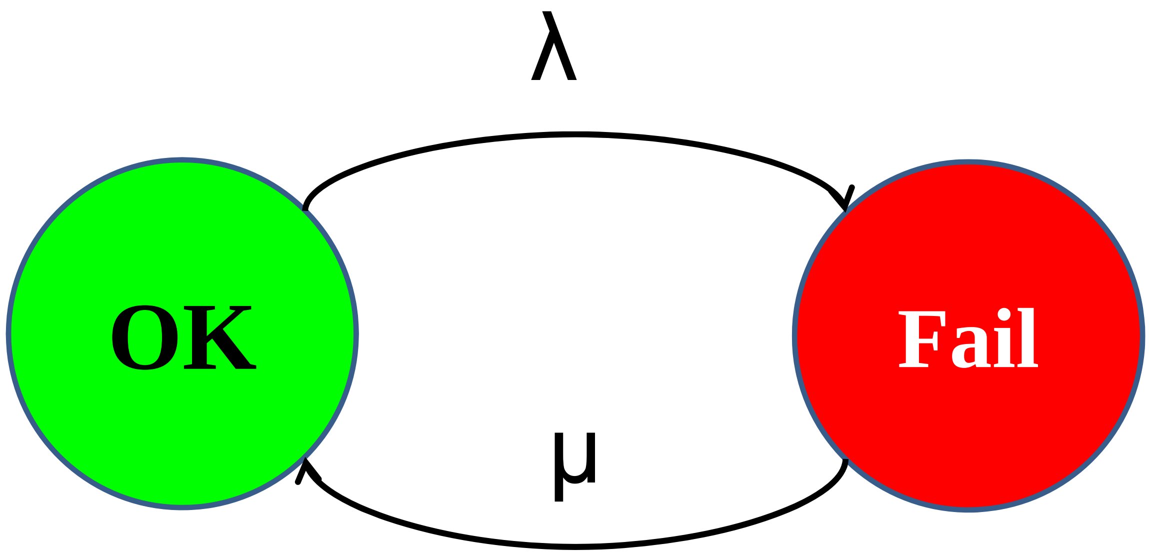
Regardless on the method used, PFD calculations require:

1. **Failure rate data for all equipment in a protection layer**
2. **Repair rate data for equipment that is on-line repairable**
3. **Test & Inspection Interval for all equipment**
4. **Operating Time Interval for non-repairable equipment**

Availability & Unavailability

$MTTF = 1 / \lambda$

$MTTR = 1 / \mu$



Constant Repair Rate

$A = MTTF / MTTF + MTTR$

$U = MTTR / MTTF + MTTR$

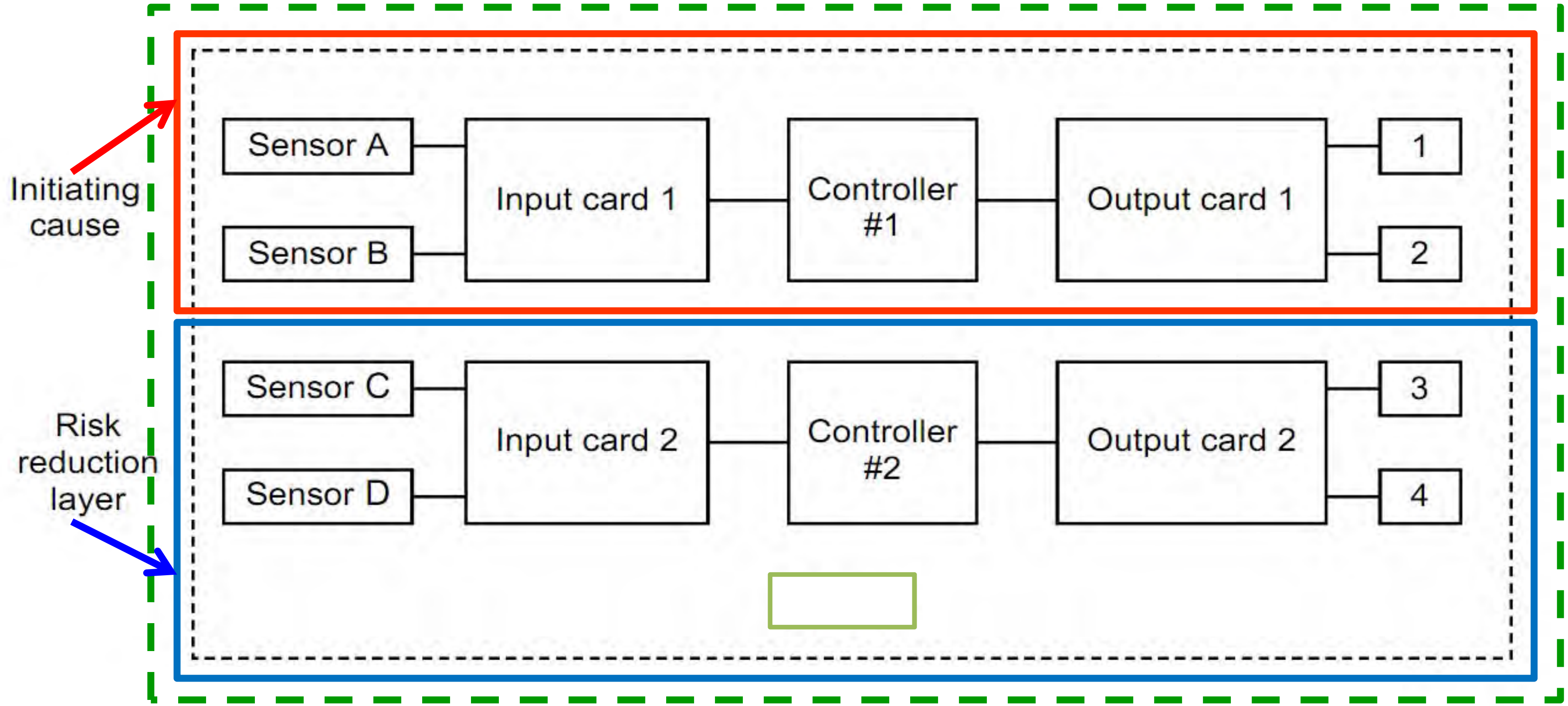
How to calculate Unavailability

$$U \approx \lambda \times T = T / MTBF$$

T is the average down-time per failure
λ = constant failure rate

Each failure causes downtime T. Therefore, the system is unavailable for time T out of total time MTBF. The fraction of time the system is not available is therefore T/MTBF.

Independence between Initiating Cause & IPL



BPCS

Definitions

DEMAND

The requirement for a Protective or stand-by system to operate owing to an abnormal process condition or process equipment failure.

DEMAND RATE

The rate at which demands occur (usually per year).

Definitions

SPURIOUS TRIP

A protective system operating, without a demand, as a result of a fail safe fault in the system.

HAZARDOUS EVENT RATE

The rate at which the hazardous event occurs, usually expressed as per year with potential to cause loss, damage or undesirable effect on plant, equipment, product, people, the environment or profit

Definitions

Probable Loss of Life (PLL)

If there were 1,058 boiler explosions and as a result of these boiler explosions there were 12 fatalities and 73 injuries. Estimate the consequence of a boiler explosion in terms of fatalities and injuries?

