12th Chemical Process Safety Sharing (CPSS)

Common pitfall in HAZOP / LOPA revalidation and IPL Credit

Yuttaphon Phungchartthai

Yuttapph@scg.com

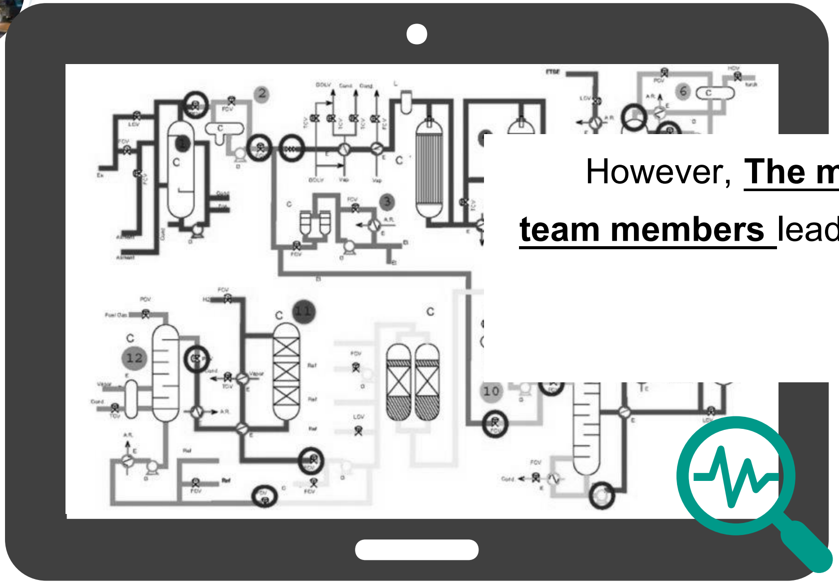
SCGC

Contents

Introduction : What is HAZOP?

Hazard and Operability study (**HAZOP**) is one of **Qualitative Process Hazard Analysis (PHA) workshop** study **developed in 1963** and wildly used in Petrochemical industry to identify, reduce and manage workplace hazards, which can cause fires, explosions and releases of toxic or flammable chemicals.

*Optional



Guide word
No (not, none)
More (more of, higher)
Less (less of, lower)
As well as (more than)

Possible Process Parameters for Process Operations			
Flow	Viscosity	Phase	Signal
Pressure	Reaction	Speed	Start/stop
Temperature	Composition	Particle size	Operate
Mixing	Addition	Measure	Maintain

Consequence (C)	Frequency of Occurrence (F)				
	F1	F2	F3	F4	F5
C1	Class II	Class III	Class III	Class III	Class III
C2	Class I	Class II	Class III	Class III	Class III
C3	Class I	Class I	Class II	Class III	Class III
C4	Class I	Class I	Class I	Class II	Class III
C5	Class I	Class I	Class I	Class I	Class II

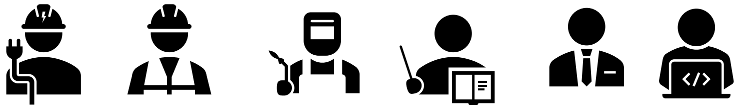
However, **The major gap of HAZOP** is the result based on **opinions of team members** leading to providing **insufficient safeguard** and resulting in **Intolerable Risk Remaining Without Noticing.**

DATE:

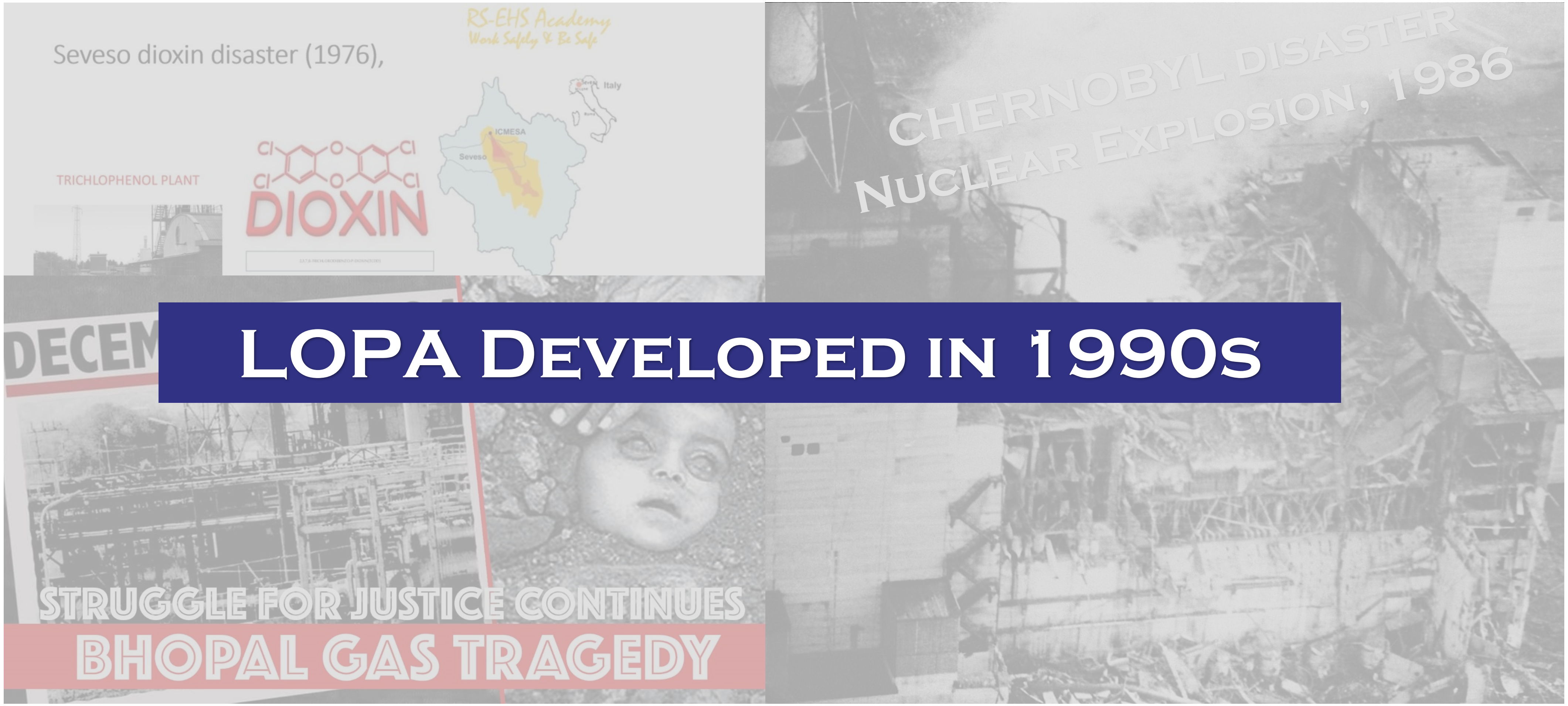
MEETING DATE:

Oil flow from the feed line, heat from the furnace
Vaporize, superheat and transfer oil vapour to the process

No.	Guide word	Element	Deviation	Possible causes	Consequences	Safeguards	Comments	Actions required	Action by
1	No	Oil flow	No oil flow	– Supply failure – Flow control valve PCV closed	Vaporizer coil overheats and may fail	Low flow alarm FAL High temperature trip TSH	Safeguard depends on quick operator response	Consider low flow element FE to close main burner valve TCV	LB
				– Plugging of coil – Blockage down-stream of vaporizer	Oil in vaporizer will boil: Possible overheating and coking of heating coil	Low flow alarm FAL High temperature trip TSH		Check whether these safeguards are adequate and the ease with which the coil could be cleaned	NE
2	No	Heat	No heat	Flame out in the furnace	Unvaporized liquid oil fed to the process	None		– Investigate effect of liquid oil on the process – Consider interlocking the furnace flame out signal with closure of FCV – Consider providing a low oil outlet temperature alarm	DH



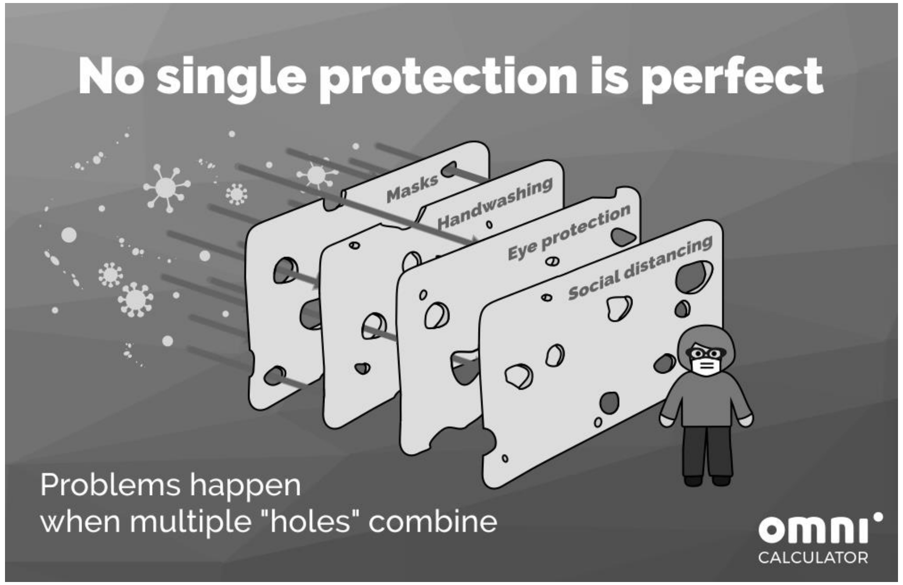
Introduction : Catastrophic events

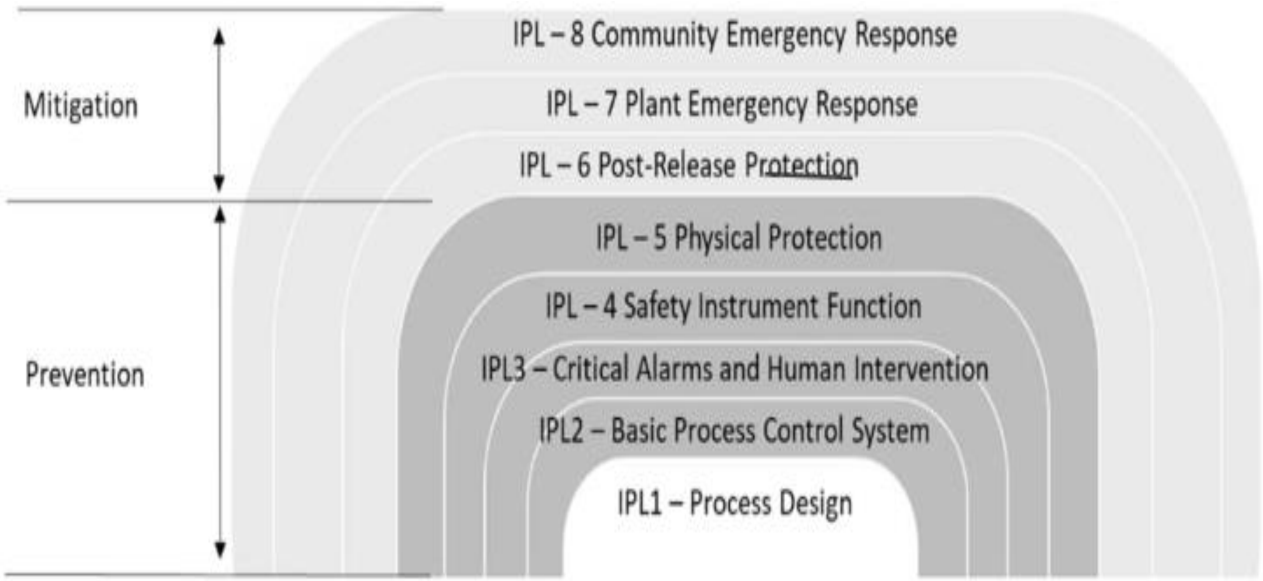


LOPA Developed in 1990s

Introduction : What is LOPA?

