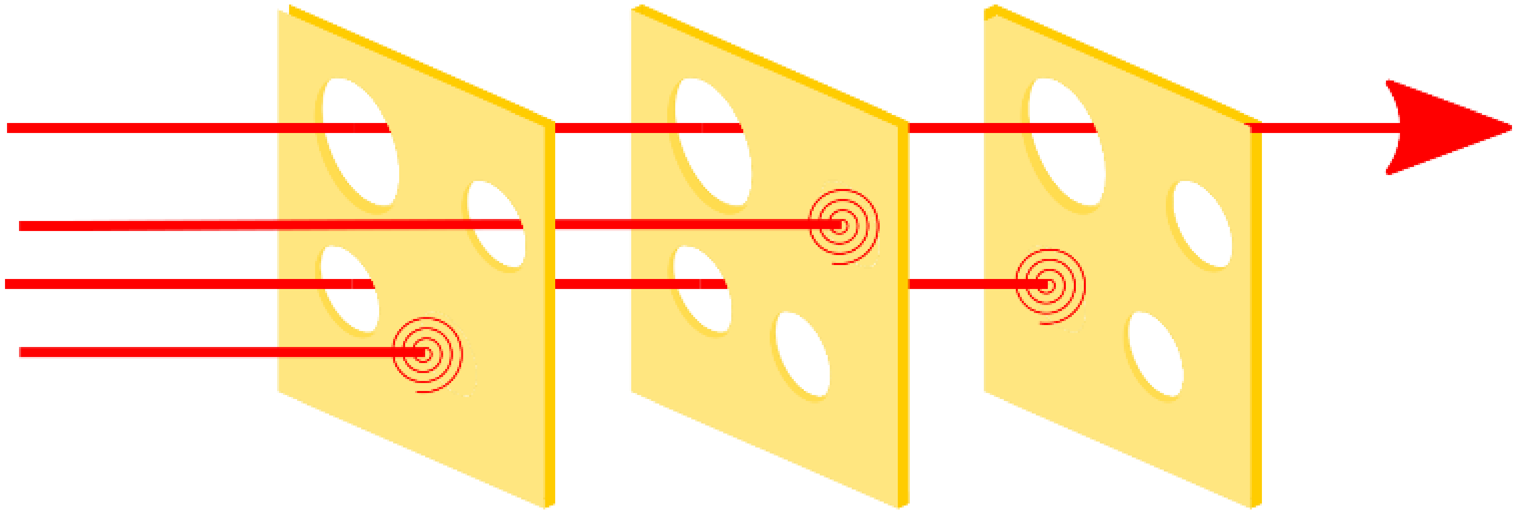
INTEGRATED RISK, ENVIRONMENTAL, & SAFETY CONSULTANTS

Challenges in Safety Barrier Identification and Control

by Shivaprakash Ponniah, Principal Consultant, IRESC

CCPS Member Company

Swiss Cheese Model



An adverse event rarely results from a single mistake. It is the consequence of **multiple, smaller errors cascading** through flawed organizational layers.

Layers of Protection

Each safeguard is a cheese layer — providing defense with inherent imperfections.

The “Holes”

Every barrier has weaknesses: design gaps, degradation or human error.

Accident Alignment

Catastrophic failure occurs only when all holes momentarily align, allowing a hazard to pass through every layer.

Barrier Types: Preventive vs. Mitigative

PREVENTIVE BARRIERS

Eliminate or reduce the likelihood of a cause

- BPCS, alarms, interlocks, ESD systems
- Mechanical protection — relief valves, check valves
- Machine protection trips — over-amps, vibration
- Operating & maintenance procedures (SOP/SMP)

MITIGATIVE BARRIERS

Reduce the severity of harm once a release occurs

- Fire and Gas detection systems
- Fire fighting — water spray, deluge systems
- ESD systems – isolation and de-pressurization
- Evacuation and emergency response plans

Barrier Classification by Nature

Barriers are not only defined by function — they are also categorized by **what form they take** within the safety management system.

Hardware Barriers

Physical systems engineered to prevent or respond to hazards.

- Shutdown & detection systems
- Structural containment
- Fire protection systems

Human Barriers

Actions and decisions made by people that interrupt hazard pathways.

- Operator response to alarms
- Adherence to permit-to-work procedures
- Supervisory interventions