For Fatality:

Probable Loss of Life = 12 / 1,058 = 1.1×10^{-2}

(number of fatalities per incident)

For Injury:

Probable Injuries = 73 / 1,058 = 6.9×10^{-2}

(number of injuries per incident)

PETRORISK MIDDLE EAST LIMITED - ABU DHABI

Demand Rate

The demand rate is established by estimating the frequency at which each initiating event may occur and totalling all these frequencies.

If independent protection layers other than the IPF under study are present, these are taken into account.

Credit may be taken for other independent protection layers (IPLs) if they comply with the requirements. The IPLs may serve to prevent the hazardous event (top event) or mitigate the consequences.

DEMAND Tree & FAULT Tree

The most common technique for analysing HOW a hazardous event can occur is **fault tree analysis**. The first step is usually to draw up a **demand tree** which shows all the basic events that could lead to the hazardous event. *This excludes all protective systems and operator interventions to correct faults.*

The **fault tree** for the hazardous event is produced by taking the demands identified in the demand tree and including the effects of the protective systems and the operator interventions by applying *frequencies* & *probabilities.*

Hazardous Event Rate

It is the number of times per year that the "top event" (i.e. the hazardous event) occurs. This is the ultimate objective of quantification of the fault tree. It is calculated by combining event frequencies and probabilities but when protective systems are involved some different procedures are required to handle the special probability, PFDavg.

Hazardous Event Rate =
Demand Rate on Protective System x Protective System Failing to Operate (PFDavg)

$$H = D \times PFDavg$$

(Applicable if D.T<1 & λ.T < 1)

PETRORISK MIDDLE EAST LIMITED - ABU DHABI

Hazard Rate - Example

A relief valve is tested every two years. If the demand rate, D, is 0.1/year and the fail to danger fault rate of the relief valve is 0.01/year, what is the hazardous event rate for the relief valve failing to prevent overpressure of the equipment?

PFDavg = 0.01 x 2 / 2 = 0.01

Before evaluating the hazardous event rate check the limiting condition:
D x T = 0.1 x 2 = 0.2 (which is much less than 1, ok)
Hence:
H = D x PFDavg
    = 0.1 x 0.01 = 0.001 /year
In other words the hazardous event will occur every l000 years on average.

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

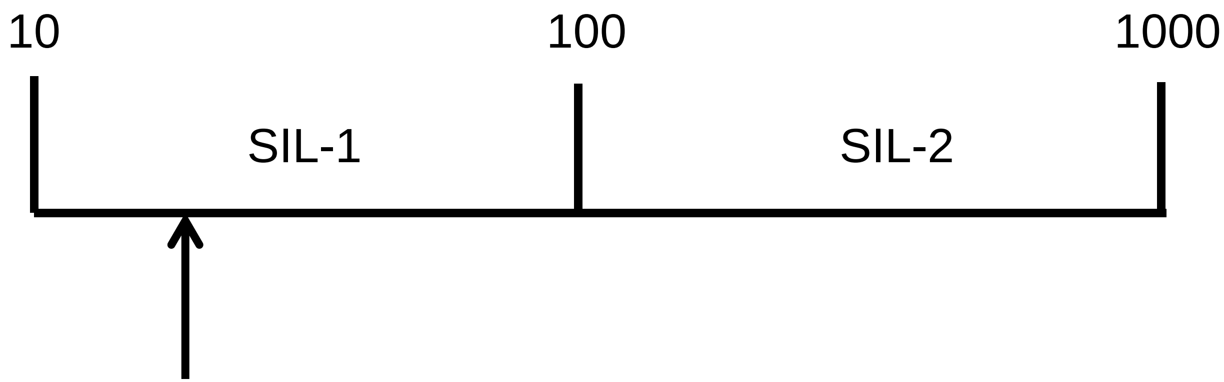
SIL Classification

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

Target vs Selected SIL Rating

For example, the required risk reduction from a safety instrumented function needs a RRF target of 20



RRF Target = 20 (PFDavg=0.05)

PFDavg = 1/RRF

Device Suitability for Application

Even if equipment is "certified" for IEC 61508 compliance, it still cannot be used unless an assessment is made by the users that the technology the device employs is suitable for the application (e.g. magnetic vs vortex flow meters)

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

Tolerable Risk Level and Consequence Receptors

Examples:

- Maximum risk tolerance 0.0005 fatal accidents per person per year
- 0.005 injuries per person per year
- 0.01 significant environmental release per plant per year
- $500,000 in business loss per plant per year, etc.
- Valuing loss of life at $10,000,000

Methods of Consequence Analysis

- Consequences can require extremely involved analysis
  - Fire
    - How much material
    - What kind of fire
  - Explosion
    - Pressure energy
    - Chemical energy
  - Toxic release
    - Concentration limits
    - Weather conditions

Results of Consequence Analysis

- Different potential outcomes identified
- Magnitude of each outcome from perspective of each receptor
  - Personnel
  - Environment
  - Financial
- Group consequence components according to safety instrumented function capable of preventing them

Consequence Results: Column Rupture Case

single variable approach

- The consequences of a column rupture are determined as follows:
  – Personnel: 3 fatalities (3*10 M$), 15 injuries (15*1.0 M$)
  – Environment: no exceptional toxic release (0 $ no fine), internal clean-up activities (0.5 M$)
  – Equipment: new column/installation (4.5 M$)
  – Business Interruption: 25% lost production 3 months (50 M$)
  – Business Liability: direct customer contract losses (25 M$)
  – Company Image: no additional cost not already considered
  – Lost Market Share: customers go to competitor(s) (15 M$)

- Total column rupture hazard consequence is 140 M$

Considering All the Impacts

- **Outcomes must be expressed in the same terms as the tolerable risk limits**
  - For the single variable method, this involves the conversion factors
- **Risk integral approach**
  - Risk integral approach can also be applied to the personnel and financial components of risk independently of each other

Risk Integral Definition

Risk integrals are a measure of the total expected loss

A summation of likelihood and consequence for all potential loss events

Risk Integral Equation

The nominal equation for the risk integral is:

$$RI = \sum_{i=1}^{n} C_i F_i$$

RI = risk integral
N = number of hazardous events
C = consequence of the event (in terms of fatalities for loss of life calculation)
F = frequency of the event

Risk Integral Application

- Risk integrals require a single loss variable
- Can be across all receptors converted to financial terms
- Can be across financial receptors only in monetary cost terms
- Can also be across personnel receptors only in equivalent or probable loss of life (PLL) terms
  - PLL can take on fractional values

Risk Integral Advantages

Risk integrals are a measure of the expected loss

- **A summation of likelihood and consequence for all potential loss events for the SIF and category in question**

Advantages of risk integral targets:

- Risk is a single number, ideal for decision-making
- Considers multiple fatality events
- Diverse risks expressed on uniform basis, essential for cost-benefit analysis

Risk Integral Personnel Example

Consider the case where the following results are available from the consequence and likelihood analyses for a group of outcomes that can be prevented by the single SIF:

Outcome	Probable Loss of Life (PLL)	Frequency Events per year
Vessel rupture with pool fire	0.5	0.1
Vessel rupture with flash fire	1	0.1
Vessel rupture with explosion	6	0.01
Vessel rupture with spill only	0.01	0.2

What is the risk integral for that particular SIF in terms of PLL per year?