Layer Of Protection Analysis (LOPA) is **semi-quantitative risk assessment method** using to reproducibly evaluate the risk of **selected accident scenarios** and identify additional **risk reduction opportunities.**



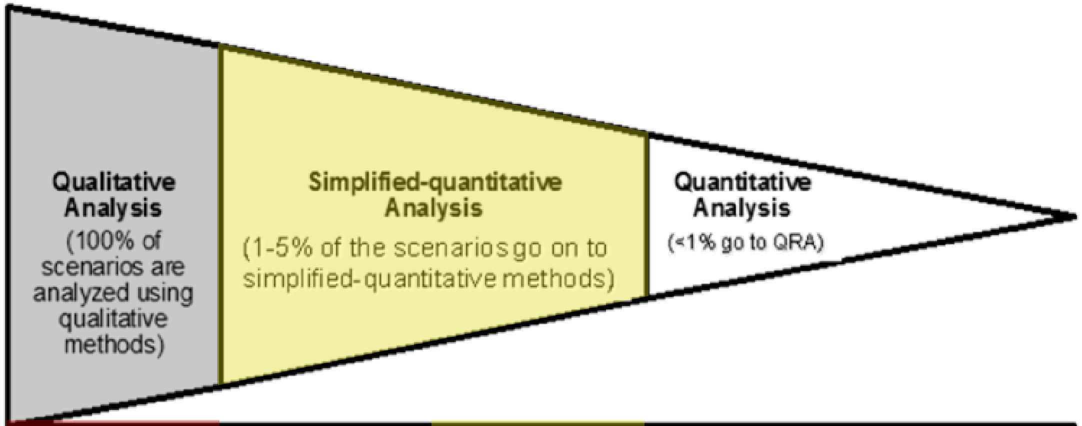


What LOPA does ?

LOPA helps team to **assess the adequacy of Safeguards** against Risk to achieve Tolerable Level.

"LOPA does not find new accident scenarios"

Introduction : Why HAZOP/LOPA ?



Techniques:	HAZOP What-if/Checklist FMEA	Quantified FMEA F&EI CEI	LOPA	Rough estimate with event tree	Event tree Fault tree HRA
Applicability to simple issues:	Good	Good	Good	Overkill	Gross overkill
Applicability to complex issues:	Poor to Okay for Risk Judgment	Okay for Risk Judgment	Usually good	Occasionally poor	Good

Courtesy of Process Improvement Institute, Inc., 2004.

HAZOP identify accident scenarios.

LOPA provides specific criteria and restrictions for the evaluation of Protection Layers.

HAZOP/LOPA

- Reducing emotionalism
- Providing clarity and consistency

Example Initiating Event Likelihood (IEL) And Independent Protection Layer (IPL) Frequency

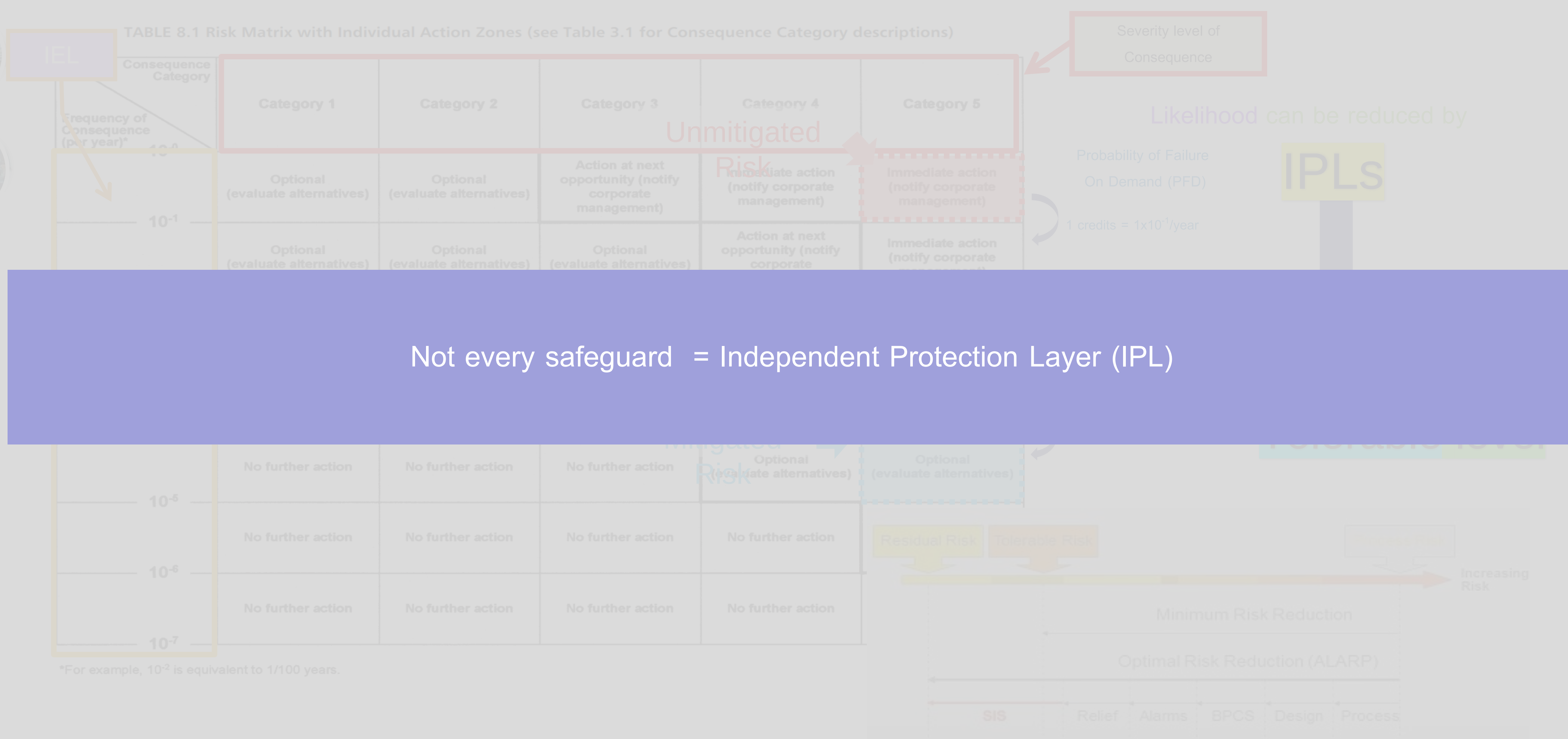
Typical Frequency Values, f^I, Assigned to Initiating Events

