INDORAMA VENTURES

Module 4 Safeguard Concepts

Last Revised – April 2024

PS Bootcamp Modules

- ✓ Module 1: Introduction
- ✓ Module 2: Hazard Identification
- ✓ Module 3: Risk Matrix
- ✓ Module 4: Safeguard Concepts
- ❑ Module 5: Explosion/Fire Protection
- ❑ Module 6: Management of Change
- ❑ Module 7: Incident Investigation
- ❑ Module 8: Facility Siting

Agenda

- Introduction to Layers of Protection Analysis
- Basic Process Control System IPLs
- Administrative IPLs
- Safety Instrumented System IPLs
- Mechanical Protective Device IPLs
- Consequence Mitigation System IPLs
- EHS Criticality

Module 4: Training Objectives

Basic Understanding of the LOPA Methodology

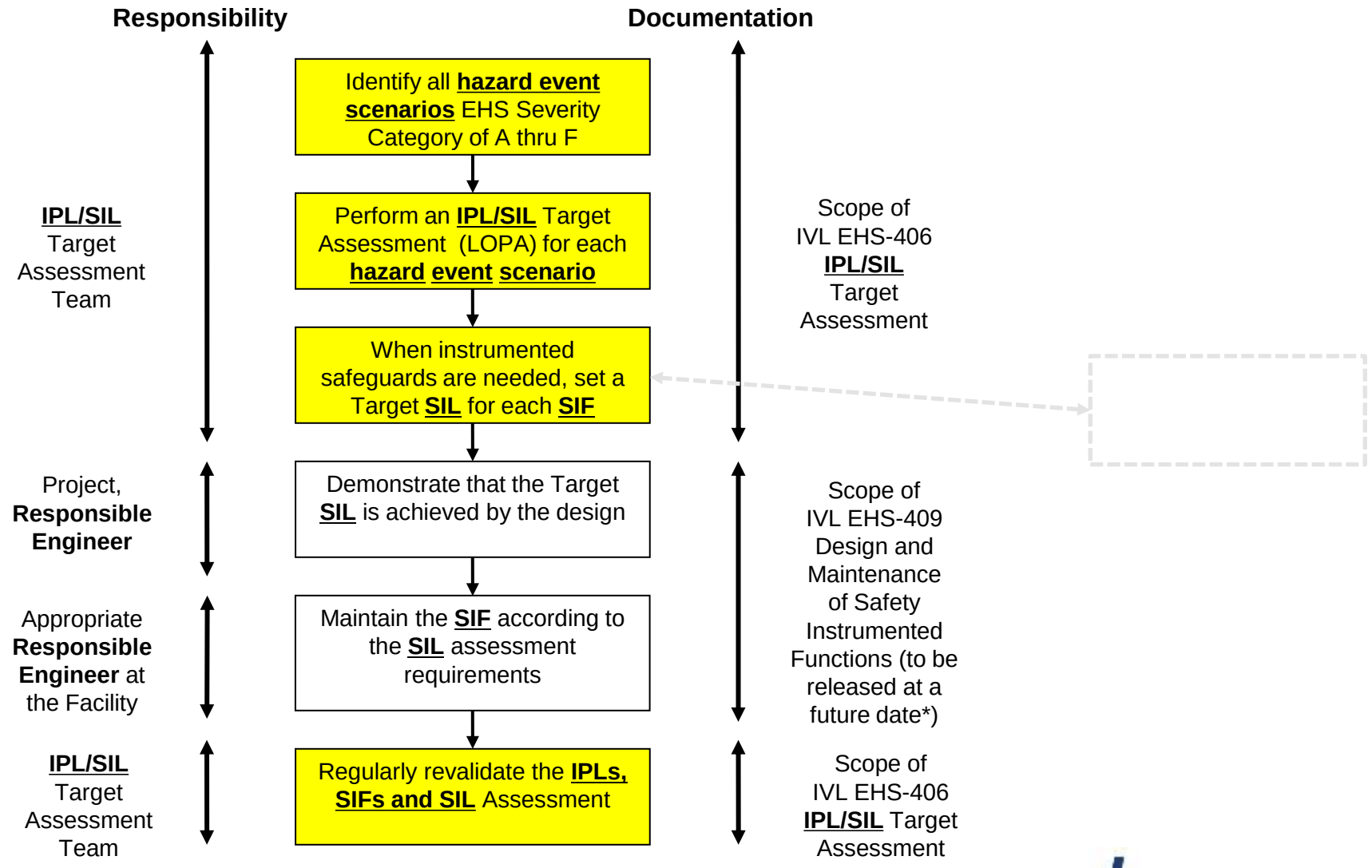
Functional Understanding the Types of Independent Protection Layers (IPLs)

- Basic Process Control System (BPCS IPL)
- Administrative
  - Alarm IPL
  - Standard Operating Procedure (SOP IPL)
- Safety Instrumented System (SIS IPL)
- Mechanical Protective Device
  - Pressure Relief System (PSV IPL)
  - Restricting Orifice (Other IPL)
- Consequence Mitigation Systems

EHS Criticality and the Relationship to LOPAs

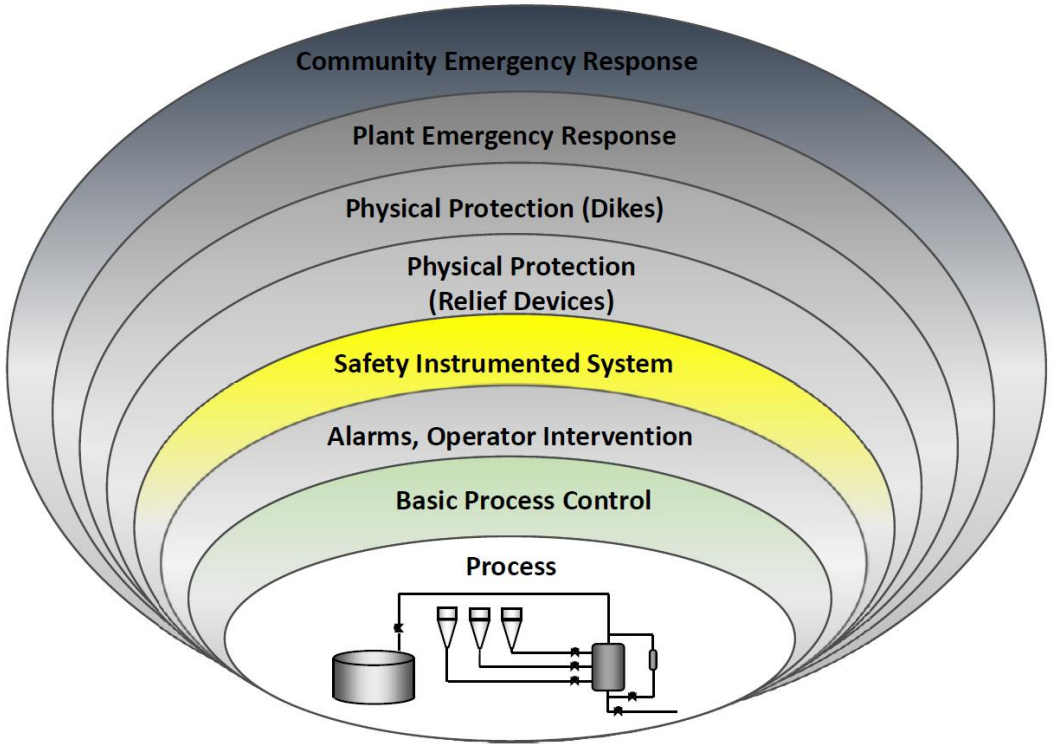
Introduction to Layer of Protection Analysis (LOPA)

IVL EHS-406 IPL/SIL Assessment Lifecycle Flowchart
Allocation of Protection Layers



Presentation Topics

Evolution of LOPA and Why to Perform One
What is LOPA
How to perform a LOPA
General Requirements
Timing
Team Makeup
LOPA Workflow
LOPA Onion and Independent Protection Layers
Limitations/Benefits
Outputs



LOPA Onion

Evolution of LOPA

1992

OSHA 29 CFR 1910.119

Requires PHAs for Safety

1994

EPA 40 CFR 68

Requires PHAs for Environmental

1996

ISA-84.01-1996

Standard specific to the process sector

1998

IEC 61508

Standard for safety-related system design

2001

CCPS LOPA Concept Book published

Formalizes approach

2003

IEC 61511

International standard specific to the process sector; Sets risk assessment and SIL target criteria

2004

ISA-84.00.01-2004

IEC 61511 adopted for US with grandfather clause

2010

IEC-61508 updated

2018

ANSI/ISA-61511

ISA-84 fully integrated IEC-61511

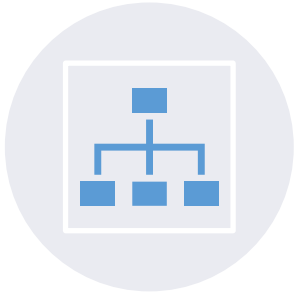
Now

CCPS continues to publish supporting literature

Industry continues to discuss and develop ideas about LOPA

LOPA is an industry standard methodology for completing the risk assessment required by ANSI/ISA-61511

What is LOPA?



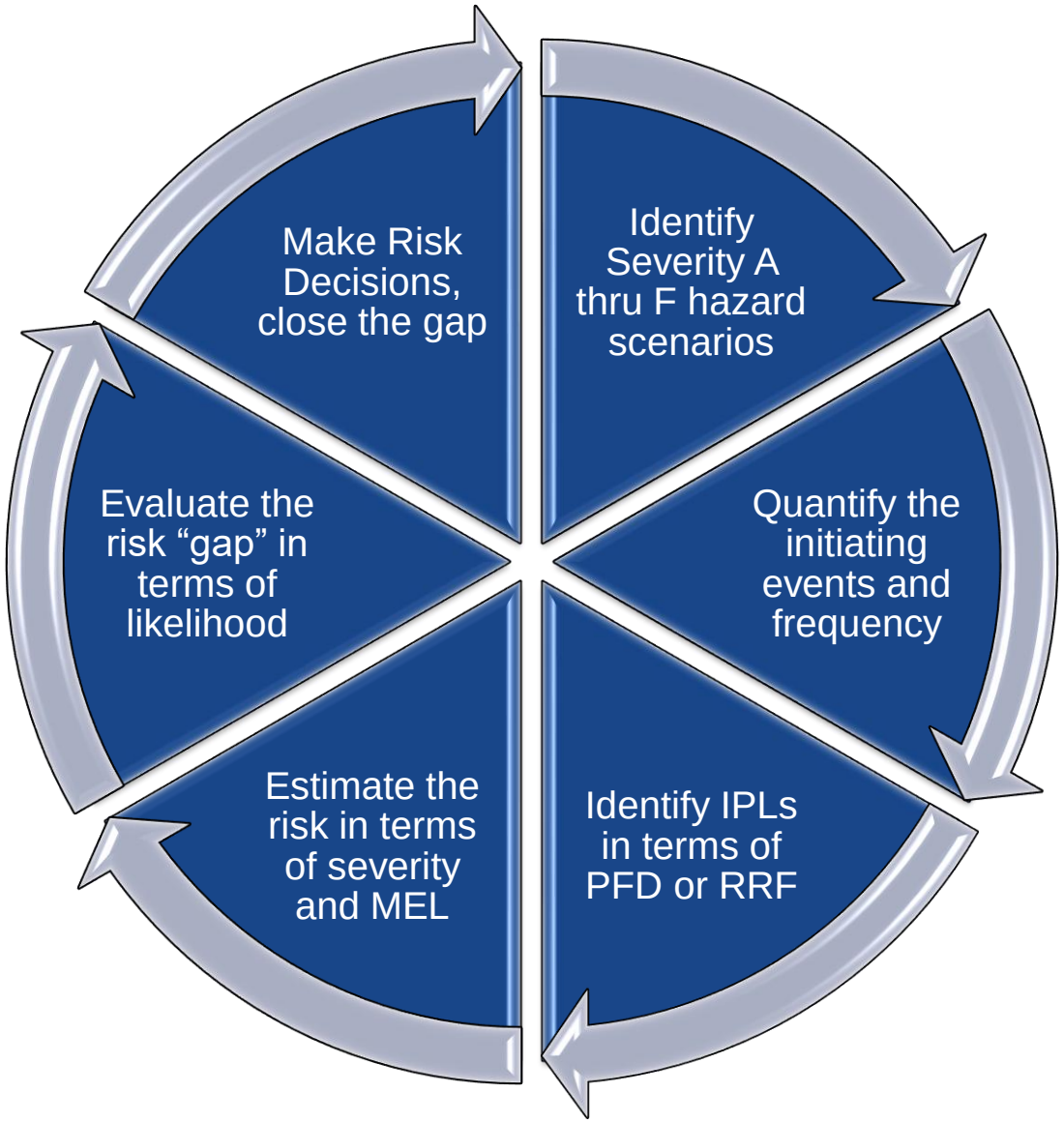
LOPA is a simplified form of risk assessment.