Risk Integral Personnel Example

Outcome	Probable Loss of Life (PLL)	Frequency Events per year	Risk Component PLL per year
Vessel rupture with pool fire	0.5	0.1	0.050
Vessel rupture with flash fire	1	0.1	0.100
Vessel rupture with explosion	6	0.01	0.060
Vessel rupture with spill only	0.01	0.2	0.002
Total Risk Integral			**0.212**

Multiplying each consequence by its corresponding frequency and summing the results at the bottom right gives the total risk integral for this pressure relief SIF of:

PLL = 0.21 fatalities per year

Single Event Risk Example

- Using the consequence and likelihood values determined for the single event column rupture and explosion hazard, calculate the inherent risk.

  - **Consequence = 140 M$**
  - **Likelihood = 2.85 x 10-4 per year**

Risk = Consequence * Likelihood

Inherent risk = 140 M$ * $2.85*10^{-4}$ /yr = 39,900 [US $/year]

PETRORISK MIDDLE EAST LIMITED – ABU DHABI

What Is the Required Risk Reduction?

Now the required risk reduction factor (RRF) can easily be calculated

Input parameters are:

– The unmitigated risk before any safety system

– The established tolerable risk level

$$RRF = \frac{\text{unmitigated risk}}{\text{tolerable risk}}$$

It is important to make sure that the inherent risk or risk integral and tolerable risk are expressed in the same units.

Risk Reduction Example 1

Given the heated vessel pressure relief SIF example with its PLL of 0.21 fatalities per year and a tolerable risk level of 0.001 fatalities per year, what is the required risk reduction?

$$RRF = \frac{\text{unmitigated risk}}{\text{tolerable risk}}$$

$$RRF = \frac{0.21 \text{ PLL per year}}{0.001 \text{ PLL per year}} = 210$$

Risk Reduction Example 2

A SIF is being considered to prevent the column rupture and explosion:

- **Consequence = 140 M$ (Including personnel, environment, equipment, etc.)**
- **Likelihood = 2.85*10-4 /yr (After accounting for all layers of protection)**

(A) A low-cost, low-performance SIL 1 SIF can provide a risk reduction factor of 10 for $5,000 per year net cost

(B) A higher-cost, higher-performance SIL 2 SIF can provide a risk reduction factor of 100 for $20,000 per year net cost

Which system should be selected?

Risk Reduction Example 2

- This example can be solved by calculating the annual cost associated with the risk of each option.
- For the case with no safety system, the cost of the hazard is $39,900 per year
- With the first case low-cost system, the RRF of 10 reduces the hazard cost to $39,900/10 = $3,990 per year, while the system itself adds $5,000 per year for a total $8,990 overall annual cost or a net savings of $30,910 relative to no safety system

Risk Reduction Example 2

Considering the second option in the same way as the first:

- For the case with no safety system, the cost of the hazard is $39,900 per year
- With the second case higher-cost, higher-performance system, the RRF of 100 reduces the hazard cost to $39,900/100 = $399 per year, while the system itself adds $20,000 per year for a total $20,399 overall annual cost or a net savings of $19,501 relative to no safety system

Option	Cost of Risk	Cost of System	Total Cost	Total Savings
Do nothing	$39,900	$0	$39,900	**$0**
SIL 1 SIF	$3,990	$5,000	$8,990	**$30,910**
SIL 2 SIF	$399	$20,000	$20,399	**$19,501**

Thus the SIL-1 SIF is the best option, with the greatest savings of ~$31,000 per year relative to doing nothing.

PETRORISK
MIDDLE EAST LIMITED - ABU DHABI

Multiple Receptors per SIF

Occasionally a set of tolerable risk levels and risk estimates gives different risk reduction factors depending on the personnel, environmental, or financial receptors considered

- **Personnel RRF = 1000**
- **Environmental RRF = 300**
- **Financial RRF = 150**

Choose highest RRF = 1000 for specifying the system

SIL Assignment

- SIL selection is performed based on the RRF calculated for the SIF

- For the heated vessel case, the RRF = 210

- Target SIL = SIL 3
  (The minimum risk reduction for SIF of 1000 guarantees that any SIL 3 system will achieve the required risk reduction factor)

Safety Integrity Level	Probability of failure on demand, average (Low Demand mode of operation)	Risk Reduction Factor
SIL 4	>=10^{-5} to <10^{-4}	100000 to 10000
SIL 3	>=10^{-4} to <10^{-3}	10000 to 1000
SIL 2	>=10^{-3} to <10^{-2}	1000 to 100
SIL 1	>=10^{-2} to <10^{-1}	100 to 10

Individual & Societal Risk

Individual risk is the frequency at which an individual may be expected to sustain a given level of harm from the realization of specified hazards.

Societal risk is the relationship between the frequency and the number of people suffering from a specified level of harm in a given population from the realization of specified hazards.

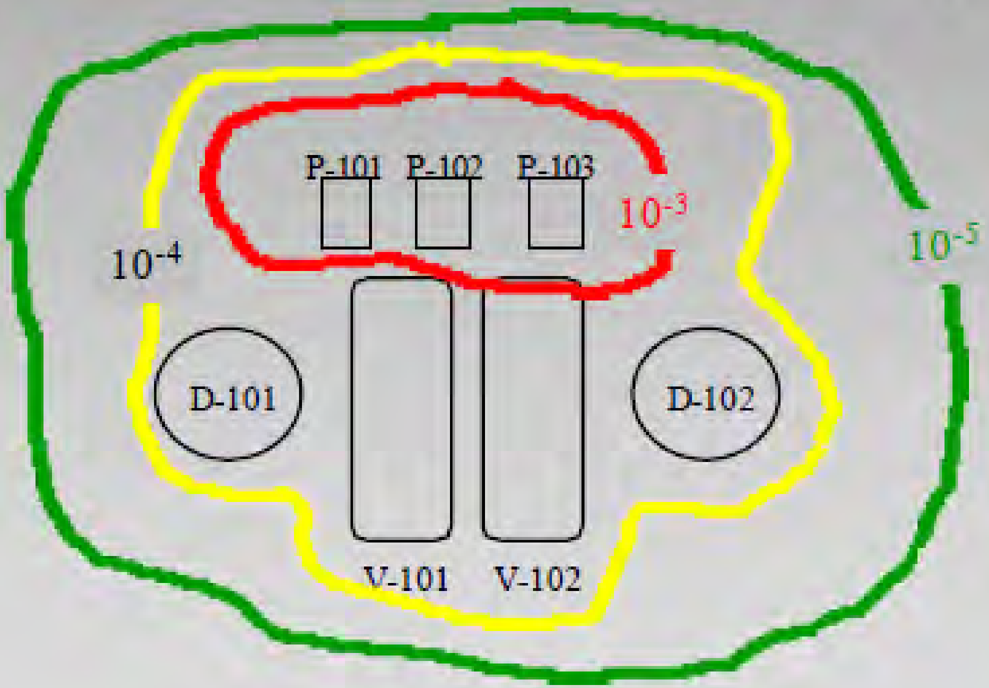
Societal Risk

Societal risk is the relationship between the frequency and the number of people suffering from a specified level of harm in a given population from the realization of specified hazards.