Initiating Event	Frequency Range from Literature (per year)	Example of a Value Chosen by a Company for Use in LOPA (per year)
Pressure vessel residual failure	10^{-5} to 10^{-7}	1×10^{-6}
Piping residual failure—100 m—Full Breach	10^{-5} to 10^{-6}	1×10^{-5}
Piping leak (10% section)—100 m	10^{-3} to 10^{-4}	1×10^{-3}
Atmospheric tank failure	10^{-3} to 10^{-5}	1×10^{-3}
Gasket/packing blowout	10^{-2} to 10^{-6}	1×10^{-2}
Turbine/diesel engine overspeed with casing breach	10^{-3} to 10^{-4}	1×10^{-4}
Third party intervention (external impact by backhoe, vehicle, etc.)	10[illegible] to 10^{-4}	1×10^{-2}

Examples of Active IPLs

IPL	Comments *Assuming an adequate design basis and inspection/maintenance procedures*	PFD from Literature and Industry	PFD Used in This Book (For screening)
Relief valve	Prevents system exceeding specified overpressure. Effectiveness of this device is sensitive to service and experience.	$1 \times 10^{-1} - 1 \times 10^{-5}$	1×10^{-2}
Rupture disc	Prevents system exceeding specified overpressure. Effectiveness can be very sensitive to service and experience	$1 \times 10^{-1} - 1 \times 10^{-5}$	1×10^{-2}
Basic Process Control System	Can be credited as an IPL if not associated with the initiating event being considered (see also Chapter 11). (See IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001) for additional discussion.)	$1 \times 10^{-1} - 1 \times 10^{-2}$ ($>1 \times 10^{-1}$ allowed by IEC)	1×10^{-1}
Safety Instrumented Functions (Interlocks)	See IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001) for life cycle requirements and additional discussion		

Introduction : How IPLs take a role in Risk Reduction in HAZOP/LOPA ?



Not every safeguard = Independent Protection Layer (IPL)

Introduction : 3 rules for Independent Protection Layer (IPL) Qualification

If Safeguard can achieve this criteria = Independent Protection Layer

Independent

Independence From
- **<u>initiating event</u>**
- **Components of <u>other IPL</u>**

Avoid Common Failure

Effectiveness

- **Be <u>specifically designed</u> on preventing the consequence**
- **Capable of performing its safety function dependably (<u>In time & Effective</u>) as its with a *known level of risk reduction* or known as *PFD*.**

Auditability

Ensure risk reduction is continually achieved by
- **<u>Documentation</u>**
- **<u>Inspection, test and preventive maintained</u>**
- **<u>Access Security</u>**
- **<u>Management of change</u>**
- **<u>Etc.</u>**

Introduction

There are **many ambiguous or misunderstanding** when evaluating the safeguards as the IPLs leading to

Improper design

and/or

Insufficient provision of protections.

Sharing common pitfalls of IPL credit mostly found during HAZOP/LOPA Revalidation workshops

1st Pitfall : Effectiveness of Alarm and Human response

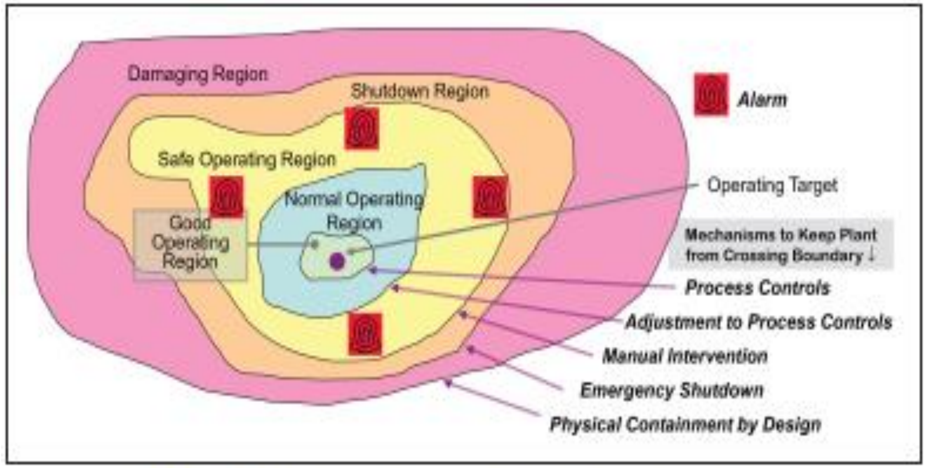


Figure 1.3.1. Operating region versus modality of remediation

Alarm is the most popular IPL taken credit in HAZOP/LOPA due to simple implementation of it.