Order of magnitude

LOPA is NOT a scenario identification tool. LOPA refines scenarios identified in other studies such as a PHA.

Determines if there are sufficient layers of protection against a hazard scenario - ***Is the risk tolerable?***

LOPA Process



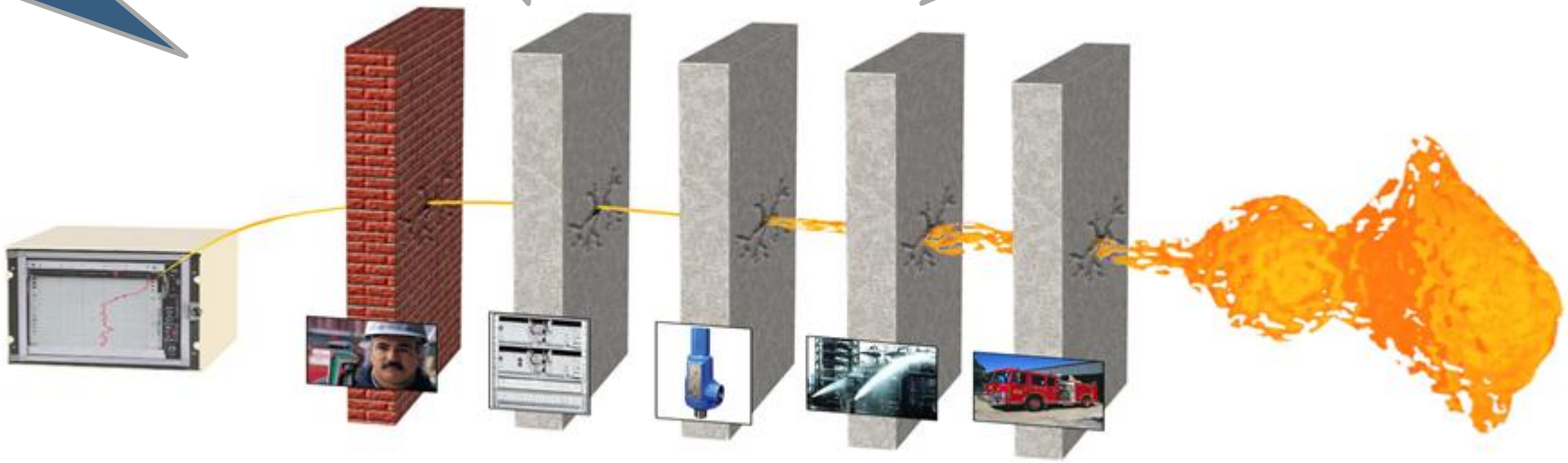
Key Questions for Protection Layers

LOPA was developed around the need to answer questions such as:

How safe is safe enough?

How many protection layers are needed?

How much risk reduction should each layer provide?



LOPA Supports Identifying the Number and Strength of Protection Layers

- ✓ Provides rational, semi-quantitative, risk-based results
- ✓ Reduces emotionalism and bias
- ✓ Quantifies existing risk and basis for recommendations
- ✓ Results in clear and consistent documentation

IVL LOPA Guidelines

Each scenario is made up of a consequence with **all** of its initiating events.

Each initiating event must be given a frequency and assigned IPLs to assess mitigated event likelihood (MEL)

See Tables in IVL EHS-406

The MEL of each initiating event for a single consequence are summed to assess total MEL against target event frequency

Number of IPLs required to achieve the tolerable risk is dependent on the severity of the event and the number and frequency of initiating events

Recognizing the **existing** safeguards that meet the requirements of IPLs for a given scenario is the heart of LOPA

Conditional modifiers such as probability of ignition or probability of people present are appropriate if defensible and all other IPL options are exhausted

General Requirements

Complete IPL/LOPA for Severity A thru F.

Maintain IPL/LOPA Report as current through the Management of Change process for the life of the asset.

IPL/LOPA for each process/unit is to be revalidated at least every 5 years.

Human error scenarios that cannot be addressed with standard LOPA IPLs should be studied using Human Reliability Analysis.

Example: Bleeder valve open after a shutdown managed through a bleeder valve checklist, a tagging policy, or required pressure check prior to introducing hazardous materials

Screening Criteria from IVL EHS-208

Table 1 - Consequence Definitions Severity Categories A-F

Severity Category	Credible Consequence of the Harmful Event		
	On-Site Injuries and Illnesses (One or More of the Consequences Below)	**Off-Site Injuries and Illnesses (One or More of the Consequences Below)**	**Environmental and Other Effects (One or More of the Consequences Below)**
A	Potential for: • 100 or more fatalities	Potential for: • 50 or more fatalities	Release of hazardous material with potential for: • Off-site release with catastrophic off-site damage and long term clean-up (restored in 1 to 5 years) Other Potential Impacts: • More severe release than the level below
B	Potential for: • 50 to 99 fatalities	Potential for: • 10 to 49 fatalities	Release of hazardous material with potential for: • Off-site release with significant clean-up (restored in 1 year) Other Potential Impacts: • More severe release than the level below • Catastrophic contamination of water/land • Catastrophic loss of wildlife and wildlife habitat • Extensive community evacuation • Threat of loss of license to operate
C	Potential for: • 10 to 49 fatalities	Potential for: • 3 to 9 fatalities	Release of hazardous material with potential for: • Off-site release with extensive clean-up (restored in months) Other Potential Impacts: • More severe release than the level below • Severe damage to rivers/sea, flora/fauna or land resulting in recovery time (months) • Severe loss of wildlife and wildlife habitat • Public outrage • Government intervention
D	Potential for: • 3 to 9 fatalities	Potential for: • 1 to 2 Fatalities • Multiple permanent partial disability injuries	Release of hazardous material with potential for: • Off-site release with prolonged clean-up (restored in weeks) Other Potential Impacts: • Major contamination of water/land • Temporary damage to rivers/sea, flora/fauna or land resulting in recovery time (weeks) • Major loss of wildlife and wildlife habitat • Harmful effect on source of drinking water • Community evacuation • Catastrophic impact to property or assets • Damage to relationships with key stakeholders
E	Potential for: • 1 to 2 Fatalities • Multiple permanent partial disability injuries	Potential for: • Permanent partial disability injury • Multiple hospitalizations (over night stay)	Release of hazardous material with potential for: • Off-site release with quick clean-up (restored in days) Other Potential Impacts: • Short term damage to rivers/sea, flora/fauna or land resulting in short recovery time (days) • Minor loss of wildlife and wildlife habitat • Contamination of water/land • Plant Evacuation • Community Shelter-in-Place • Severe impact to site property or assets
F	Potential for: • Permanent partial disability injury • Multiple recordable injuries	Potential for: • Single hospitalization (overnight stay) • Multiple first aid injuries	Release of hazardous material with potential for: • On-site release beyond secondary containment and requiring clean-up and possible response by the site ERT Other Potential Impacts: • Plant Shelter-in-Place • Moderate impact to site property or assets • Regulatory compliance issue which leads to a regulatory consequence, such as a Notice of Violation or Compliance Order • Limited Community Impact

General Requirements continued

Mechanical, instrument, alarm, or administrative systems credited as IPLs shall be tested, inspected and maintained to achieve the availability and integrity level credited to them.

IPLs that protect against Severity Category A thru F are EHS Critical and must meet the requirements of IVL EHS-405, EHS Criticality.

Consequences shall be considered with and without Consequence Mitigation Systems (CMS) during the LOPA.

If a secondary hazard results from activation of a CMS, it shall be analysed as a separate hazard event scenario.

- *The Cause event must start with "Activation of XX"…and the Consequence must start with "Secondary hazard of…"*

General Requirements - Timing

Capital Projects – With Preliminary (HS2) and/or Detailed (HS3) PHA

Management of Change (IVL EHS-204)

Initial PHA or five-year revalidation (IVL EHS-403)

Other sources for Hazard Event Scenarios that could require LOPA

- Facility Siting Assessments
- Incident Investigations
- Fire Risk Assessments
- Design Reviews
- Other Hazard Identification Forums

Timing – Actions

Action items must be closed per IVL EHS-208 Table 3

Existing operating plants:

- EHS-4: Notify Site Head; implement immediate measures to mitigate the risk to EHS-3 or discontinue operations
- EHS-3: Within 9 months for administrative; 66 months for capital expenditure

New design:

- EHS-4: Modify design; apply inherent safety
- EHS-3: Preference to modify design/apply inherent safety; permissible to apply additional safeguards

Whenever further studies are required in order to develop the basis for recommendations, studies should be completed, and resolution identified within 12 months.

SIL Target Assessment (or LOPA) Team Makeup

SIL Target Assessment Team shall consist of at least two competent individuals, comprised of the following:	Optional attendees may include:
• SIL Target Assessment (LOPA) Leader • Process Engineer • Operations Specialist or Operator	• Process Chemist • Maintenance Engineer • Project Manager • Functional Equipment Specialist • EHS/PSM Specialist • Vendor Representative

One person may perform more than one role within the team.