Management System Elements

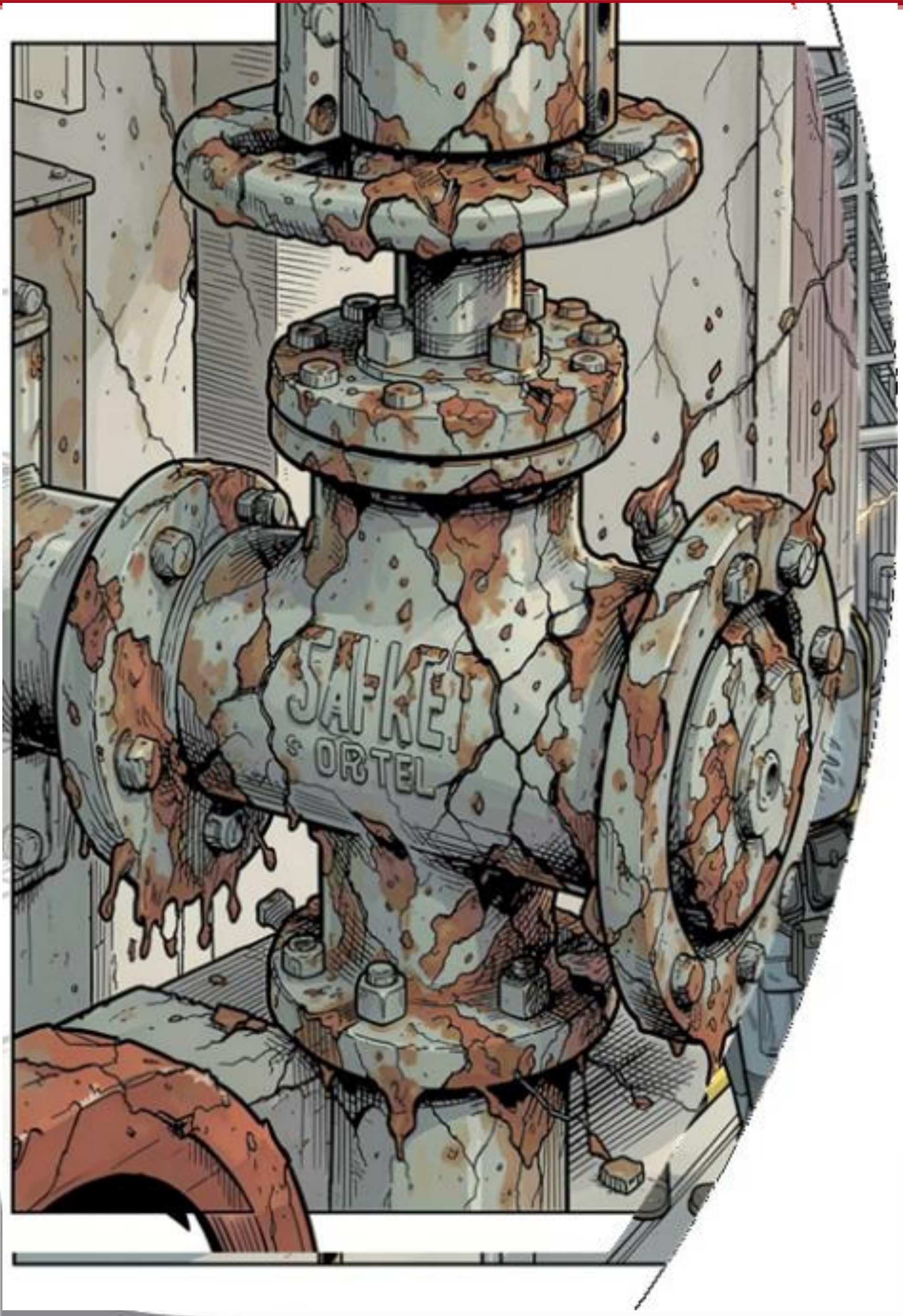
Organizational processes that sustain barrier integrity over time.

- Management of Change (MOC)
- Competency management
- Inspection & testing programs

Barrier Degradation with time

Not all barriers degrade at the same rate. Understanding degradation timelines is critical for **prioritizing inspection, testing, and maintenance** activities.

Degradation Rate	Typical Degradation Rate	Example Barriers
Fast	Less than 1 year	• Procedural Barriers (Procedures without refresh training) • Most Human Barriers • Active Barriers (Gas Detectors, Emergency Lighting)
Medium	1-5 years	• Active Barriers – ESD Systems • Safety Documentation • Process Containment- Subject to more rapid corrosion
Slow	> 5 years	• Active Barriers (Relief Valves) • Process Containment- Subject to normal corrosion rates • Passive Barriers (Tank Dykes, Firefalls)
Static	Life of Facility	• Separation distances (provided these are maintained by planning)



Why Barriers Fail

Design & Engineering Gaps

A barrier may be fundamentally inadequate — undersized, incorrectly specified, or never designed for the actual hazard scenario it is meant to address.

Maintenance & Monitoring Deficiencies

Without consistent inspection, testing, and verification, even well-designed barriers silently degrade until they fail when needed most.

Human & Organizational Weakness

Unclear procedures, weak training, unrealistic assumptions about operator behavior, and inconsistent management oversight all erode human and organizational barriers over time.

The Piper Alpha Disaster — 1988

On July 6, 1988, the Piper Alpha platform in the North Sea suffered a catastrophic explosion and fire, killing **167 people**. A chain of barrier failures turned routine maintenance into the deadliest offshore disaster in history.

Maintenance Initiated

Pump-A isolated; PSV removed; flange sealed with hand-tightened disk cover.

Permit Gap

PSV permit noted pump unfit - but this was not transferred to the overhaul permit.

Communication Breakdown

Duty engineer left PSV permit in control room; it was lost. Night shift was not briefed.

Catastrophic Restart

Pump-B failed; operators started Pump-A. Gas escaped past the blind flange — explosion followed.

Piper Alpha Accident – Barrier Failures

iresc

Procedural Failure

PTW: During routine maintenance, workers failed to complete the required paperwork to indicate the pump was incomplete and should not be operated.

Hardware Failure

Maintenance Failure: A temporary metal disk (blind flange) was only hand-tightened on the open pipe where the valve had been.

Communication Failure

Communication: Day shift did not brief night shift on pump status; critical permit was lost.

Human Failure

Operations Error: The night shift started attempted to start the stand-by pump without checking the maintenance logs.

Mitigation Failure

Secondary System Failure: The emergency fire pumps were set to manual mode allowing the fires to rage out of control and destroy the platform.

Do our plant have high risk scenarios?

1

Know your top risks

Does your team clearly know the top 5 risks in your plant?

2

Identify your barriers

What barriers protect against these high-risk scenarios? Are they documented and understood

3

Asset current status

What is the real-time health of these critical barriers? Are they currently degraded or bypassed

4

Verify Maintenance & Compensating Measures

Are barriers maintained on schedule? Are compensating measures in place when a barrier is unavailable?