One constrain that is not proved in HAZOP/LOPA session.

"Can operator action in time?"

Solution:

Alarm Rationalization Study

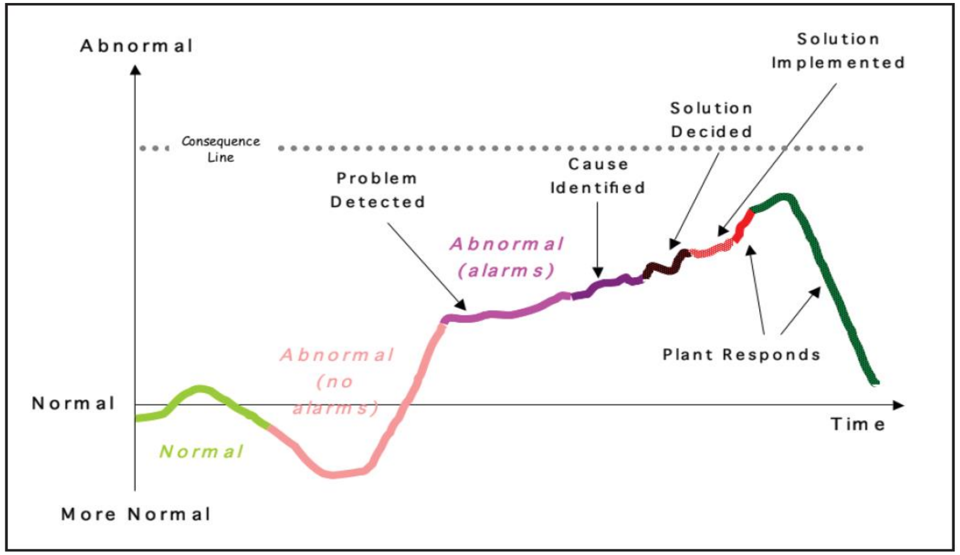
Sharing common pitfalls of IPL credit mostly found during HAZOP/LOPA Revalidation workshops

What is Alarm Rationalization Study ?

Alarm Rationalization study (**ARS**) is detail workshop by which each needed alarm is selected and the configuration design and supporting information for the task is built.

Actions in ARS includes

1. Deciding/Identifying which points to alarm (including calculated and imputed variables)
2. Determining/Identifying the alarm activation point, the setting of priority and all other remaining alarm response information including potential causes, appropriate operator responses, and likely consequences of error.



Benefits

1. Screen out the ineffective alarm (No sufficient time for operator to response) and can manage with this unseen remaining risk
2. Minimize number of alarms - fewer alarm activations and fewer nuisance alarms
3. Operator response to alarms will be swifter and more effective

Reference: ANSI/ISA ISA18.2, EEMUA 191

Sharing common pitfalls of IPL credit mostly found during HAZOP/LOPA Revalidation workshops

ARS Workflow

Input information

- Hazard Analysis (Hazard and Operability Study, HAZOP/Safety Integrity Level, SIL Classification /Layer of Protection Analysis, LOPA Reports)
- Latest P&ID
- Process Flow Diagram (PFD)
- Process Description & Control Philosophy/ Narrative
- Cause & Effect (C&E) Diagrams
- List of Alarm and Trip Setting
- Calculated or simulated of Time to consequence (TTC) of each process alarms.

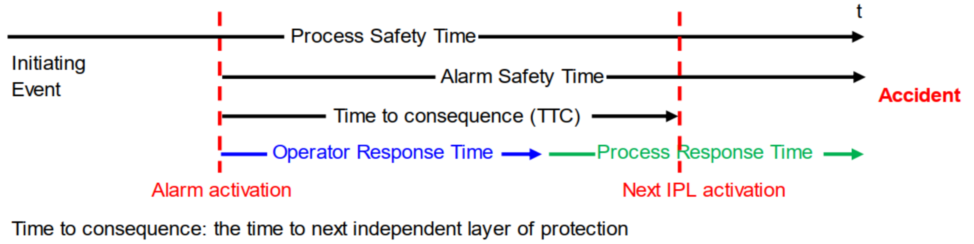


Figure 1B. Response time for ARS (Alarm Safety Time is not equal to TTC, as there is next IPL after alarm before accident)