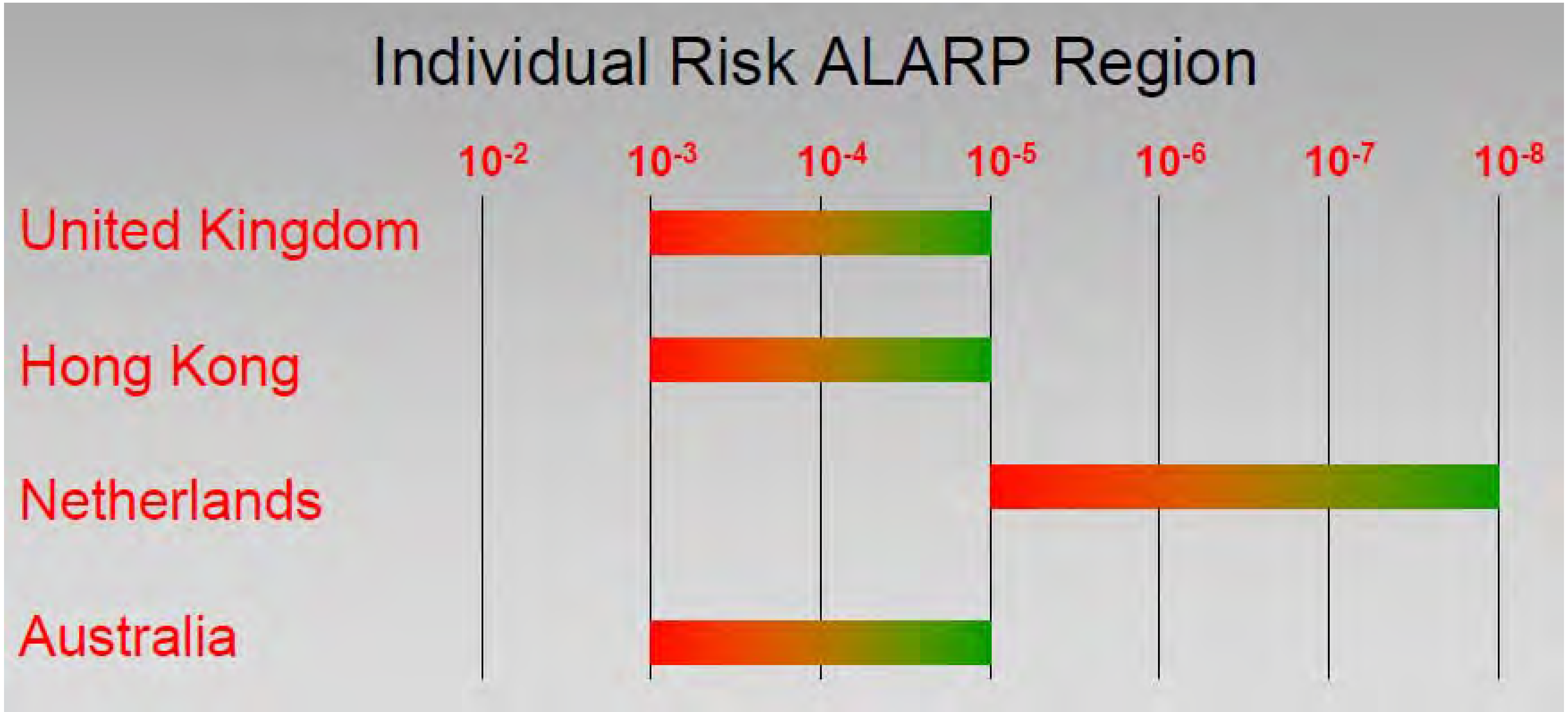
- **Typically shown as an F-N Curve of number of fatalities plotted against cumulative frequency**
- **Typically used by government for large-scale disasters; not often used in SIL selection risk analysis**

Geographic Risk

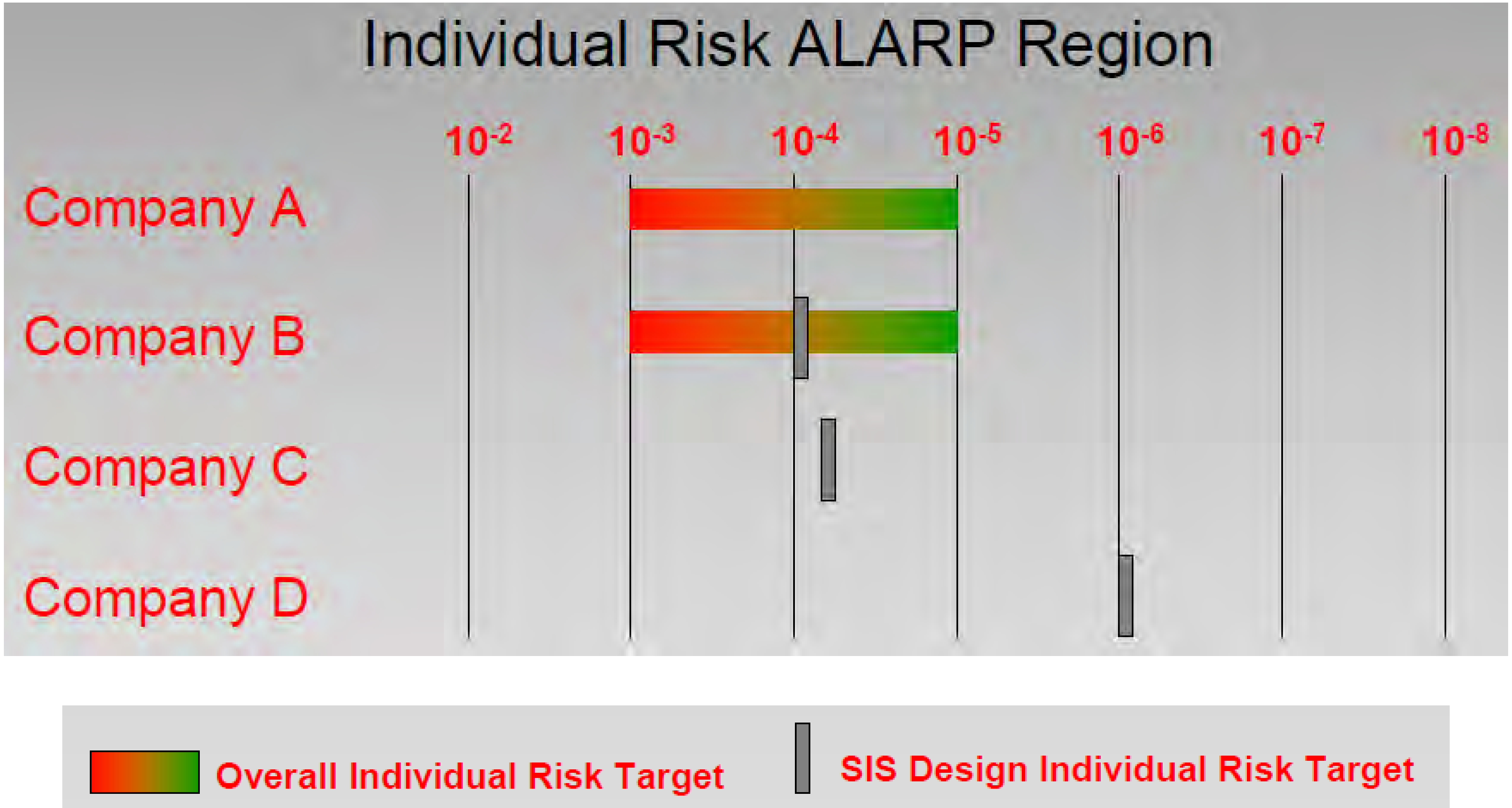
Geographic risk is a measure of the probability that an event will occur in a specific geographic location.