Hazard Identification

Hazard identification is the essential first step in **uncovering threats** and **shaping effective barriers** before high-risk scenarios escalate

Revealing High-Risk Scenarios

HAZID, HAZOP and LOPA studies pinpoint events with severe consequences forming the central “top event”

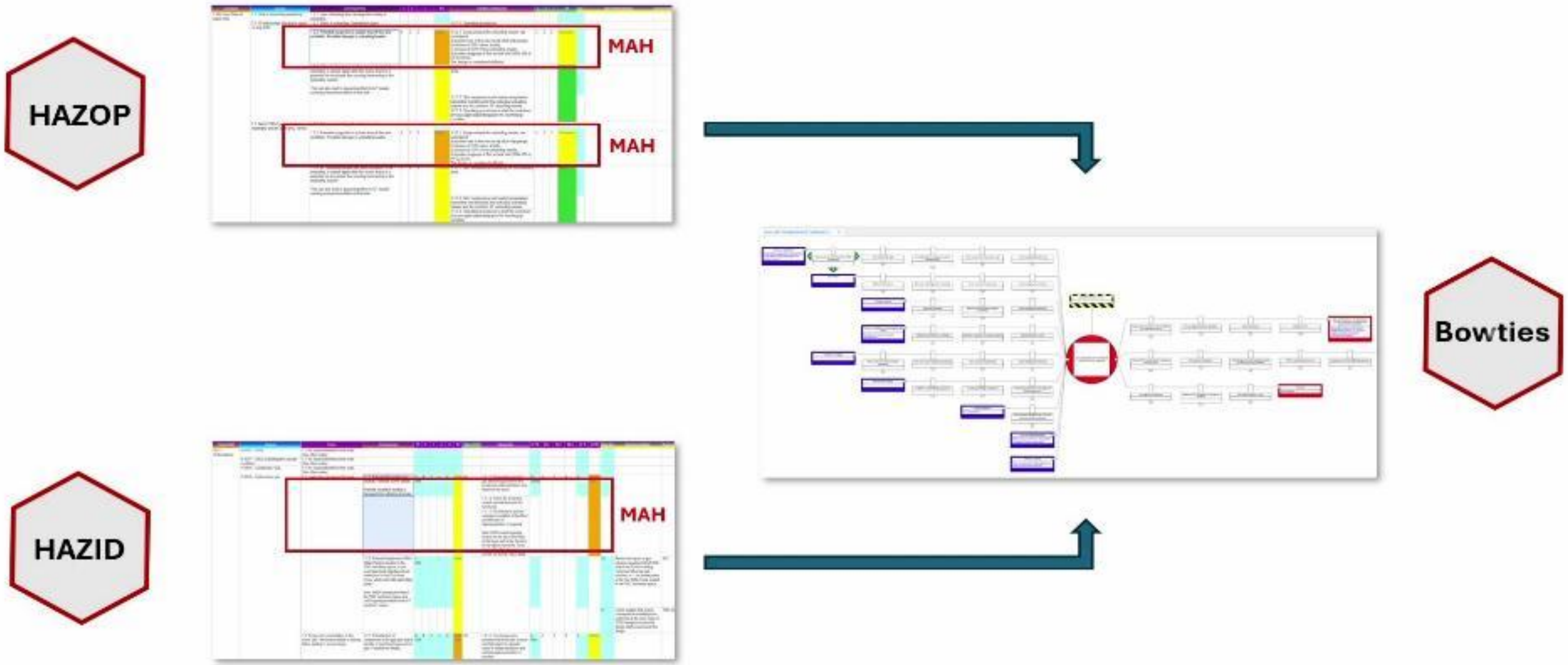
Building Effective Barriers

Hazard identification informs the design of **preventive** and **mitigating** barriers on both sides of the Bow-Tie.

The Crucial Link

Without robust hazard identification, the Bow-Tie is incomplete — leaving high-risk scenarios unaddressed.