Alarm Prioritizing Criteria

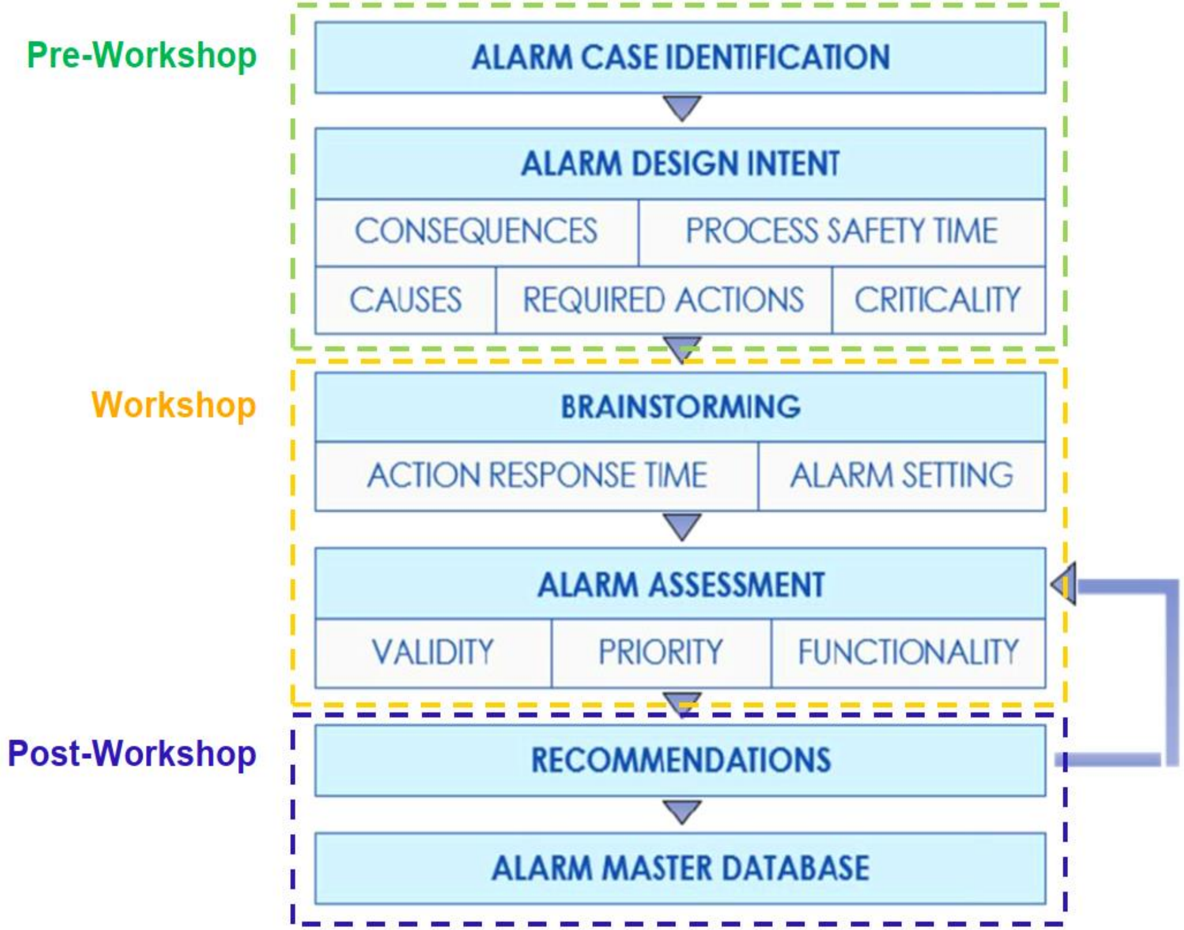
- Consequence (Usually following HAZOP Risk matrix)
- Alarm Priority (Three or Four levels)
- Time to response criteria (Up to team set up)

Example of Alarm Priority matrix

Consequences of Inaction				
Impact Areas	**Consequence Category 1 (None)**	**Consequence Category 2 (Minor)**	**Consequence Category 3 (Major)**	**Consequence Category 4 (Severe)**
Personnel	None	Minor or no injury, no lost time.	One or more severe injury(s).	Fatality or permanently disabling injury.
Environmental	None	Minor	Release which results in agency notification, permit violation or fine.	Significant release with serious offsite impact.
Financial	None	Impact to equipment or production < $50K.	Impact to equipment or production $50K to $500K	Impact to equipment or production > $500K
Operator Urgency (Time to Respond)				
Not Urgent (> 30 mins)	**No Alarm**	**Re-engineer the alarm for urgency**		
Prompt (15 to 30 mins)	**No Alarm**	**Medium**	**Medium**	**High**
Rapid (5 to 15 mins)	**No Alarm**	**Medium**	**High**	**Highest**
Immediate (< 5 mins)	**No Alarm**	**High**	**Highest**	**Invalid (redesign)**

Sharing common pitfalls of IPL credit mostly found during HAZOP/LOPA Revalidation workshops

ARS Workflow and guideline for good results



Guideline for good results (Not Mandatory)

Three Alarm Priority

Priority Level	Alarm configured during system design*
High (Priority 1)	3-7 % of total
Medium (Priority 2)	15-25% of total
Low (Priority 3)	70-80% of total