Tolerable Risk Benchmarks: Government



Tolerable Risk Benchmarks: Industry



Tolerable Frequency Data of a Company

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.

Initiating Event & Consequence

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

Environ-mental

Asset

Reputation

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

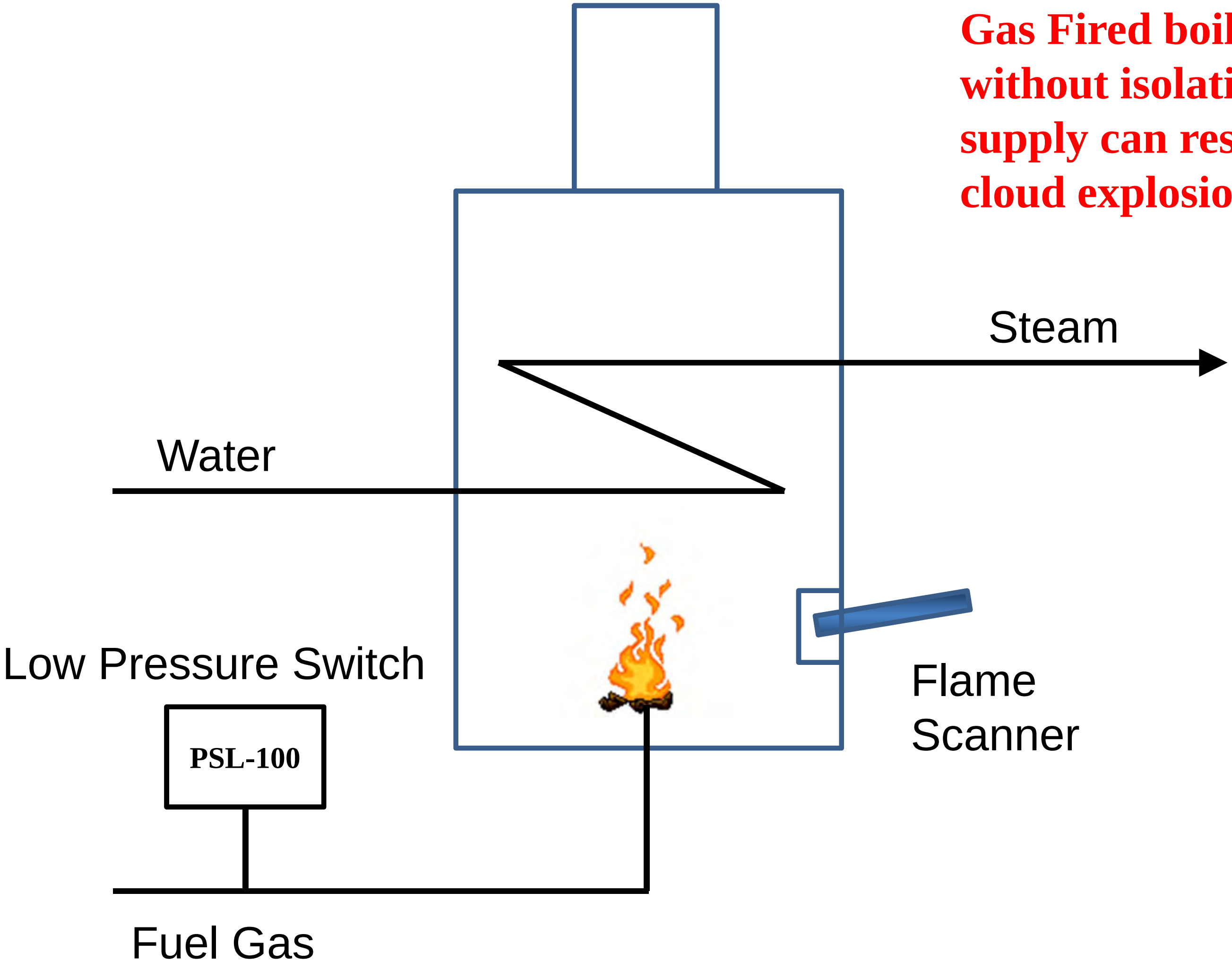
It would be wrong to take inverse of 3.3E-03, which would be 300 years, and say that a smoker would die every 300 years