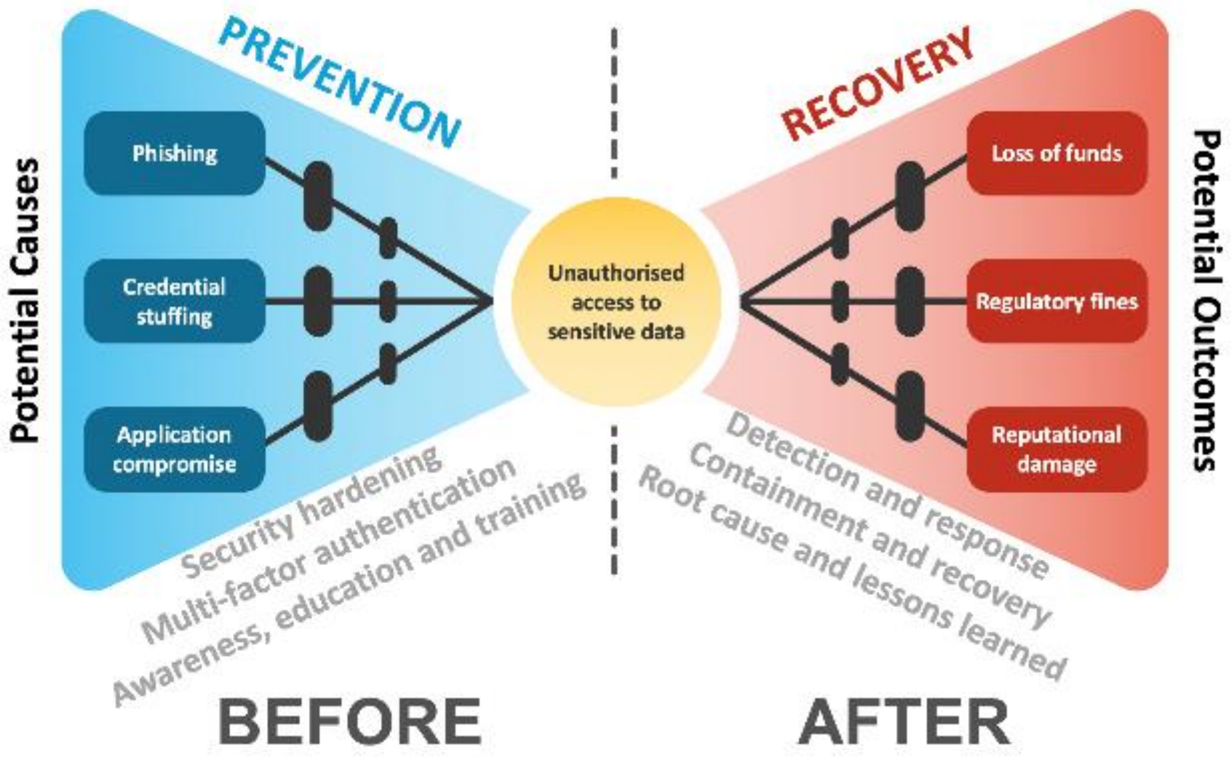
MAH Identification to Bow-Tie



Bow-Tie

Methodology used to analyze how hazards cause **critical events** and how **barriers control** these risks

Visually bridges the gap between proactive risk prevention and reactive consequence mitigation



Left Side

Threats → Top Event — preventive barriers

Right Side

Top Event → Consequences — mitigative barriers

Safety Critical Elements and Performance Standards

1

Identification

Identify all the SCEs in our plant.

2

Register

Maintain formal SCE register.

3

Testing Plan

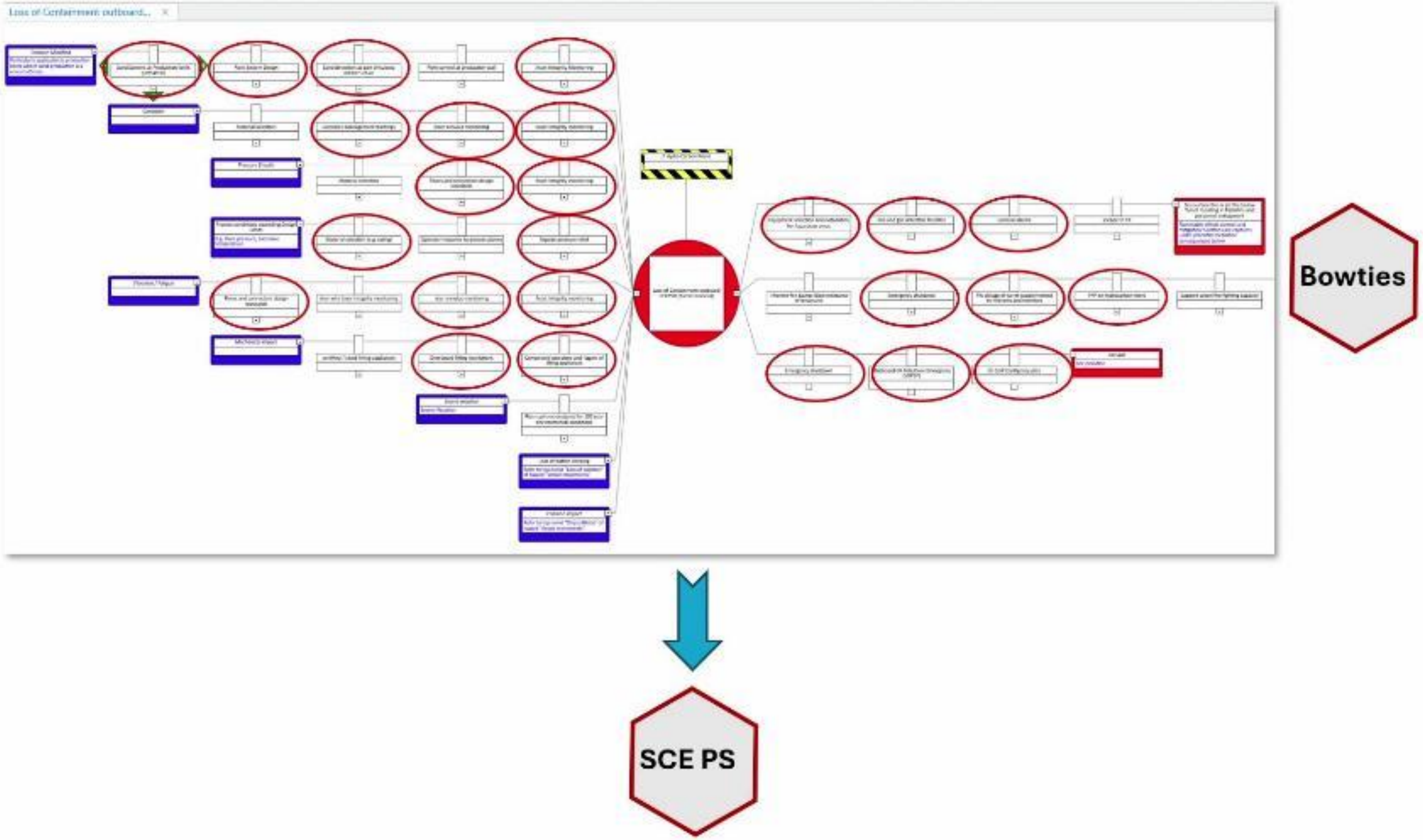
Make periodic testing and maintenance plan.