IPL Select Team Makeup

IPL Select Team shall consist of at least four (4) competent individuals, comprised of the following:

- SIL Target Assessment (LOPA) Leader
- Process or Production Engineer
- Operations Specialist or Operator
- **Process Control Engineer**
- **Functional Safety Engineer**

Optional attendees may include:

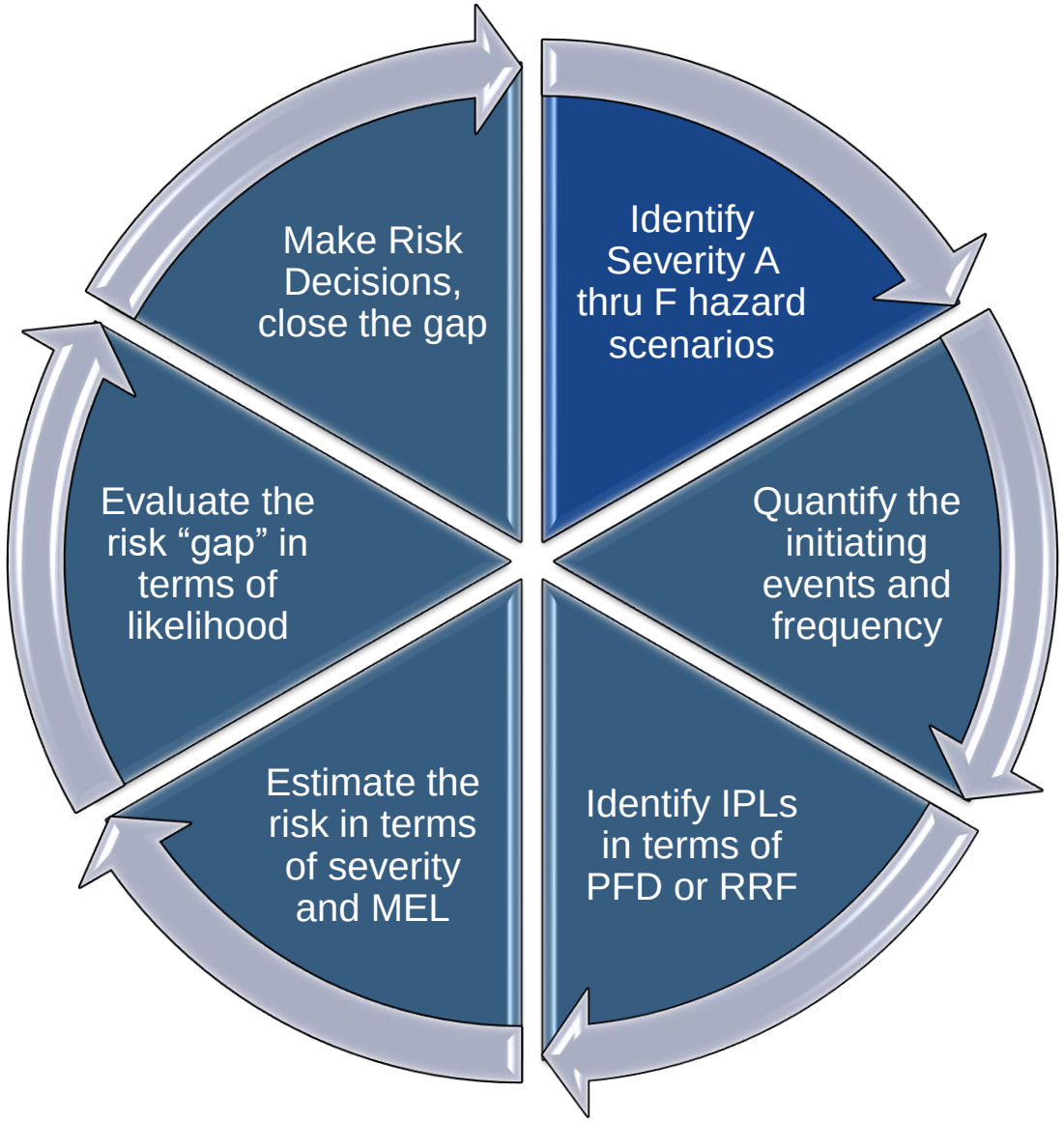
- Process Chemist
- Maintenance Engineer
- Project Manager
- Functional Equipment Specialist
- EHS/PSM Specialist
- Vendor Representative

One person may perform more than one role within the team.

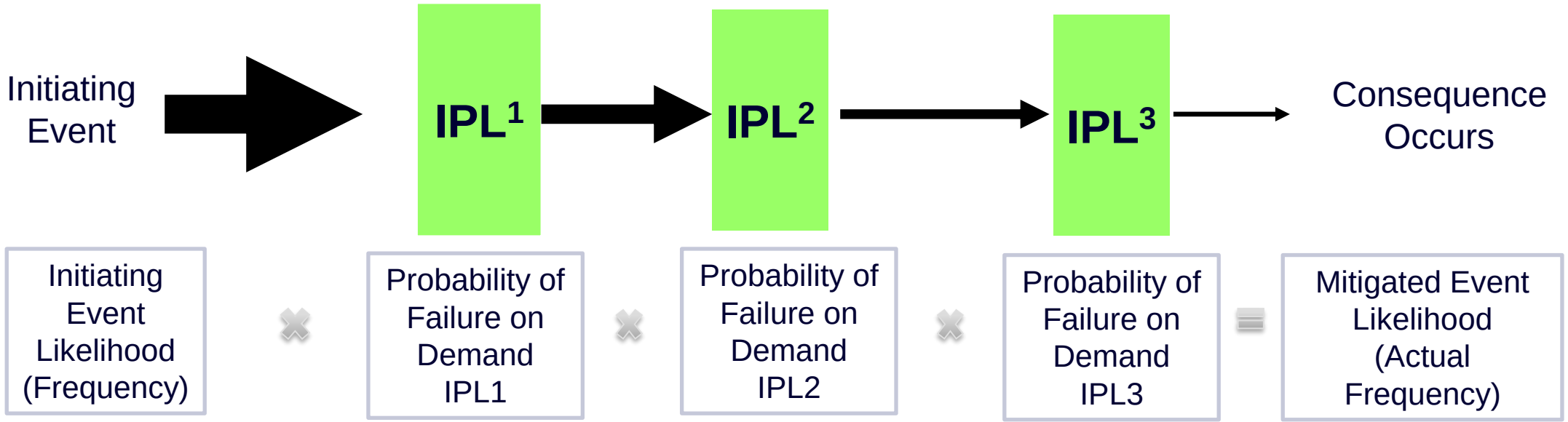
Roles and Responsibilities

Roles and Responsibilities				
Site Head	Appoint IPL/SIL Target Assessment Leader and Responsible Instrument Engineer	Ensure IPL/SIL Target Assessment documentation is passed to the Responsible Instrument Engineer	Oversee the assessment through into design (To be addressed in IVL EHS-409, Design and Maintenance of Safety Instrumented Functions (Plant Trips) and IPL Integrity and Verification at a future date)	Ensure there is a process to keep the IPL/SIL Target Assessment current
Project Manager	Appoint IPL/SIL Target Assessment Leader and Responsible Instrument Engineer	Ensure Responsible Instrument Engineer performs a post-analysis review of assumptions	Oversee the assessment through into design (To be addressed in IVL EHS-409, Design and Maintenance of Safety Instrumented Functions (Plant Trips) and IPL Integrity and Verification at a future date)	
IPL/SIL Target Assessment Leader	Select methodology and ensure it is applied appropriately	Ensure the IPL/SIL Target Assessment complies with regulatory requirements and RAGAGEP	Approve the final IPL/SIL Target Assessment documentation	

LOPA Process



LOPA Math



Target Mitigated Event Likelihood (Target Frequency)

÷

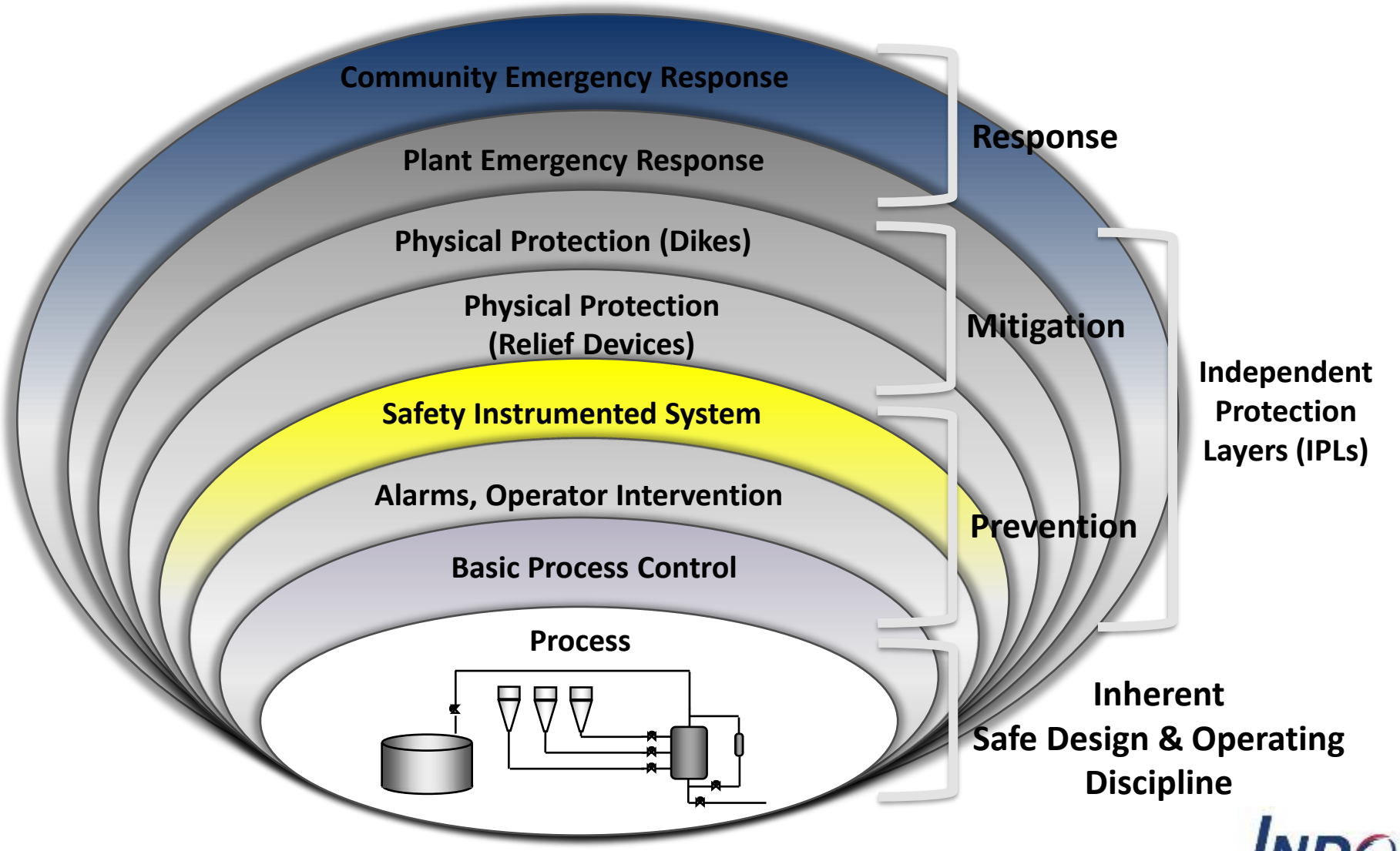
Mitigated Event Likelihood (Actual Frequency)