PETRORISK MIDDLE EAST LIMITED - ABU DHABI

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

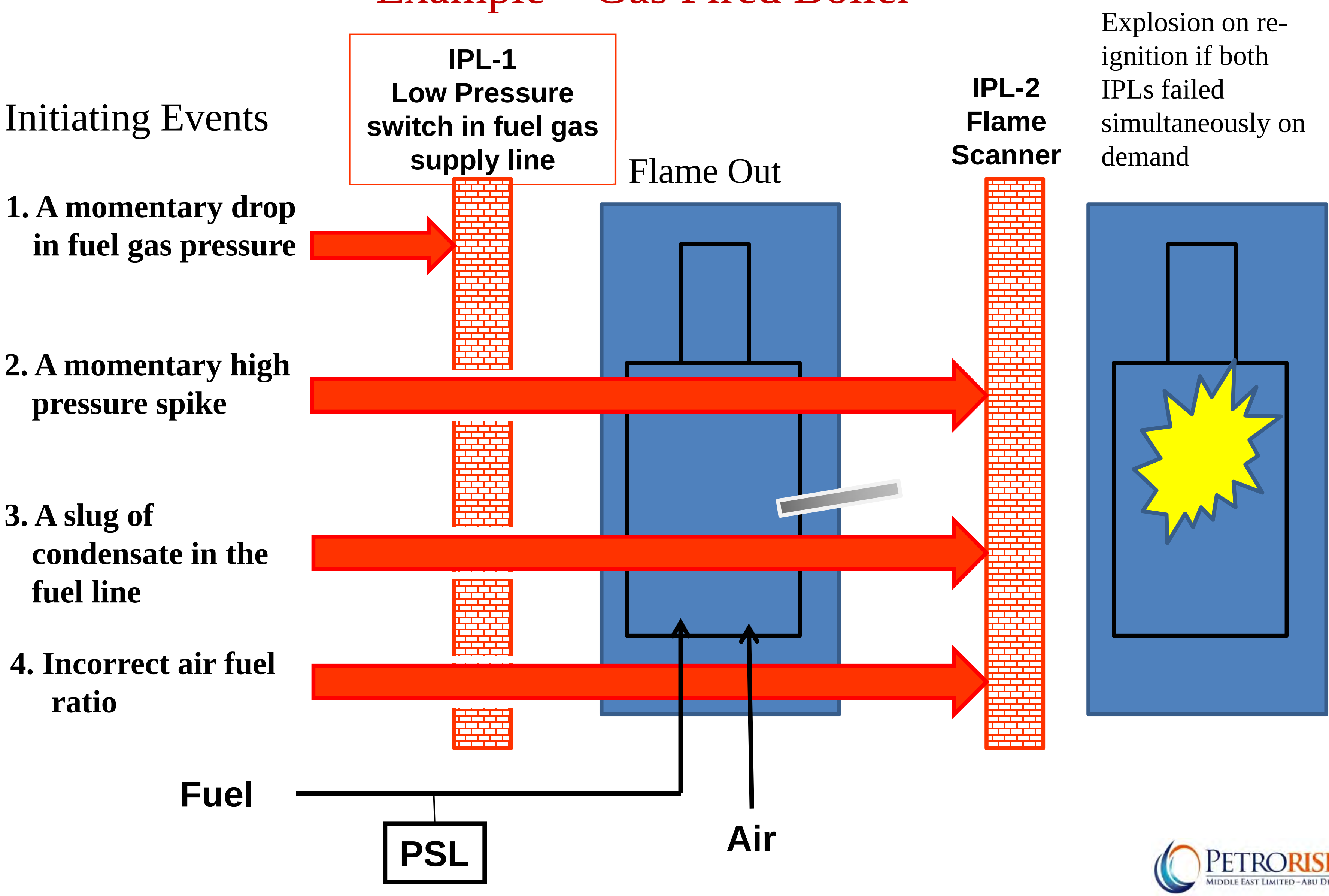
2. A momentary high pressure spike

3. A slug of condensate in the fuel line

4. Incorrect air fuel ratio

Effective & Non-Effective IPLs

Example – Gas Fired Boiler



Effective & Non-Effective IPLs

Example – Gas Fired Boiler

Initiating Event	IPL - 1 Low Pressure Switch on Fuel Supply Line	IPL-2 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

Layer of Protection Analysis (LOPA)

A variation of Event Tree Analysis

– More structured

– Like event tree analysis, the initiating event starts the chain of events

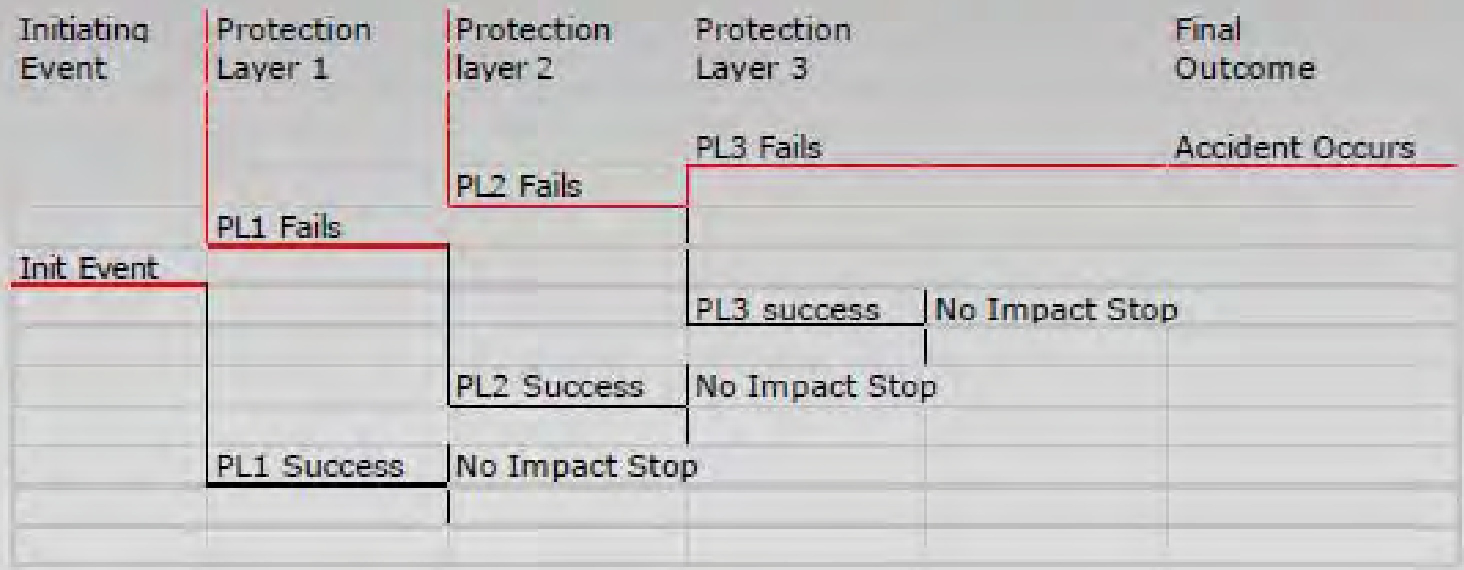
– Branches are layers of protection

– Consider only two outcomes:

- accident
- no event

Layer of Protection Analysis

- A variation of Event Tree Analysis
  - **Optimized, Limited, More structured**



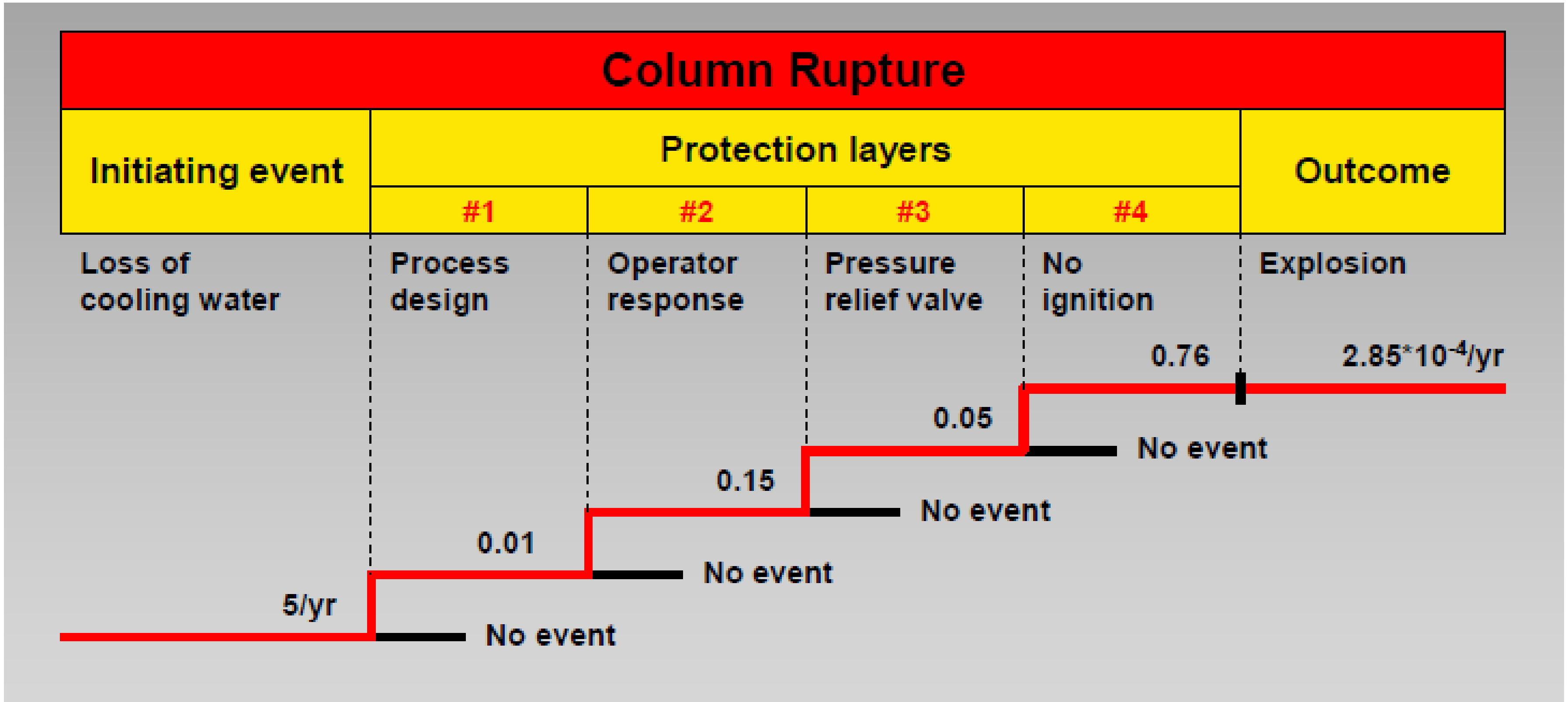
Branches are layers of protection

Layer of Protection Analysis

INIT EVENT	PL #1	PL #2	PL#3	PL#4		OUTCOME
Loss of	Process	Operator	Pressure	No		Fire
Cooling Water	Design	Response	Relief Valve	Ignition		
				0.3		1.8E-04
			0.1			Fire
		0.15				
	0.01					
4 /year						
						No Event

$$L = 4\ /year * 0.01 * 0.15 * 0.1 * 0.3 = 1.8 \times 10^{-4}/year$$

LOPA for Column Rupture



Layer of Protection Analysis

PFD must be calculated for each layer of protection

This is done using different methods depending in the situation.

– Non-repairable systems

(unreliability function is used to calculate PFD)

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

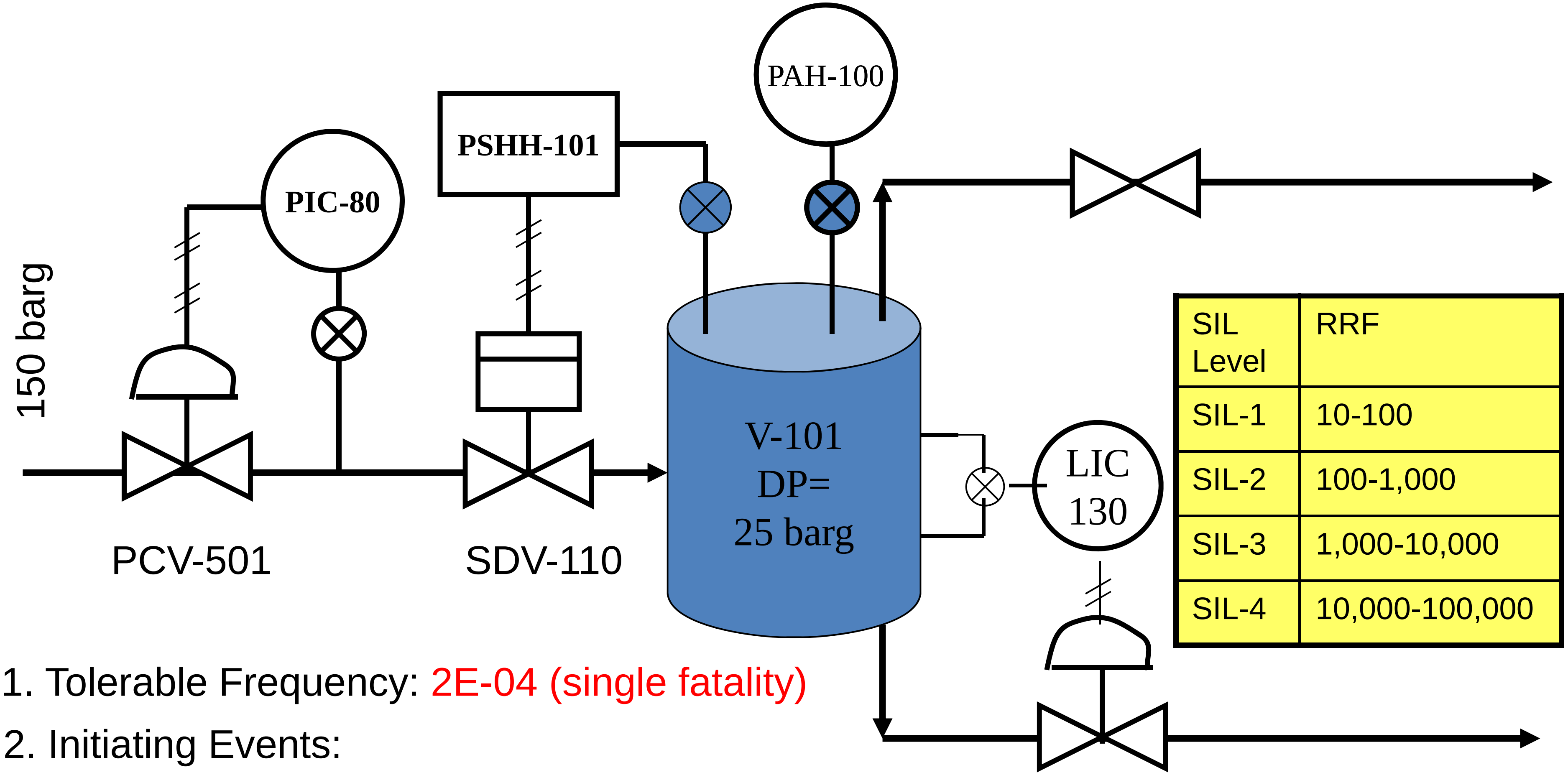
– Repairable systems

(unavailability methods provide an average PFD)