4

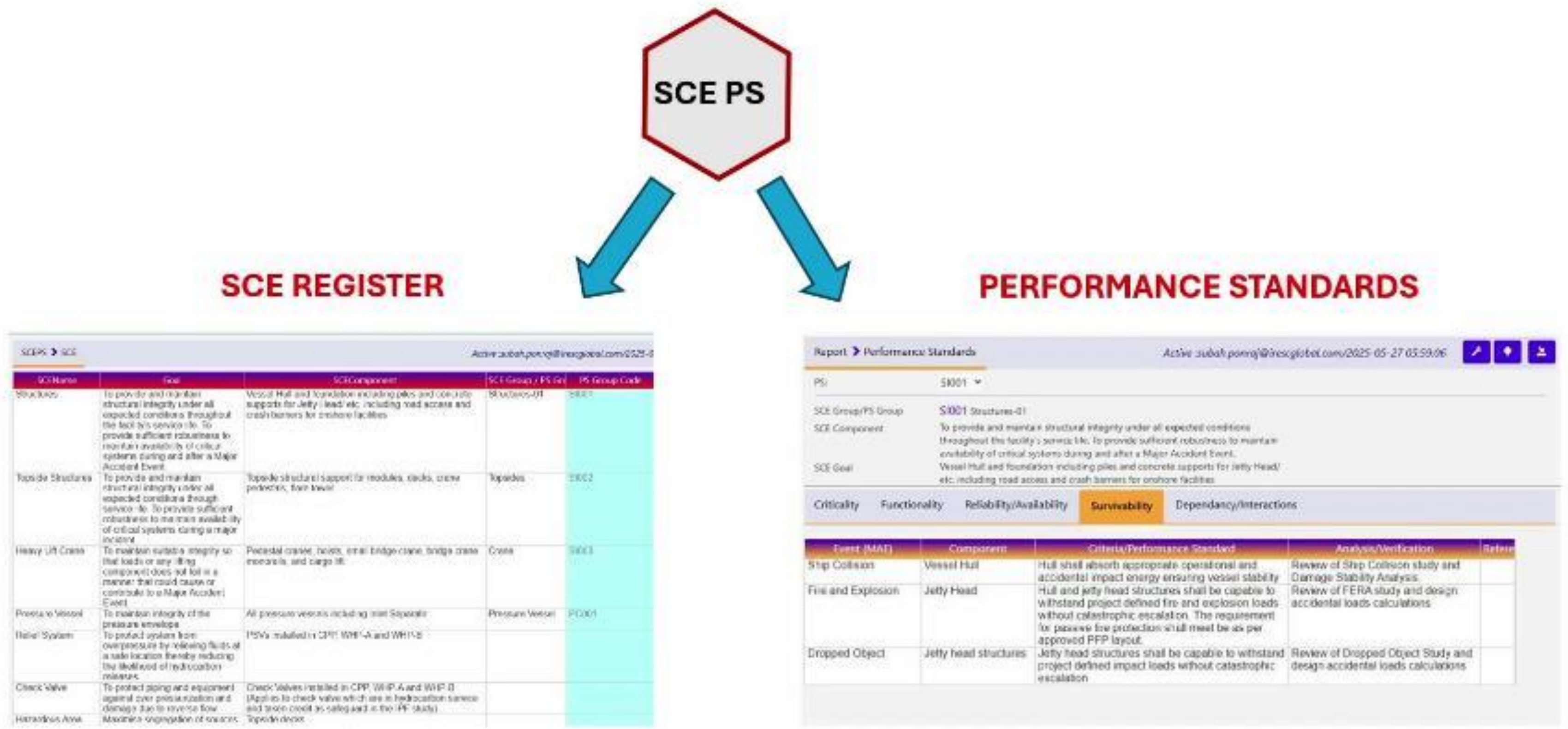
Performance Standards

Define Performance Standards to be met by SCE

Bow-Tie Integration with SCE PS



SCE PS Workflow



Key Takeaways

Know Your High-Risk Scenarios

Robust hazard identification technique to assist in mapping all high-risk scenarios

Barrier Identification

Identify all critical barriers that helps in maintaining risks in ALARP

Testing and Maintenance

Make a routine testing and maintenance plan to ensure robustness of the SCEs

Performance Standard

Define performance standards to be achieved by the SCEs

Real world SCE degradation examples for Preventive Barriers

Operator-Based

Manual interventions and overrides that bypass or degrade SCE function without formal authorisation.

SIF testing gaps

Temporary removal of protection during proof testing creates unprotected windows if not properly managed.

PSV based concerns

Relief valve degradation, incorrect sizing, or blocked outlets that compromise overpressure protection.

Bypass of IPL

<u>Hazard!!!!</u>

- The risk reduction assumed as part of SIL Allocation and subsequent design is no longer valid. May result in increase in SIL requirement by one order.