Note: * EEMUA Guidelines for Alarm Configuration

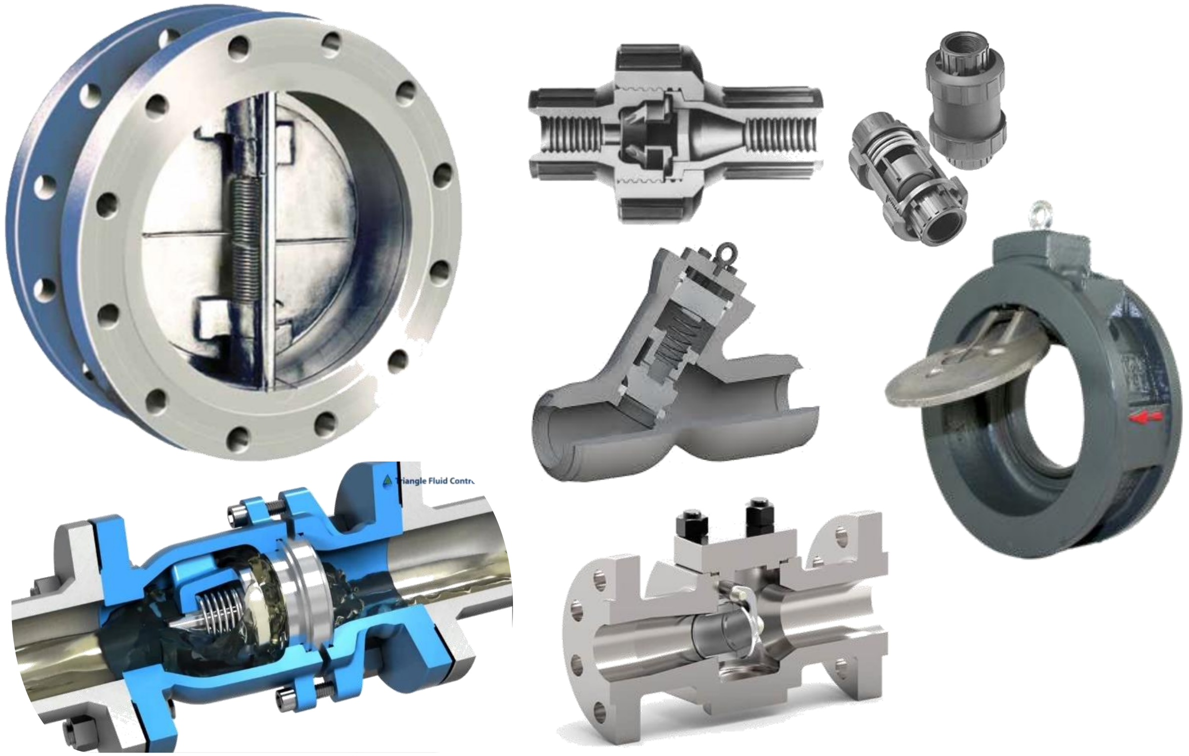
Four Alarm Priority

Priority of alarm	Number configured
Critical (emergency)	About 20 (total)
High	5% of total configured
Medium	15% of total configured
Low	80% of total configured

Overall Alarm System Performance Level (EEMUA 191)

Sharing common pitfalls of IPL credit mostly found during HAZOP/LOPA Revalidation workshops

2nd Pitfall : Effectiveness of Check valve as IPL



Check valve

One of argued element during HAZOP/LOPA sessions

Some consider it as IPL

, But some not.

How we should consider?

Sharing common pitfalls of IPL credit mostly found during HAZOP/LOPA Revalidation workshops

Check valve & LOPA

- At the time of CCPS LOPA (2001)
  - Due to a lack of data supporting their reliability, Check valves were not considered to be valid IPLs.
- Update from CCPS on Guidelines for IE and IPLs in LOPA (2015)
  - Check valve can be considered as Initiating Event (IE) or Independent Protection Layer (IPL) as below.
- Article in AIChe (2020): Crediting check valves as IPLs? Testing protocol to better understand check valve reliability by Jody E. Olsen.
  - There is comparison of single, double and triple check valves with no common and common cause of failure. (Using similar design valves).

Consider as IE (Check valve Failure)		**Consider as IPL**			
High demand mode (Challenged > 1 time/yr)		Low demand mode (Challenged ≤ 1 time/yr)			
Single Check Valve	Double Check Valves	Single Check Valve	Double Check Valves		Triple Check Valves
No common cause failure		No common	No common	10% common	10% common
IEL : 0.1/yr	IEL : 0.01/yr	PFD : 0.1/yr	PFD : 0.01/yr	PFD : 0.0181/yr	PFD : 0.0107/yr

Note: In case of double check valves, If both valves are not individually tested, IEL or PFD for a single check valve would applicable.

Sharing common pitfalls of IPL credit mostly found during HAZOP/LOPA Revalidation workshops

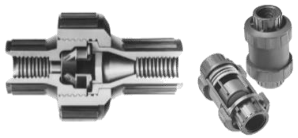
Check valve selection

Types (examples)

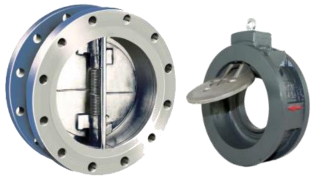
Swing Check Valve:

Ball Check Valve:

Diaphragm Check Valve

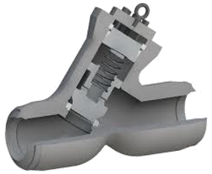


Wafer Check Valve



Axial Check Valve

Piston Check Valve



Sharing Our Practice

1. Select the check valves fitting to the process.
2. Credit for LOPA shall be take only

"Dissimilar-Type double check valves (0.01)"

Optional for more stringent process :

One shall be High quality type (Axial or Wafer)

Leak Classification

by ANSI/FCI 70-2 2006 (European equivalent standard IEC 60534-4)

Valve Leakage Classification - Overview

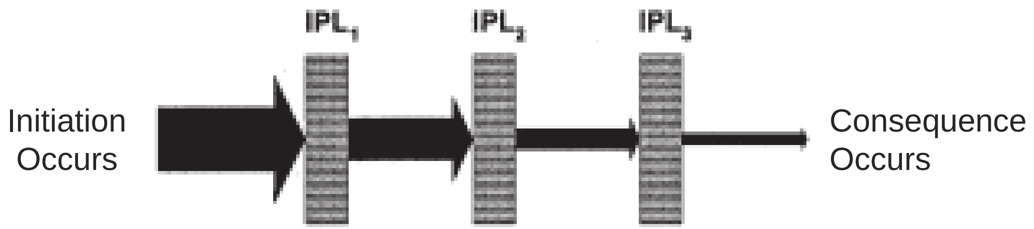
Leakage Class Designation	Maximum Leakage Allowable	Test Medium	Test Pressure	Testing Procedures Required for Establishing Rating
I	x	x	x	No test required
II	0.5% of rated capacity	Air or water at 50 - 125° F (10 - 52°C)	45 - 60 psig or maximum operating differential whichever is lower	45 - 60 psig or maximum operating differential whichever is lower
III	0.1% of rated capacity	As above	As above	As above
IV	0.01% of rated capacity	As above	As above	As above
Metal Seat V	0.0005 ml per minute of water per inch of port diameter per psi differential	Water at 50 to125°F (10 to 52°C)	Maximum service pressure drop across valve plug not to exceed ANSI body rating	Maximum service pressure drop across valve plug not to exceed ANSI body rating
Soft Seat (i.e. PTFE) VI	Leakage limit depends on valve size (0.15 to 6.75 ml per minute of 1 inch to 8 inches valve)	Air or nitrogen at 50 to 125° F (10 to 52°C)	50 psig or max rated differential pressure across valve plug whichever is lower	Actuator should be adjusted to operating conditions specified with full normal closing thrust applied to valve plug seat