=

Gap Design Criteria as a Probability of Failure on Demand (PFD)

PFD = 1 or > 1 No Gap
PFD < 1 Gap

Safety Measures and Independent Protection Layers



Common Types of IPLs

Standard Operating Procedure (SOP)

Basic Process Control System (BPCS)

Local Control Loop or Shutdown (LOCAL)

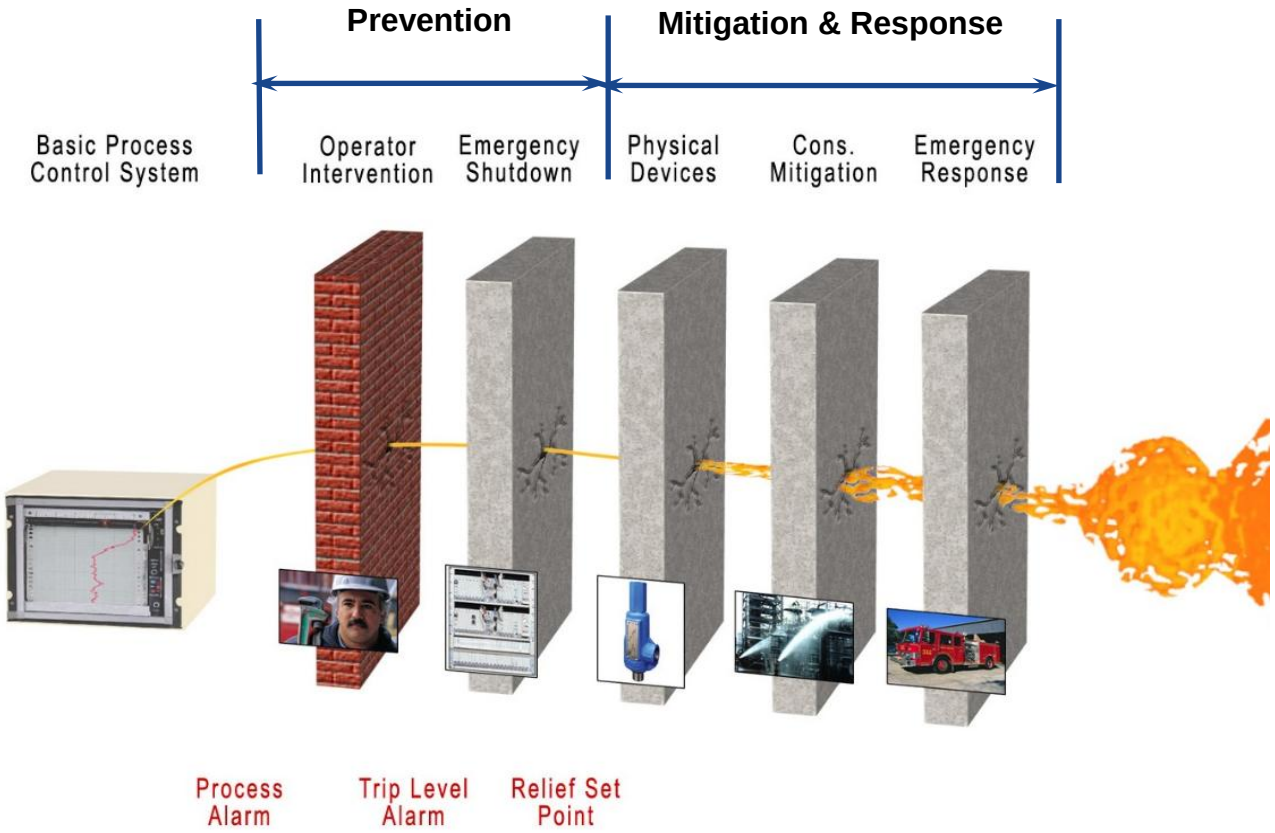
Alarms with Operator Response (ALARM)

Safety Instrumented System (SIS)

Consequence Mitigation System (CMS)

Pressure Relief Valves (SRDs)

Other Miscellaneous (OTHER)



CONSEQUENCES	Target Freq.	CAUSES	Freq	Freq Modifiers	PFD	Independent Protection Layers (IPL 1)	PFD	IPL 2	PFD	Gap	RECOMMENDATIONS
Loss of cooling across Heat Exchanger resulting in increased reaction rate and elevated reactor temperature and initiation of a decomposition reaction. Potential for reactor vessel rupture with release of toxic and flammable EO vapors. Potential for 3 to 9 onsite fatalities. Potential for offsite illness, Injuries and Community Shelter in Place. Release of EO above RQ of 100 lbs. Sev. D	1×10^{-5} (0.00001)	1. Reactor Recirculation Pump (P-1) Malfunctions Off	0.1	Reactor charging EO 10% of the batch time.	0.1	1. BPCS: (FT-1) Low Recirculation Flow closes EO feed valve (FV-1).	0.1	1. (TT-01)(TT-02) 1oo2 High High Reactor Temperature closes EO feed block valves (XV-01) and (XV-02) 1oo2	0.01	1	

This happens when — This happens — AND — This happens — AND — This fails — AND — This fails

MEL (Current Frequency) of the Consequence = [Initiating Causes] X [Frequency Modifiers] X [PFD of IPLs]

MEL = 0.1 x 0.1 x 0.1x 0.01 = 0.00001/yr.

$$\text{PFD gap} = \frac{\text{TMEL}}{\text{MEL}} \quad \frac{\text{Target Frequency}}{\text{Actual Frequency}} = \frac{0.00001}{0.00001} = 1.0$$

$$\text{RRF gap} = \frac{1}{\text{PFD}} = \frac{1}{1} = 1 \text{ RRF}$$

PFD Gap >/= 1 RRF </= 1 No Gap

PFD Gap < 1 RRF > 1 Gap

Risk Management with LOPA

	Frequency Category								
	$\leq 10^{-6}$	$> 10^{-6}$ to 10^{-5}	$> 10^{-5}$ to 10^{-4}	$> 10^{-4}$ to 10^{-3}	$> 10^{-3}$ to 10^{-2}	$> 10^{-2}$ to 10^{-1}	$> 10^{-1}$ to 1	> 1	
Severity Category	1	2	3	4	5	6	7	8	
A	EHS-2	EHS-3	EHS-3	EHS-3	EHS-3	EHS-4	EHS-4	EHS-4	Facility Siting Scope
B	EHS-2	EHS-3					EHS-4	EHS-4	
C	EHS-2	EHS-2	EHS-3	EHS-3	EHS-3	EHS-4	EHS-4	EHS-4	
D	EHS-1	EHS-2					EHS-4	EHS-4	LOPA Scope
E	EHS-1	EHS-2	EHS-2	EHS-3	EHS-3	EHS-3	EHS-4	EHS-4	
F	EHS-1	EHS-1	EHS-2	EHS-2	EHS-3	EHS-3	EHS-3	EHS-4	
G	EHS-1	EHS-1	EHS-1	EHS-2	EHS-2	EHS-2	EHS-3	EHS-3	HazOp Scope
H	EHS-1	EHS-1	EHS-1	EHS-1	EHS-1	EHS-2	EHS-2	EHS-3	

SIF = 0.01
High Temp Trip EO

BPCS = 0.1
Low Flow Trip EO

EE = 0.1
EO Charge

Inherent Risk of Recirc Pump Failure – Loss of Cooling
0.1/yr. Initiating Cause Frequency

Limitations of LOPA

Risk comparisons of scenarios are only valid if the same LOPA methodology/risk tolerance criteria are used.

Numbers generated by LOPA studies are not precise risk values (they are approximations of risk).

In general LOPA studies take more time to complete than qualitative risk studies (PHAs).

LOPA methodology is not intended for hazard identification. LOPA builds upon scenarios that have been identified and developed using a hazard analysis methodology such as HAZOP, PHR, What-If, etc.

Benefits of LOPA

International recognized methodology that provides a more defensible basis for risk-based decision making than qualitative methods.

Requires less time than a Numerical Analysis or Quantitative Risk Analysis (QRA).

Helps to resolve conflicts in likelihood assessments and in defining critical protection layers.

Improves clarity and documentation of risk evaluations.

Consistent methodology provides comparative results across units, plants and companies.

Benefits of LOPA - Continued

Foundation for developing Basis for Safety Concept

Helps to identify risk in operations and practices that were previously thought to have adequate safeguards.

Helps to focus management attention on critical safeguards.

Sets integrity level requirements for each independent protection layer.

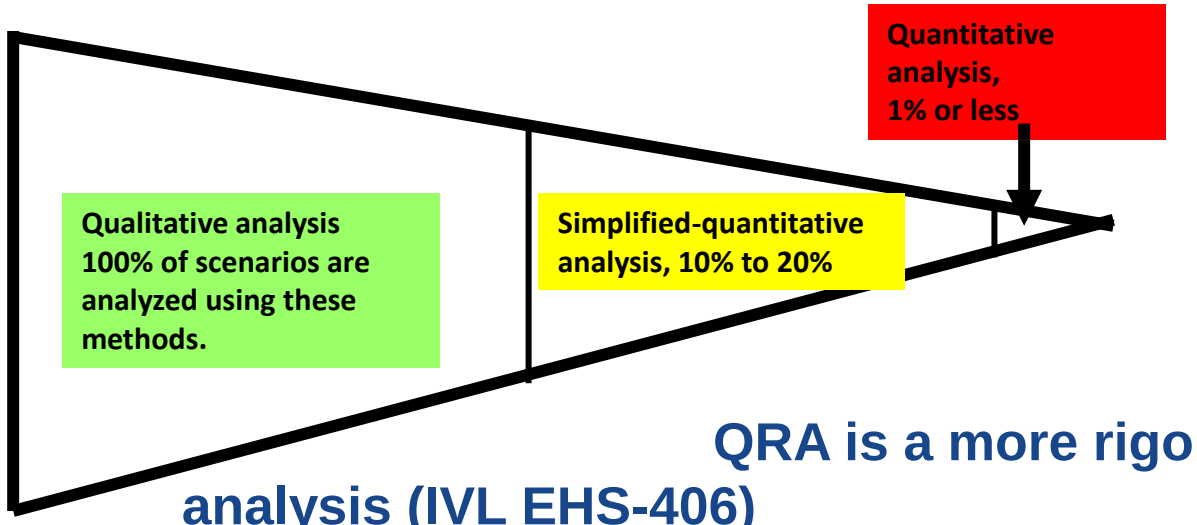
Tool for knowledge-based bypass management.