Consider the following event tree that was originally used during LOPA

Probability of over pressurisation (with BPCS) = 0.001

Probability of over pressurisation (without BPCS) = 0.01

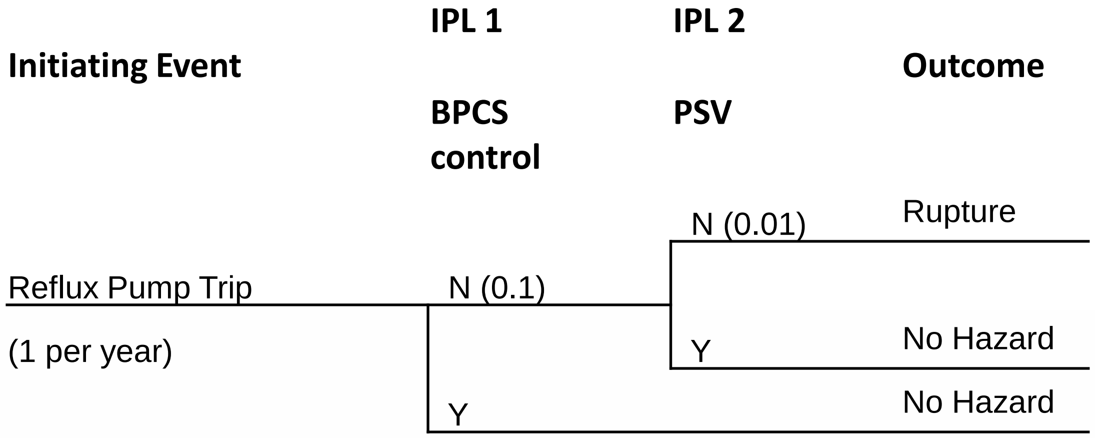
Probability of over pressurisation (BPCS offline for a month) = 0.00163

If Tolerable risk is 1E-5 / year

SIL 1 RRF 100

SIL 2 RRF 1000

SIL 2 RRF 163



BPCS Alarm Setpoint and bypasses

While SIF setpoints are typically password-protected, pre-alarm setpoints and control loops often lack equivalent safeguards.

SIF Setpoints

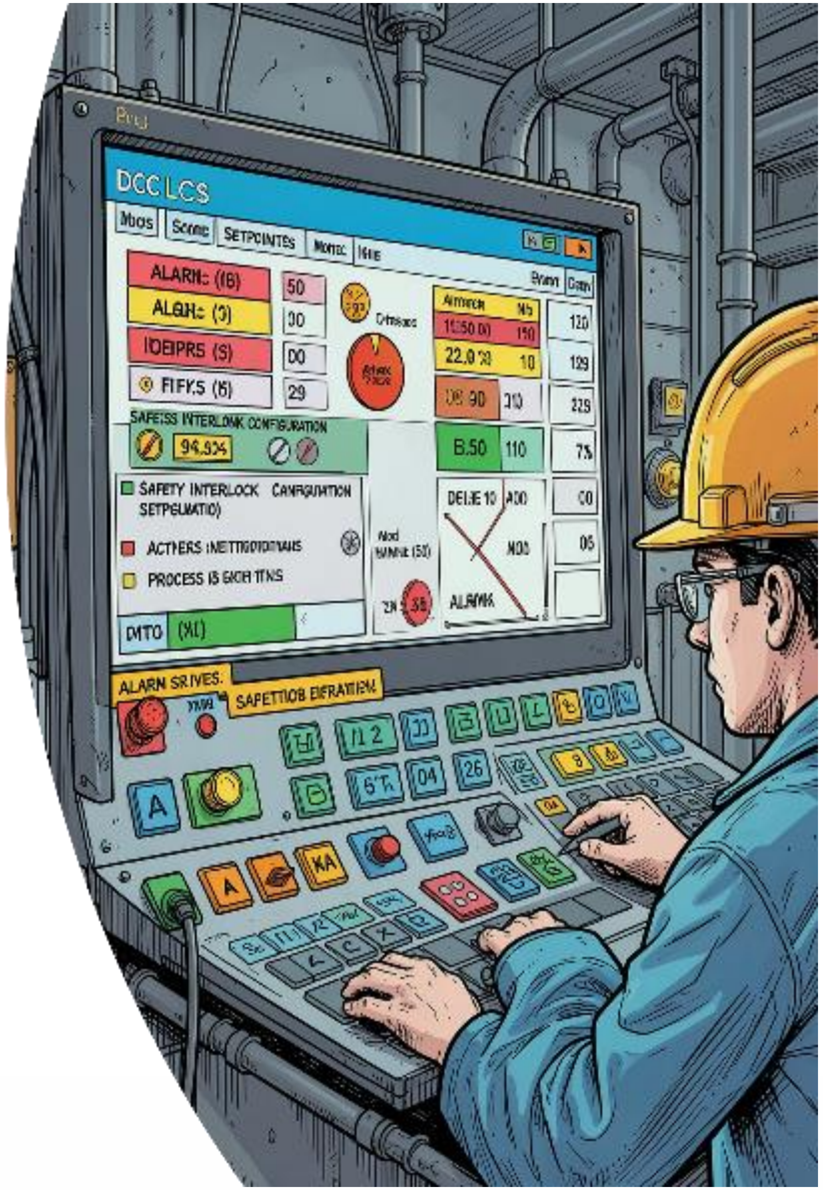
Typically Password-protected — cannot be modified without authorisation.

Pre-Alarm Setpoints

Are protections in place to prevent inadvertent changes?

Control Loops (Example PIC / LIC/ FIC Loops)

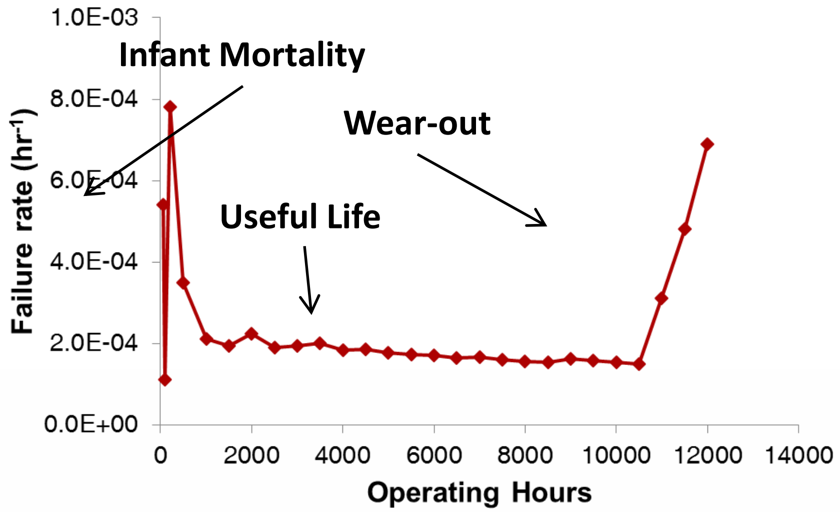
Switching SCE control loops to Manual Mode must be based on authorisation