The most commonly used

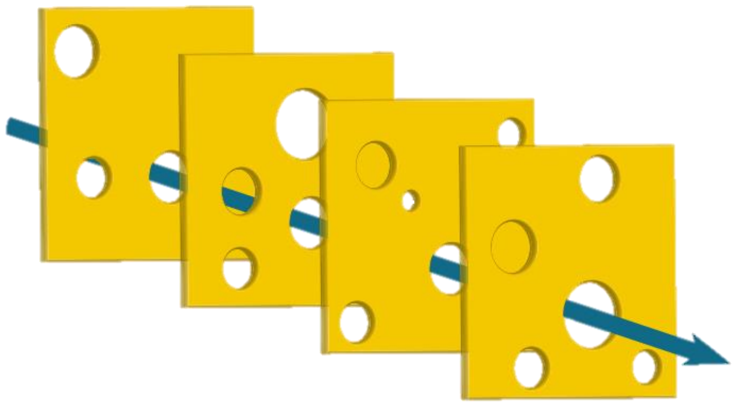
Sharing common pitfalls of IPL credit mostly found during HAZOP/LOPA Revalidation workshops

3rd Pitfall : Effectiveness of Partially Dependent Layer of Protection

Some safeguards seem to be independent from each others



Both of them may be taken credits as IPL



But actual design, both of them act as one IPL

This may lead to <u>Intolerable Risk Remaining Without Noticing.</u>

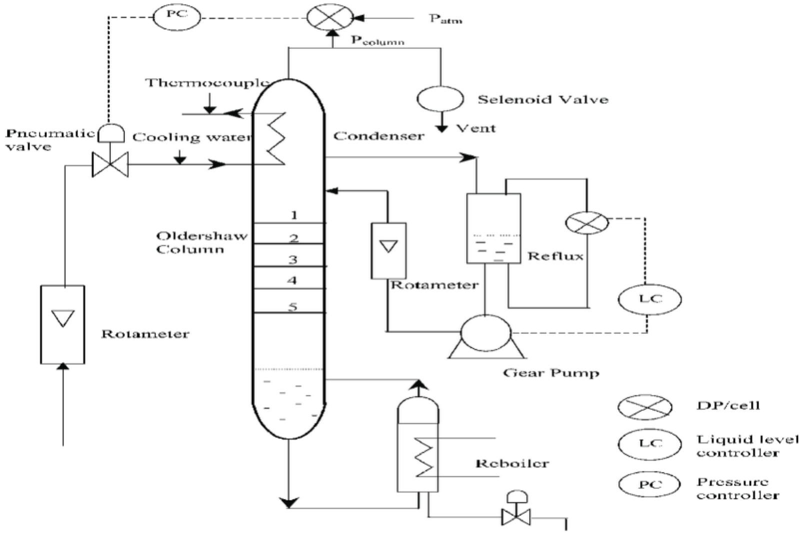
Sharing common pitfalls of IPL credit mostly found during HAZOP/LOPA Revalidation workshops

Example for Partially Dependent IPLs

Partially Dependent Layer of Protection affects decreasing in probability of failure on demand (PFD) if another safeguard did not work well.

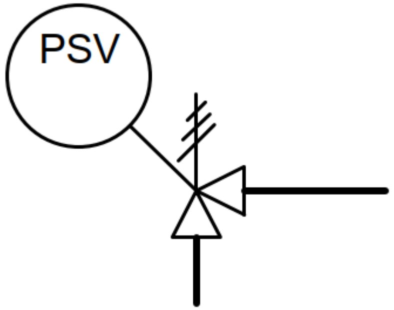
Example: Relief load reduction concept for PSV design by added another safeguard.

Basic Process Control/Interlock



To cut-off feed or heating media in scenario of thermal expansion

Reduce Relief Load



Fire Protection Insulation

To reduce heat flux to inventory equipment in fire scenario.

Reduce Relief Load

Dissimilar-type Double check valve

To reduce probability of reverse flow

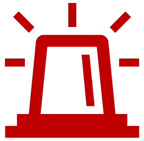
Reduce Relief Load/ Ignore this case

In Sum

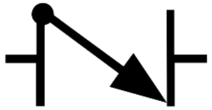
PHA team shall **confirm/verify the design of All credit taken IPLs** to ensure their effectiveness.

Summary

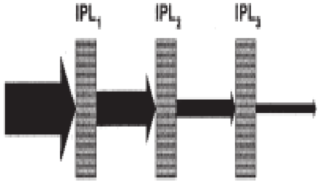
HAZOP/LOPA is not just providing sufficient Layers of protection (IPL) but also need for considering that the provided IPLs are achieved the risk reduction credit or not.



Effectiveness of each Alarm → Alarm Rationalization Study (ARS)



Effectiveness of Check valve → Right design selection and Proper IPL credit given



Effectiveness of Partially Dependent IPL → confirm/verify the design of All IPLs

One IPL may consist of more than one safeguard.

Q&A

Thank you for your attention