When to use Quantitative Risk Analysis (QRA)

Complex Severity Category A thru F scenarios

Normal means of safeguards can not be used for gap closure

SIL Category for SIF seems impracticable compared to industry practice



QRA is a more rigorous numerical analysis (IVL EHS-406)

Outputs of LOPA & IPL Select

Documentation Requirements from PHA-Pro® File

Hazard event scenario descriptions with Initiating Causes, Enabling Conditions, IPLs, Conditional Modifiers, MELs, TMELs, RRF Gaps

IPL List

- IPL List (SOP, BPCS, LOCAL, ALARM, SIS, SRDs, and Other)
- Consequence Mitigation System List
- Enabling Event and Conditional Modifier List

EHS Critical Task List

SIF List with SIF Description, Target PFDavg and SIL Rating, Demand Rate

List of Recommendations

IPL descriptions (incl. Alarm and Operator Response and SIF Descriptions)

Instrumented IPLs

F6 Unit - AsBuilt

Unit/ Facility	IPL Type	IPL #	P&ID Drawing	Normal Control Mode	Function Description	Study Name / LOPA Xref	Hazard			Initiating Cause	Process Safety Time (s)	Test Procedures		Inputs					Control Nodes	Outputs		Alarm Location	Operator Procedural (Correcting) Action	PFDavg Target	RRF Target	Safety IPL	Remark
							Node	Deviation	Consequence			Procedure	Test Interval (mo)	Tag	Input Type	Set Point	Tolerance	Engr Units		Tag	Output Type						
F6 Unit	Alarm with Response	F6-ALM-031	F-F6-1-3046		FAL-0260 via FT-260A/B/C Low Hot Oil Flow Alarm with Operator Action to Close FV-0260	O53:07.08.1							66	F6-FT-0260-A	Unknown	6.2	6.2-6.2	MGPM		SOP F6-031	Unknown		Close FV-0260	1.00e-1	10	No	
														F6-FT-0260-B	Unknown	6.2	6.2-6.2	MGPM									
														F6-FT-0260-C	Unknown	6.2	6.2-6.2	MGPM									
F6 Unit	Alarm with Response	F6-ALM-032	F-F6-1-3040		FAL-0290 via FT-290A/B/C Low Hot Oil Flow Alarm with Operator Action to Close FV-0290	O53:07.08.1							66	F6-FT-0290-A	Unknown	6.2	6.2-6.2	MGPM		SOP F6-032	Unknown		Close FV-0290	1.00e-1	10	No	
														F6-FT-0290-B	Unknown	6.2	6.2-6.2	MGPM									
														F6-FT-0290-C	Unknown	6.2	6.2-6.2	MGPM									
F6 Unit	Interlock	F6-PIF-003	F-F6-1-1456 F-F6-1-1788 F-F6-1-1789		Low Low Reabsorber Wash Water Flow (FT-1750A) (FT-1750B) (FT-1750C) 2oo3 [stope Reclaim Compressor C-F6-135 (RY-135CB) 1oo1 OR closes suction valve (XV-0973) 1oo1] 1oo2	O53:23.10.4					51		36	F6-FT-1750-A	Unknown	640	0-1300	GPM		C-F6-135-M1	Motor Contactor - Fail Open		N/A	1.00e-1	10	No	Rev 0, Issued for Design, 3/10/2022 2022 Project Scope: See C0505020007 project SOW. Modification to triplicate sensors included in F6-SIF-056 scope. EHS Procedure 1
														F6-FT-1750-B	Unknown	640	0-1300	GPM		F6-XV-0973							
														F6-FT-1750-C	Unknown	640	0-1300	GPM			On-Off Valve - Pneumatic - Fail Close						
F6 Unit	BPCS	F6-PIF-009	F-F6-1-3042 F-F6-1-920		(AT-6101) or (AT-6102) OMS Outlet (Reactor Inlet) Oxygen Analyzers Control (FV-6104) Oxygen Feed through BPCS Control								0	F6-AT-6101	Unknown					F6-FV-6104	Unknown					No	EHS Procedure 1
														F6-AT-6102	Unknown												
														F6-FT-6104	Unknown												
F6 Unit	BPCS	F6-PIF-011	F-F6-1-1456		(PT-451) Reabsorber Overhead Pressure Control Loop PC-451 will open (PV-451B) with venting to atmosphere at a safe location	O53:19.1.10 O53:19.1.11 O53:19.9.3 O53:22.01.3 O53:22.01.7 O53:22.09.3 O53:23.10.2 O53:23.10.3 O53:23.10.4 O53:23.10.5 O53:23.10.6 O53:25.10.6								66	F6-PT-0451	Unknown					F6-PV-0451-B	Unknown		N/A	1.00e-1	10	No	EHS Procedure 1
F6 Unit	BPCS	F6-PIF-016	F-F6-1-1489		(LT-506A) or (FT-504) Purification Column Level Cascade Control Loop opens (FV-504)	O53:29.06.1							66	F6-LT-0506-A	Unknown					F6-FV-0504	Unknown		N/A	1.00e-1	10	No	
														F6-FT-0504	Unknown												
F6 Unit	Interlock	F6-PIF-017	F-F6-1-1456		High High Reabsorber Overhead Flow (FT-1751A) (FT-1751B) (FT-1751C) 2oo3 closes (PV-0451A) 1oo1 OR (HV-1057) 1oo1 to isolate the Incinerator Seal Pot and Waste Gas System	O53:24.10.1g					47		60	F6-FT-1751-A	Unknown	10	0-12	MPPH		F6-HV-1057	Unknown		N/A	1.00e-1	10	No	Rev 0, Issued for Design, 3/10/2022 2022 Project Scope: See C0505020007 project SOW. Modification to triplicate sensors included in F6-SIF-058 scope.
														F6-FT-1751-B	Unknown	10	0-12	MPPH		F6-PV-0451-A	Unknown						
														F6-FT-1751-C	Unknown	10	0-12	MPPH									
F6 Unit	Interlock	F6-PIF-018	F-F6-1-922		Low Contactor F-F6-102 Level (LT-1565A) OR (LT-1565B) as selected in the PLC closes Contactor Bottoms Valve (XV-1565)	O53:14.01.3							60	F6-LT-1565-A	Level Transmitter	15	15-15	%		F6-XV-1565	On-Off Valve - Pneumatic - Fail Close		N/A	1.00e-1	10	No	
														F6-LT-1565-B	Level Transmitter	15	15-15	%									

Severity Type Options: Custom (Safety, Environmental, Commercial, Reputational, Include Data without Targets)

Project IPLs: All

Name	Description	PHA Reference	SIF Type	Target		Achieved			Inputs				Sensor Group Voting	Outputs				FE Group Voting	Logic Solvers		Remarks
				IL	RRF	IL	RRF	PFD	Tagname	Testing Interval (months)	Voting	Drawings		Tagname	Testing Interval (months)	Voting	Drawings		Logic Solver	Testing Interval (months)	
F6-SIF-001	OMS Discharge High Oxygen measured at (AT-6101) OR (AT-6102), whichever is not selected as BPCS control, OR High Oxygen measured by any 1 of 2 of the 6 reactor outlets (AT-6201) (AT-6202) (AT-6203) (AT-6204) (AT-6266) (AT-6296) closes OMS Unit Oxygen Feed Block Valves (XV-6116) (XV-6119) 1oo2	O53:01.08.1 O53:01.10.2 O53:01.10.3 O53:02.07.2 O53:02.13.1 O53:04.01.2 O53:04.08.1 O53:04.08.3 O53:04.09.3 O53:04.10.1 O53:04.10.2 O53:04.10.3 O53:04.10.4 O53:04.15.2 O 53:12.08.10 O53:15.04.1 O53:15.04.4 O53:19.4.1 O53:19.4.2	SIF	3	2,116	3	2,145	4.66e-4	F6-AT-6101 F6-AT-6102	0	1oo1	F-F6-1-3042	1oo2	F6-XV-6116 F6-XV-6119	8	1oo2	F-F6-1-920	1oo1	F6-SIS-LS-1	60	O2 Analyzer Test Frequency is 3 days per SIL calculations.
									F6-AT-6201 F6-AT-6202 F6-AT-6203 F6-AT-6204 F6-AT-6266 F6-AT-6296	0	1oo2	F-F6-1-1452 F-F6-1-3039 F-F6-1-3043 F-F6-1-3044 F-F6-1-3045 F-F6-1-571									
F6-SIF-002	(PT-1747A) (PT-1747B) (PT-1747C) High High Cycle Gas Pressure shutdown of Ethylene Feed closing Block Valves (XV-1704A) (XV-1704B)	O53:01.07.3	SIF	2	1,000	2	1,141	8.76e-4	F6-PT-1747-A F6-PT-1747-B F6-PT-1747-C	60	2oo3	F-F6-1-3042	1oo1	F6-XV-1704-A F6-XV-1704-B	60	1oo2	F-F6-1-3042	1oo1	F6-SIS-LS-1	60	
F6-SIF-003	Low Side Draw Pot Level (LSLL-1710) to shut off EO Transfer Pumps P-F6-194A/B contactors (P-F6-194A-M3) & (P-F6-194B-M3) 1oo1, only one pump is considered running	O53:30.06.1 O53:30.06.2	SIF	1	12	1	12	7.88e-2	F6-LSLL-1710	48	1oo1	F-F6-1-1489	1oo1	P-F6-194-A-M1 P-F6-194-A-M2	25	1oo2	F-F6-1-3113	1oo1	F6-SIS-LS-1	60	F6-SIF-003 is used in conjunction with F6-SIF-035/036 to satisfy the RRF target. Combined target RRF = 40,000 Combined achieved RRF = 40,673
														P-F6-194-B-M1 P-F6-194-B-M2	25	1oo2	F-F6-1-3113				
F6-SIF-004	Low Sparger Differential Pressure measured at (PDT-6110A) (PDT-6110B) (PDT-6110C) closes O2 Block Valves (XV-6116) (XV-6119) 1oo2 AND opens H-6-102 Nitrogen Purge Valves (XV-6121A) (XV-6121B) (XV-6121C) 1oo3	O53:02.08.1a O53:02.08.1c O53:03.08.1	SIF	3	1,050	3	1,168	8.56e-4	F6-PDT-6110-A F6-PDT-6110-B F6-PDT-6110-C	60	2oo3	F-F6-1-3042	1oo1	F6-XV-6116 F6-XV-6119	8	1oo2	F-F6-1-920	2oo2	F6-SIS-LS-1	60	
														F6-XV-6121-A F6-XV-6121-B F6-XV-6121-C	60	1oo3	F-F6-1-920				
F6-SIF-005	Sparger High Differential Temperature measured at (TT-6110A) (TT-6110B) (TT-6110C) 2oo3 with (TT-1329A)/ (TT-1329B)/ (TT-1329C) OR (TT-6802A) (TT-6802B) (TT-6802C) 2oo3 with (TT-1329A)/ (TT-1329B)/ (TT-1329C) closes OMS Unit Oxygen Block Valves (XV-6116) (XV-6119) 1oo2	O53:02.10.1	SIF	3	2,000	3	3,010	3.32e-4	F6-TT-1329-A F6-TT-1329-B F6-TT-1329-C F6-TT-6802-A F6-TT-6802-B F6-TT-6802-C	60	Complex	F-F6-1-3042	2oo2	F6-XV-6116 F6-XV-6119	8	1oo2	F-F6-1-920	1oo1	F6-SIS-LS-1	60	
									F6-TT-1329-A F6-TT-1329-B F6-TT-1329-C F6-TT-6110-A F6-TT-6110-B F6-TT-6110-C	60	Complex	F-F6-1-3042										

Summary of Key Points

What - LOPA is a semi-quantitative methodology to assess the frequency of a hazard scenario

Why – LOPA is IVL ’s preferred method for identify IPLs, defining the functional safety requirements for SIFs, and the related EHS Critical List

How – PHA/LOPA and IPL Selection Teams and LOPA Workflow, IVL EHS-406, IPL/SIL Target Assessment

When – During or soon after the PHA or other process activity that defines a Hazard Scenario

Questions/Comments

Independent Protection Layers

Independent Protection Layers

Topics to be Covered

What is an IPL?