Plant Life, Mission Time and Useful Life

- Plant Life ≠ Mission Time ≠ Useful Life
- PFDavg estimated will increase after Mission Time, unless the SIF components are replaced or refurbished to as-new condition
- Useful life of the component also need to considered
- Element overhauling will reset the clock on both mission time and useful life.

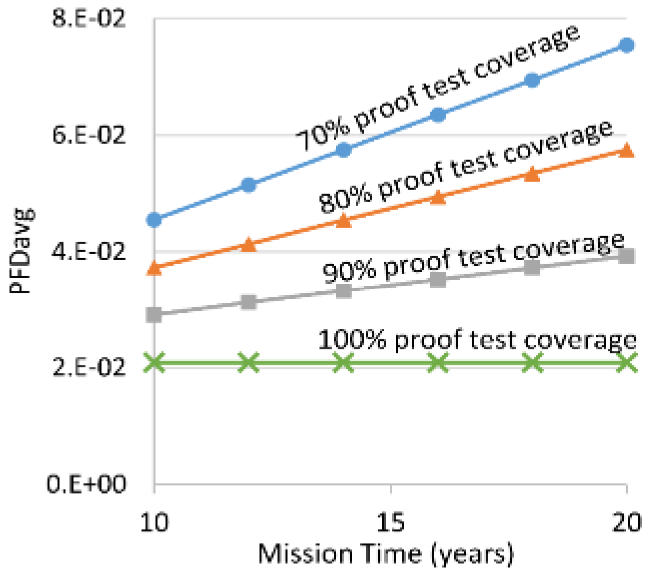
The Bath Tub Curve

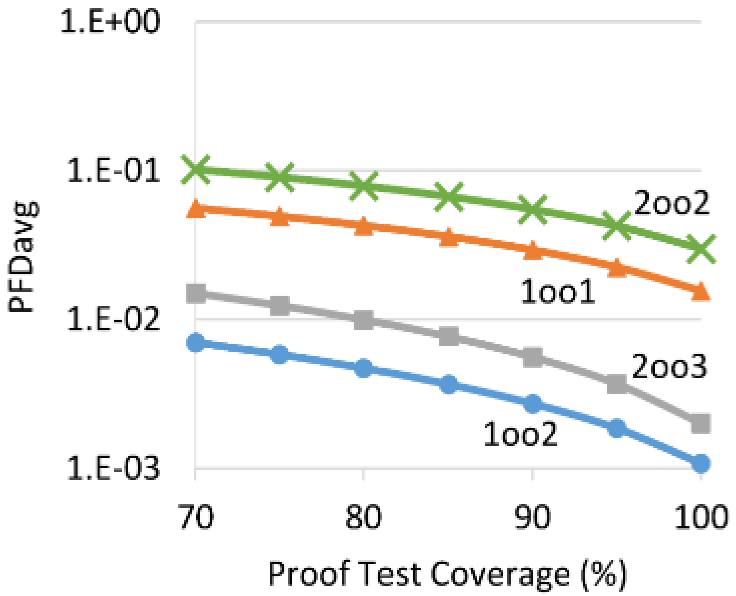


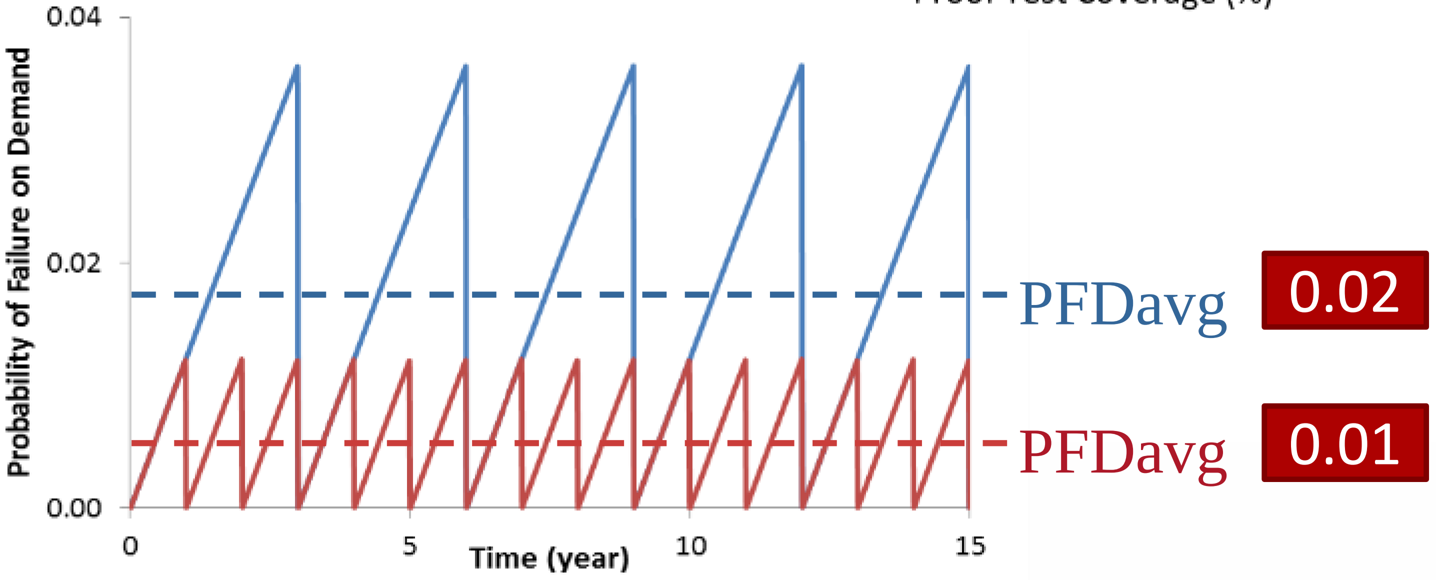
Typical Useful Life

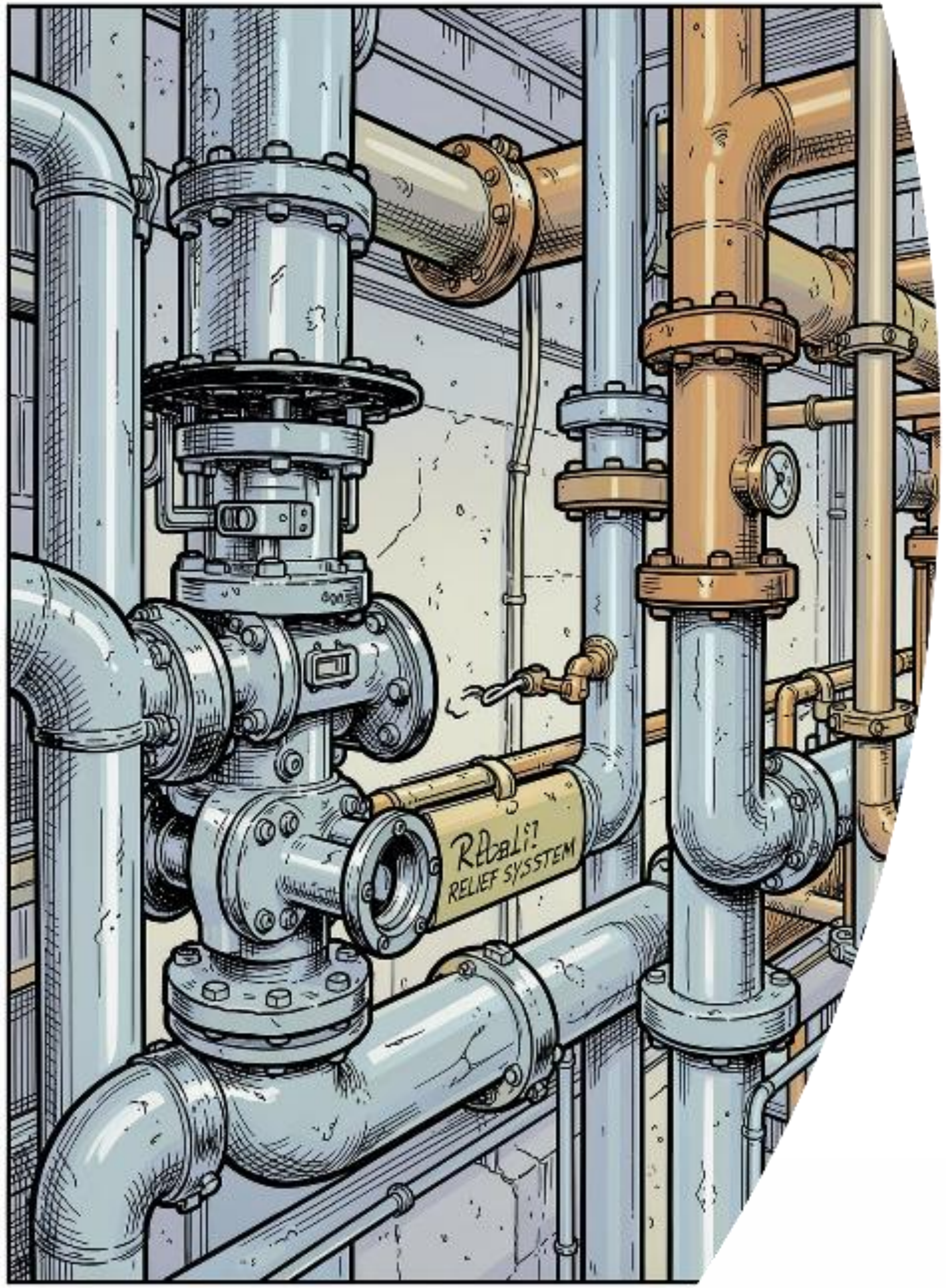
Transmitters	8 ~ 12 years
Solenoid Valves	10 ~ 15 years
Valves (mechanical with elastomeric seals)	10 ~ 15 years
Valves without elastomeric seals	15 ~ 30 years

Testing and Maintenance – SIF Degradation









PSV-Related Integrity Issues

→ **Dual Check Valves**

Are dual check valves — used to minimise reverse flow — tested on schedule?

→ **Control Valve Bypasses**

Administrative controls on bypasses - gas blow-by scenarios may have additional load if bypass left open.

→ **Restriction Orifices (RO)**

PSV sizing depends on RO data — are these understood and managed as safety-critical?

→ **Choke / PV Erosion**

Erosion creates larger flow paths, invalidating PSV sizing assumptions and relief capacity.

Q&A

tnche1

QR Code - Evaluation