U = PFDavg = (λ* TI) / 2

– Probability Estimation

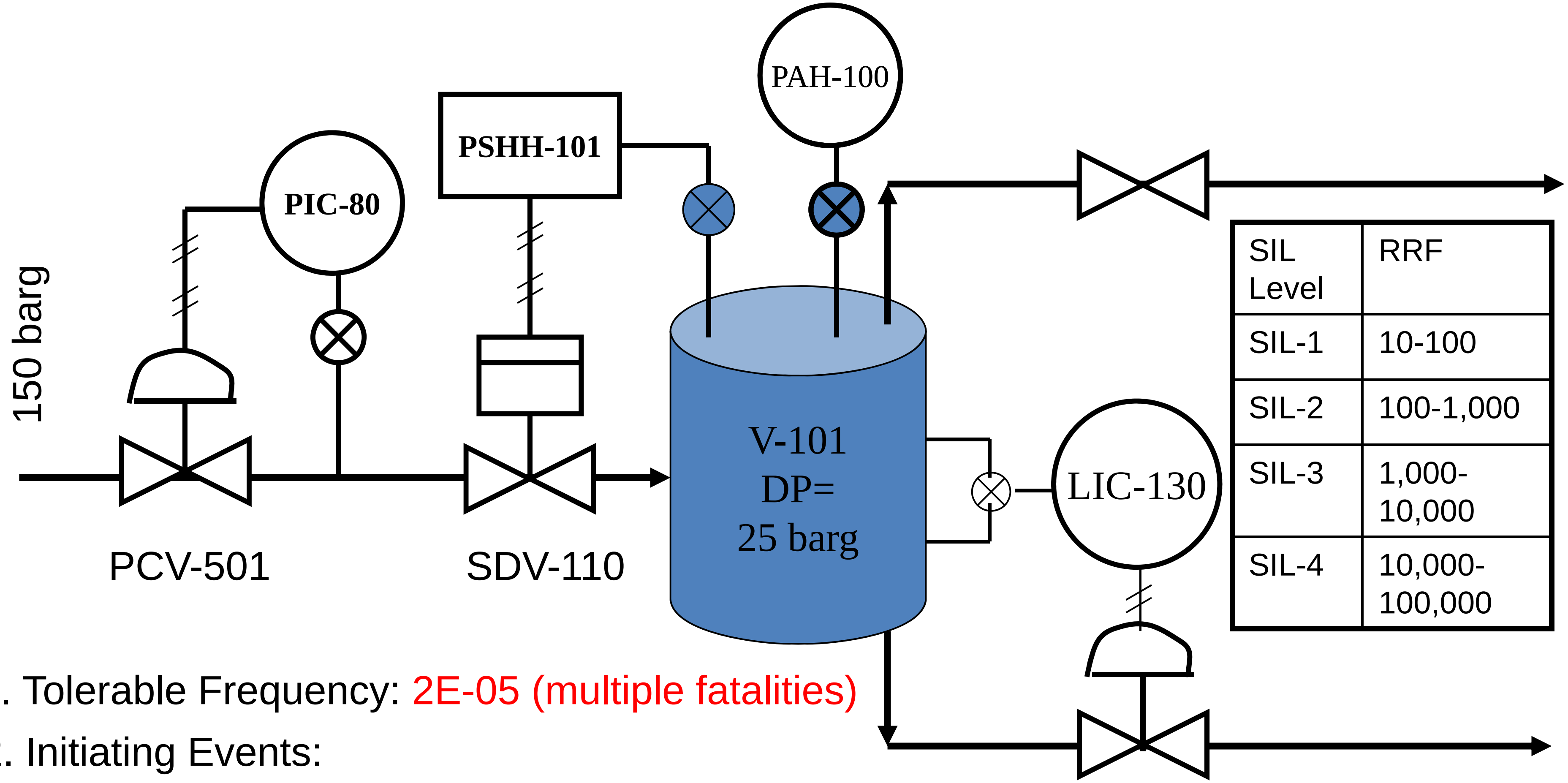
LOPA Calculation



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)

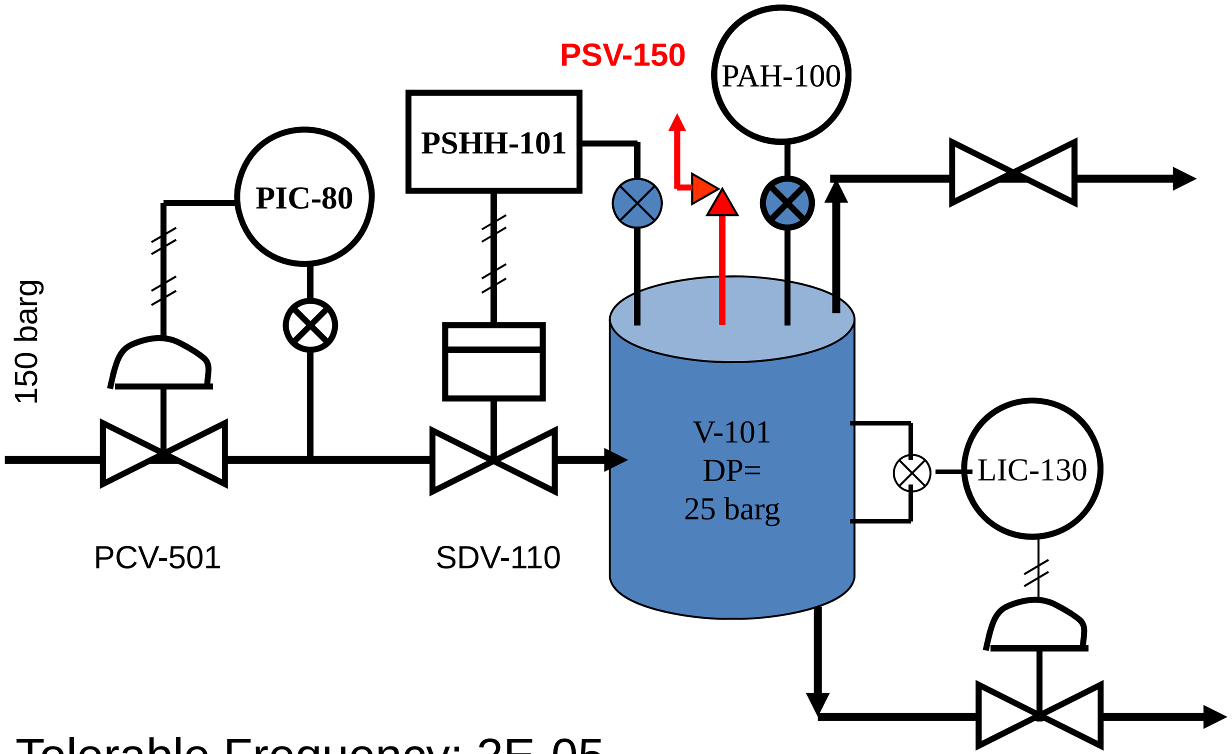
LOPA Calculation



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)

LOPA 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 LIMITED - ABU DHABI