Preventative and Mitigative IPLs

Passive and Active IPLs

IPL Rules and Characteristics

Purpose of IPL

PFD_{avg} and RRF

IPL Types

Examples

What is an IPL?

IPL Definition: An IPL is a device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the Initiating Event or the action of other IPLs associated with a scenario.

Typical IPLs: BPCS, SIS, Alarm with operator response, pressure regulator, pressure relief, restricting orifice, etc.

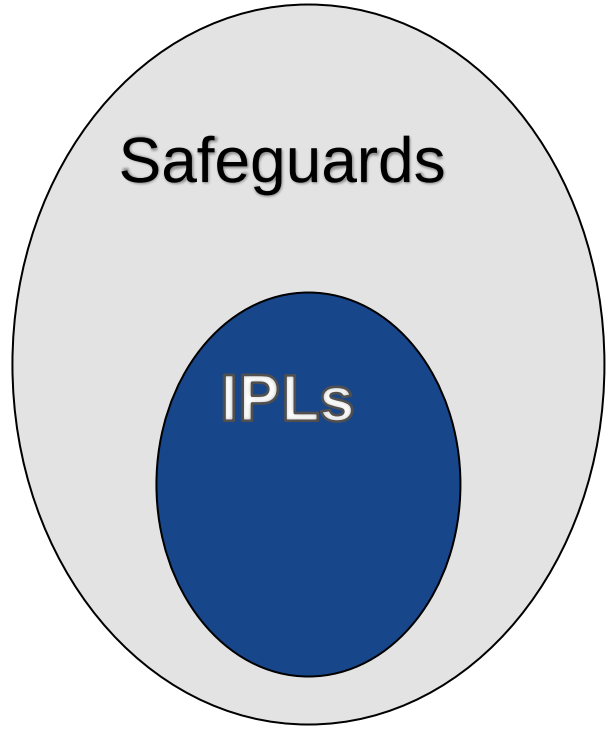
IPLs should be considered when the initiating cause frequency is greater than the Target Mitigated Event Likelihood.

Safeguards vs IPLs

What is the distinction between an IPL and a Safeguard?

- **Safeguard** - Any device, system or action that would likely interrupt the chain of events following an Initiating Event. (e.g., operator training)

- **IPL** - A device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the Initiating Event or action of other IPLs associated with this scenario (e.g., BPCS Trip). IPLs are credited with specific risk reduction.



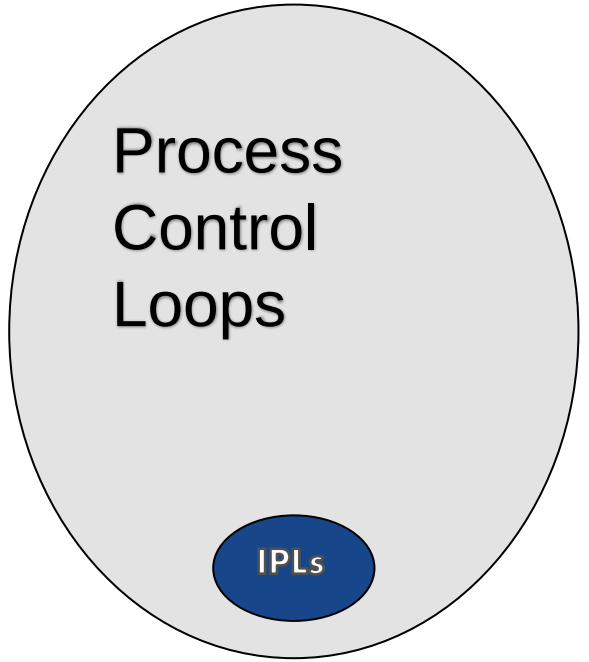
All IPLs are safeguards, but not all safeguards are IPLs.

Process Control Loop vs IPLs

What is the distinction between an IPL and process control loop?

- **Process Control Loop** – All the physical components and control functions to automatically adjust a value of a measured process variable (PV) to equal the value of a desired set-point (SP) (e.g., sensor, logic solver, final control element)

- **IPL** - A device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the Initiating Event or action cf other IPLs associated with this scenario (e.g., BPCS Trip). IPLs are credited with specific risk reduction.



Most Process Control Loops are not IPLs.

Preventative and Mitigative IPLs

IPLs can be Preventative or Mitigative

- **Preventative:** Occurs after the initiating event but prior to the loss of containment event
- **Mitigative:** Occurs after the loss of containment but prior to the consequence of concern

Preventative IPLs are preferred over Mitigative IPLs!

Passive and Active IPLs

IPLs can be Passive or Active

Passive: Not required to take an action to achieve its function in reducing risk

- *Examples: Dikes or bunds, blast walls, flame arrestors*

Active: Required to move from one state to another in response to a change in a measurable process property or a signal from another source

- *Examples: Automated shutoffs, operator response, pressure relief valves, gas detection and deluge, etc.*

Passive IPLs should be evaluated as IPLs and not as part of the consequence determination. Passive IPLs are preferred over Active IPLs.

IPL Rule Set

IPLs must be:

Specific	Designed with the “functionality” to prevents or mitigate the consequence of the identified hazard scenario
Independent	Of the initiating event and the components of any other IPL on the same scenario
Dependable	Have the “integrity” to meet the required specifications and “reliability” to operate as intended for a specified period of time
Auditable	Capable of validating periodically from documentation
Access Security and MOC	Is managed by design or administrative procedure to prevent unauthorized changes

Indorama's Types of IPL

- Standard Operating Procedure (SOP)
- Basic Process Control Loop (BPCS)
- Local Control Loop or Shutdown (LOCAL)
- Alarms with Operator Response (ALARM)
- Safety Instrumented System (SIS)
- Consequence Mitigation System (CMS)
- Pressure Relief Valve (SRD)
- Other Miscellaneous (OTHER)

SOP IPLs - Preventative

Written and auditable procedure

Readily available to all operating personnel

Requires a written log of the pertinent process variable being used to detect the initiating cause

- **Lists the required operator action(s)**
- **Describes the details of the alarm and its functionality**
- **Must be independent of the initiating cause and all other IPLs including alarm IPLs**
- **Only one SOP IPL per hazard event scenario**
- **No more than two administrative IPLs (SOP or Alarm) can be used on any single hazard event scenario**
- **Should be considered AFTER inherent safety and automated or partially automated IPLs (SIS, LOCAL, BPCS, ALARM)**

BPCS IPLs - Preventative

- Implemented in the system used for normal process control
- May be DCS or PLC-based
- Must completely prevent or mitigate the hazard event scenario without assistance from systems
- Sensors, logic solvers and final elements must be independent of the initiating cause, events, and other IPLs
- Must run in automatic mode during all operational phases when the hazard event scenario exists (designed to function “stand-alone”)
- Trip points cannot be set from the operator graphical interface
- Must meet the limitations in Tables C-5 and C-7 of EHS-406

BPCS Initiating Events and IPLs – Two Credits

If the initiating cause is in the BPCS, then only one BPCS can be used as an IPL

If the initiating cause and enabling event(s) do not involve the BPCS, then up to two BPCS IPLs can be credited provided that the only common element is the logic solver

Each BPCS IPL function requires:

- I/O, sensors, final elements, and communication bus for each function shall be independent of the initiating cause, any enabling event, or any other device, system or action already credited as an IPL for the same hazard event scenario.
- The BPCS IPL must run in automatic (i.e., non-settable) mode during all operational phases, and be designed to function in truly "stand alone" fashion.
- Such installations shall be proven in use to be highly available and reliable.
- There shall be appropriate management of change and security procedures and practices in place to ensure the integrity of the IPL and related software.
- Accepted configuration for BPCS system shall include redundancy and fault tolerance of control processors and communications between control processors and I/O modules.

Note: taking greater than a FRF of 10, or less than a PFDavg of 0.1, is outside the limit established by IEC 61511 unless all of the associated requirements noted in Figure C-3, IVL EHS-406, are met and adequate demonstrations are made.

LOCAL IPLs - Preventative

NOT implemented in the system used for normal process control

Typically, locally hardwired (relay logic)

May be used when the initiating event is in the BPCS

Risk reduction is limited by the integrity of the individual devices and logic solver

Sensors, logic solver and final elements must be independent of the initiating event and all other IPLs

If RRF > 10 is applied to a local IPL, the IPL should be submitted for evaluation by an SIS engineer as an SIS IPL

- Typically, local hardwired functions cannot achieve higher than a mid-level SIL 1 capable function.
- RRF < 100 (less than 2 levels of credit)

ALARM IPLs - Preventative

Operator response to alarm must be specific

Operator has sufficient time to respond (Table C-5 through C-8)

Operator response must be proceduralized and operator is trained on the response

Operator is independent of the initiating cause and all other IPLs

Alarm is not operator re-settable

Operator cannot inhibit or modify the set point

Only one alarm with operator response per hazard event scenario

No more than two administrative IPLs (SOP or Alarm) can be used on any single hazard event scenario

If the alarm is implemented in the BPCS, all rules for applying BPCS credit apply

ALARM IPLs - Cont'd.

The following are considerations when assigning credits to an Alarm with Operator Response IPL:

Timing:

- A single console operator in the control room must have at least 10 minutes to respond. The console operator must be able to take action from the control room.
- A single field operator in the field must have at least 30 minutes to respond. If the console operator must notify the field operator of the condition, then the console operator must also be independent of the initiating cause and other IPLs.

If multiple console operators in the control room or multiple field operators in the field will receive the same information and can make independent responses, then two levels of operator credit are permitted (Table C-7 of IVL EHS-406).

- All other criteria for Alarm IPLs including the timing criteria above apply when taking multiple Alarm credits

SIS IPLs – Preventative Key Terms

SIF – Safety Instrumented Function

- A combination of sensors, the logic solver and final elements with a specified safety integrity level that detects an out-of-limit (abnormal) condition and brings the process to a functionally safe state without human intervention, or by initiating a trained operator response to an alarm.

SIS – Safety Instrumented System

- Instrumented system used to implement one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), Logic Solver(s), and final elements(s).

SIL – Safety Integrity Level

- Discrete level (one out of three) for specifying the safety integrity requirements of the Safety Instrumented Functions to be allocated to the safety instrumented systems.

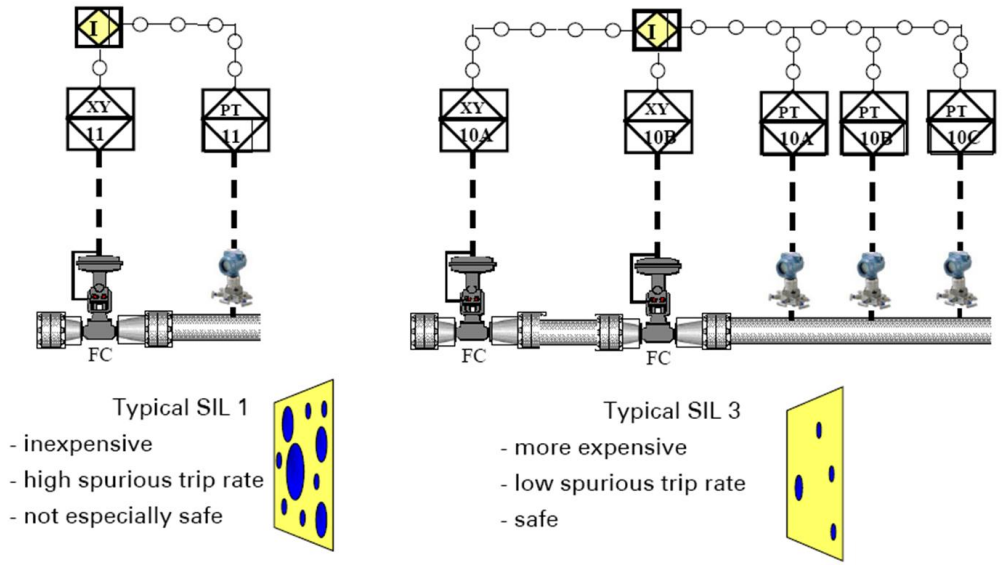
SIS IPLs - Preventative

NOT implemented in the system used for normal process control

Meet the requirements of ANSI/ISA 61511

- Safety Requirements Specification
- SIL Calculations
- Functional Proof Test Plan

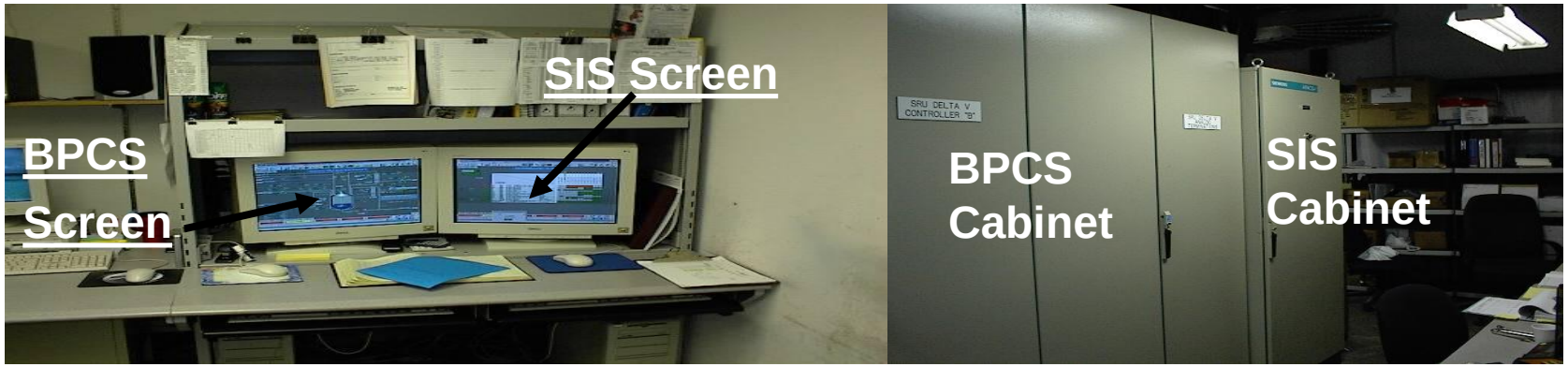
Functional Testing in Place

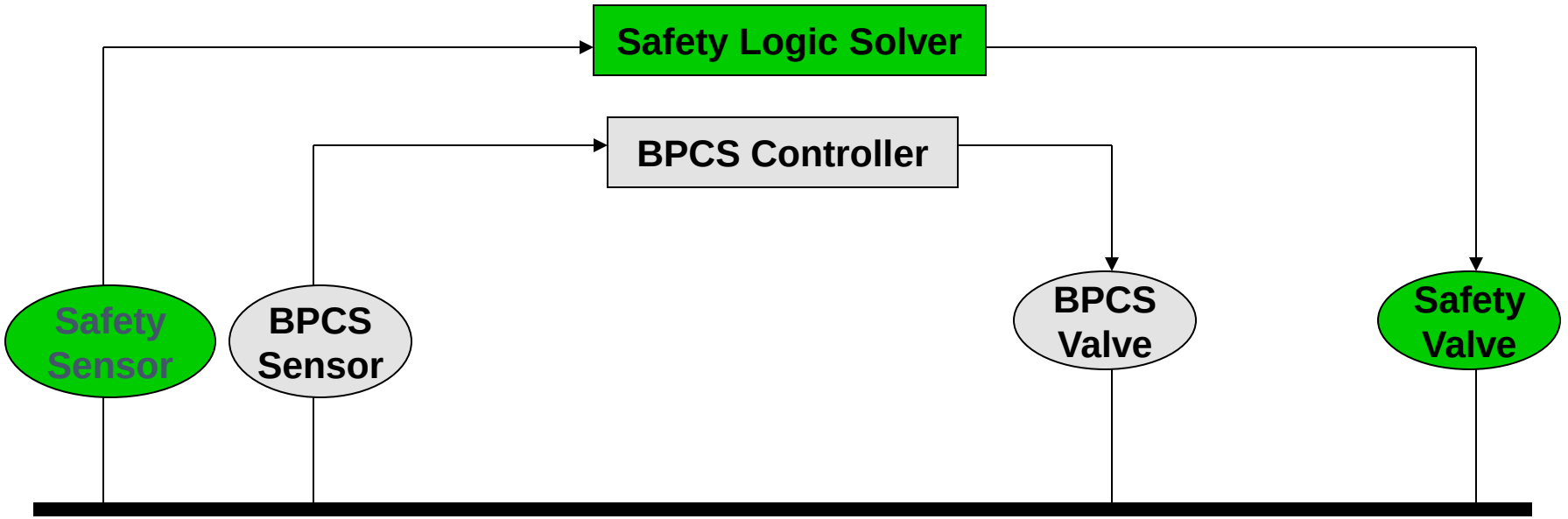


Demand rate and historical test results support its use in this service

SIS Independence

INDEPENDENCE





CMS IPLs - Mitigative

Occurs after the loss of containment has occurred

Prevents the consequence of concern

Includes fire and gas systems, etc.

- Must be designed to mitigate the hazard event scenario (e.g., knock-down vapors or prevent radiant heat knock-on effects.)
- Must be independent of the initiating cause and all other IPLs
- For manually initiated IPLs, operator and operator response must be independent of the initiating cause and all other IPLs
- May reduce the frequency of an escalated event or the consequence
- When reducing the consequence, requires evaluation of the consequence after CMS activation

This may require evaluation of TWO or more scenarios.
The original consequence mitigated by the CMS, and any secondary consequences after activation of the CMS.

Pressure Relief - SRD IPLs
Preventative and Mitigative

Ensure that activation of the relief device under demand is addressed in study.

- This requires setting up a secondary scenario for the relief case to assess if it vents to a safe location.

Ensure that the relief devices are sized for the scenario of concern. Evaluate the relief cases.

- If the relief case does not exist, make a recommendation to evaluate the relief case.

Multiple relief valves can only be given credit if all valves can independently resolve the scenario and they have staggered set-points to eliminate chatter

Multiple relief valves cannot exceed three levels of credit (PFD_{avg} >= 0.001).

Other IPLs

The following are considerations when using an Other Miscellaneous IPL:

Do not fit into any of the categories already listed

Typically, physical or mechanical devices

- Bunds, Dikes, Blast Walls
- Flame or Detonation Arrestors
- Mechanical stops on valves

May also be:

- Enabling Events
- Conditional Modifiers

Other IPLs

When utilizing pump seals as a layer of protection:

Ensure that the seal is a double-mechanical seal.

Ensure that there is indication of seal failure.

- There must also be a method to address seal failure.

If detection is not automated, seal failure is typically found on operator rounds, therefore scenario timing and SOP must be addressed.

The detection method would drive this to be an ALARM IPL or an SOP IPL

Exercise

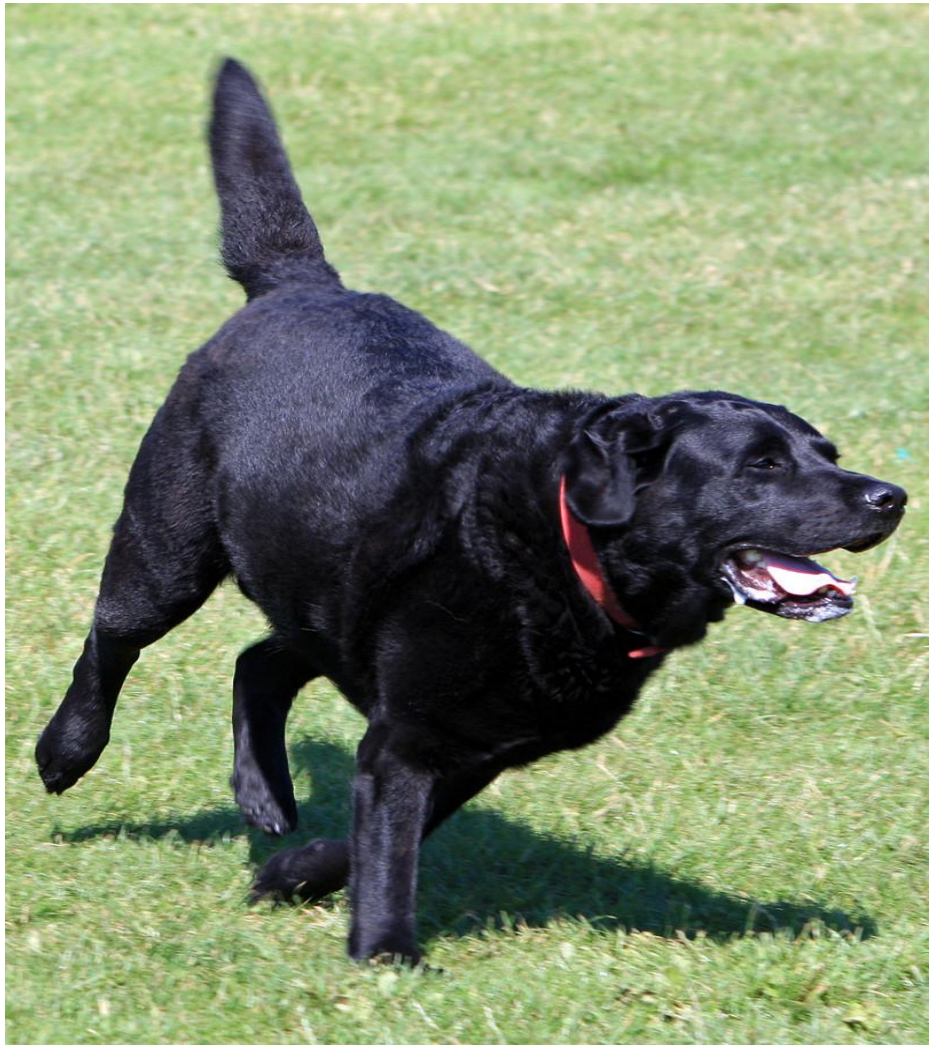
Dog and Goldfish:

A Labrador runs through a kitchen chasing a bird which flew in through the window.

The Labrador loses control, slides across the floor and knocks a shelf holding a stack of cookbooks.

One of the cookbooks falls from the shelf onto a goldfish bowl below, which is fatal to the goldfish.

What are four ways to prevent this consequence?



Exercise

Dog and Goldfish:

1. Move the goldfish to a location with no hazards from above (inherent safety)

2. Provide screening on the window so the bird cannot enter (passive IPL)

3. Constantly stand beside the shelf and catch the book before it hits the goldfish (active IPL)

4. Provide PPE for the goldfish (general safeguard)

Questions/Comments

Module 04 - Breakout Exercises

Review the Breakout Examples provided.

Use the P&IDs provided and the comments in the LOPA worksheets as a basis.

Complete the following sections:

- **IPLs**
- **CMS**

Breakout Exercise Solutions

Example 1 (Storage Tank Overfill)

IPL 1:

- **Description:** High Level LT-102 on T-1 operator alarm with response to stop feed
- **Prob (0 to 1):** 0.1
- **Justification:** Alarms - single console operator with >10 minutes response time, annunciated in control room, alarm independent of cause, trained on response with procedures available to review. alarm is not re-settable
- **IPL/CMS/EE/CM:** IPL

IPL 2:

- **Description:** High High-Level LT-103 on T-1 closes LCV-103
- **Prob (0 to 1):** 0.025
- **Justification:** SIS: Must be independent of BPCS hardware and software. Achieves SIL 1.
- **IPL/CMS/EE/CM:** IPL

What questions should be asked to validate each of these IPLs?
What if the alarm was for the field operator?

Breakout Exercise Solutions

Example 2 (Pump Deadhead)

IPL 1:

- **Description:** Low low flow FT-202 at pump discharge stops pump P-2
- **Prob (0 to 1):** 0.1
- **Justification:** SIS: Must be independent of BPCS hardware and software. Achieves SIL 1.
- **IPL/CMS/EE/CM:** IPL

The available credit for this SIF has not been provided, therefore we will assign the lowest permissible credit for a SIL 1 (Prob = 0.1)

How could the SIF be assigned more credit?

Breakout Example Solutions

Example 3 (Reactor Explosion)

IPL 1:

- **Description:** PRV-302 on R-3 set at 300 psig relieves to flare
- **Prob (0 to 1):** 0.01
- **Justification:** Relief Valve - clean service PRV sized to completely mitigate the scenario
- **IPL/CMS/EE/CM:** CMS

IPL 2:

- **Description:** High high temperature TT-303 on R-3 opens quench valve TV-303
- **Prob (0 to 1):** 0.1
- **Justification:** SIS: Must be independent of BPCS hardware and software. Achieves SIL 1.
- **IPL/CMS/EE/CM:** IPL

Does anything else need to happen at this point?

Breakout Exercise Solutions

Further Discussion

For each of the examples discussed, were the IPLs applied active or passive?

Are there any potential opportunities in these scenarios for passive IPLs? If so, what are they?

- Discuss any further implications of applying potential passive IPLs.

Summary of Key Points

Defined an IPL

Discussed differences between preventative and mitigative IPLs and between passive and active IPLs

Discussed general rules and characteristics of IPLs

Discussed the different types of IPL

Discussed the need to assess the secondary hazards of CMS IPLs

Discussed how to represent the effectiveness of an IPL: PFD_{avg} and RRF

Discussed key Tables within EHS-406

- Table C-4 Typical Initiating Cause Frequencies
- Table C-5 Risk Reduction Factors (With BPCS Initiating Causes)
- Table C-6 Risk Reduction Factors (With Human Factor Initiating Causes)
- Table C-7 Risk Reduction Factors (With Other Initiating Causes)
- Table C-8 Risk Reduction Factors (Misc. Initiating Causes)
- Table C-9 Risk Reduction Factors (Based on Consequences Mitigation Systems)

EHS Criticality IVL EHS-415

Definition: EHS Critical IVL EHS-405

EHS Critical Protective Devices: **Any single device, or combination of devices, which are identified in an EHS permit, regulatory, and/or corporate requirement or in a PHA as an Initiating Cause, a Conditional Modifier, an Independent Protection Layer (IPL), or a Mitigation Device that is intended to prevent or mitigate non-compliance or Severity Category F or more severe hazardous process safety events.**

EHS Critical Equipment: **Any equipment whose failure, as identified in an EHS risk assessment and/or PHA, could credibly result in a Severity Category F or more severe consequences or whose failure could lead to non-compliance with EHS permit, regulatory, or corporate requirements.**

EHS Critical Structures and Foundations: **Any structures and/or foundations designed to hold / support or contain / isolate (e.g., blast walls) EHS Critical equipment.**

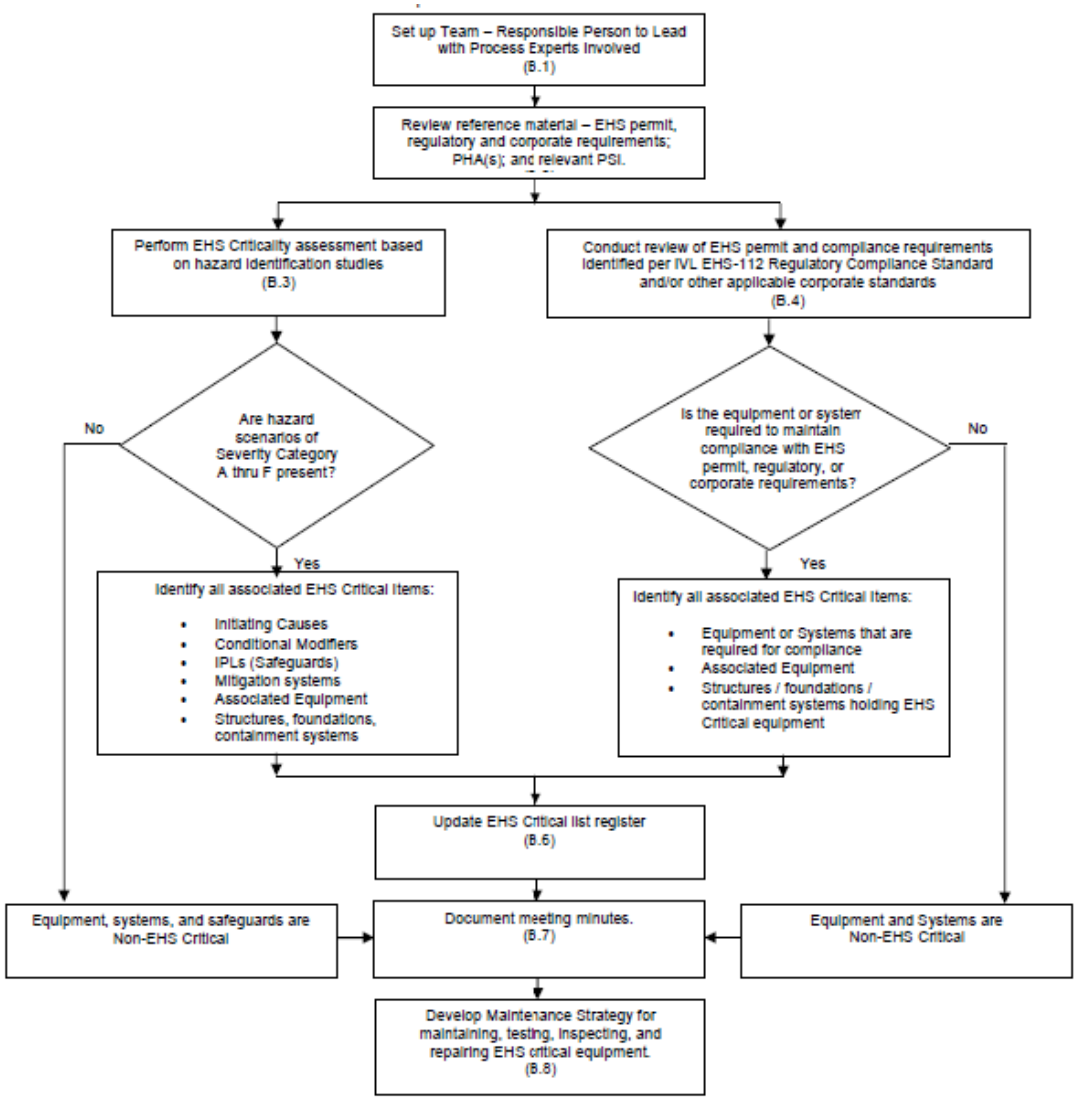
Definition: EHS Critical IVL EHS-405

Critical IPLs: **All mechanical, instrument, alarm, or administrative system (or procedure) credited as an IPL to meet the target risk criteria for Severity of A thru F events shall be considered EHS Critical IPLs.**

Critical EE/CM: **All Enabling Events (EEs) and Conditional Modifiers (CMs) credited with risk reduction, or frequency modification, on Severity A thru F events shall be considered EHS Critical enabling events or conditional modifiers.**

Critical Operator Tasks: **Any failure to perform a procedure or sequence of tasks in an operating procedure that was recorded as an initiating cause for a Severity Category A thru F hazard event scenario shall be identified as an EHS Critical Operator Task.**

EHS Criticality Assessment: Overview from IVL EHS-405



EHS Critical Examples

EHS Critical	Non-EHS Critical
Primary containment equipment (such as piping, pumps, compressors, towers, exchangers, drums, vessels, tanks, etc.) **containing** flammables or toxic chemicals whose failure, as identified in a PHA, **could credibly result** in Severity Category A thru F consequence, and equipment whose failure **could credibly result** in a non-compliance with EHS permit, regulatory, or corporate requirements. 1) Equipment credited for risk reduction as an independent protection layer **(For Severity A thru F Consequences)**: • Instrumented Trips (high temperature, pressure, level, etc.) • Instrumented systems related to Alarms coupled with trained operator response • Process Analyzers • Hydrocarbon Detectors 2) Consequence mitigation systems such as: • Pressure Relief Device/Streams/Systems • Deluge / Fire protection equipment • Ventilation Systems • Process Control Uninterrupted Power Supply • Site-wide Evacuation Alarms • Emergency Shutdown Devices 3) Passive layers of protection or structures: • Dikes/berms • Fire Walls • Blast Walls	Primary containment equipment (such as piping, pumps, compressors, towers, exchangers, drums, vessels, tanks, etc.) containing flammables or toxic chemicals whose failure, as identified in a PHA, **could not credibly result** in Severity Category A thru F consequence, and equipment whose failure **could not credibly result** in a non-compliance with EHS permit, regulatory, or corporate requirements. Basic Process Control (if not required to meet EHS permit, regulatory, or corporate requirements and not credited as an IPL for a Severity A thru F consequence) Utility Services which are not required to meet EHS permit, regulatory, or corporate requirements and are not credited as an IPL protecting against Severity A thru F consequences.

Additional Requirements

For all EHS Critical items:

- assign a unique identity number;
- maintain a site register; and
- maintain EHS Criticality assessments as current for the life of the asset.

EHS Criticality assessments shall be carried out prior to commissioning for changes to existing facilities subject to IVL EHS-204, Management of Change, and for capital projects.

EHS Criticality Assessments should be kept current with changes to National or Local legislation through the Management of Change process.

Questions/Comments