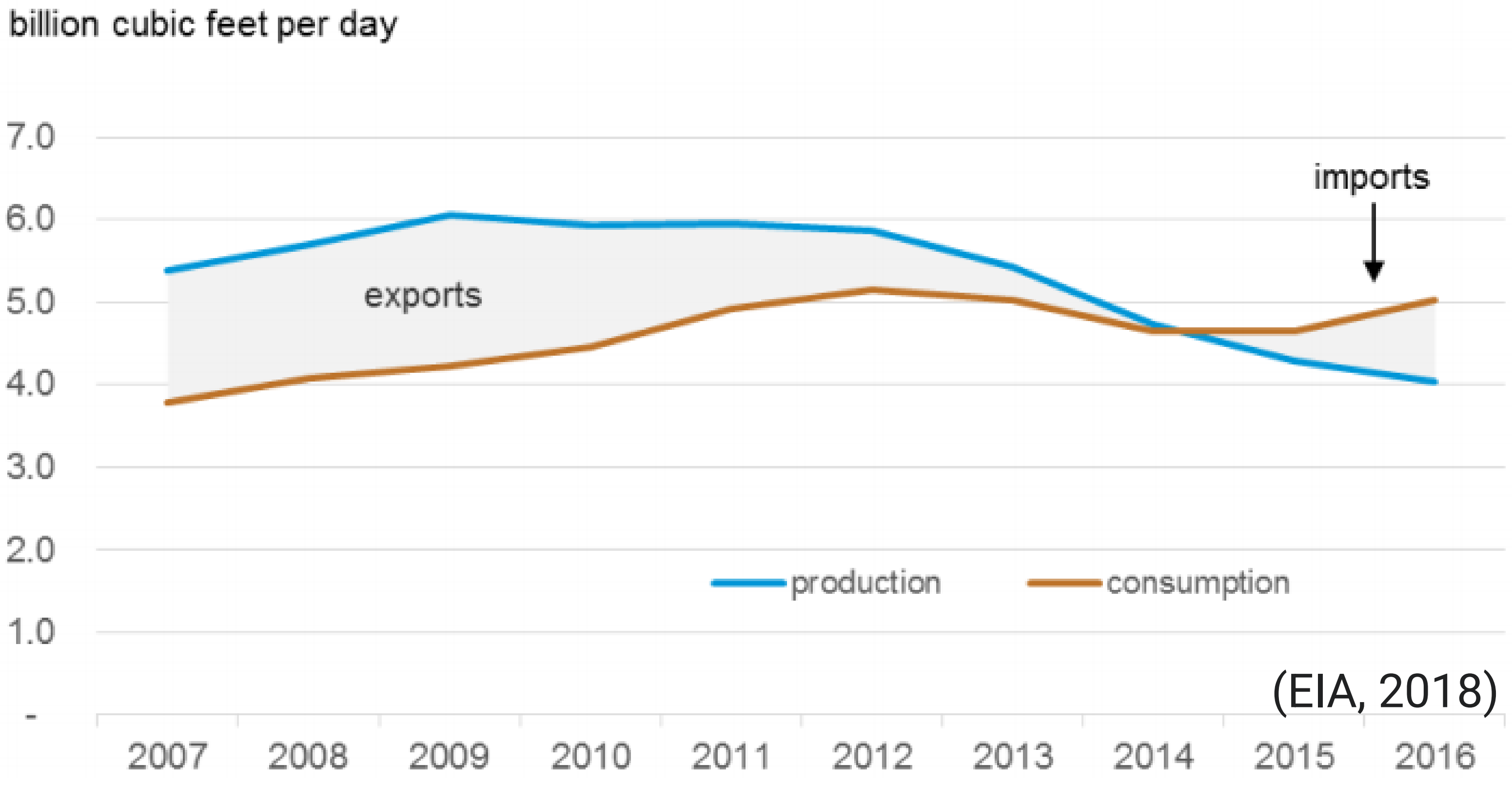
Cumulative Risk Model of Safety Barriers – Case Study

Yasser Fathy Taha, Process Safety Manager, Rashpetco Petroleum

Egyptian Natural Gas Production, Consumption, Net Exports, Net Imports



(EIA, 2018)

Introduction

- Accidents happen if multiple barriers fail to perform their intended function
- Safety Critical Tasks (SCTs).
- BT Diagram (BTD)
- Safety barriers - Faults/Failures
  - (1) Detected or undetected,
  - (2) Within the SOL or out of SOL, and/or
  - (3) Subject to instant adjustment and compensation

What is the Problem?

- Two years overdue of planned shutdown for maintenance –
- **Mainly -** Assurance or Repair Safety Critical Tasks
  1. **Sealine valve replacement** – a passing isolation valve

     An Emergency Shutdown valve that provides boundary isolation between offshore/subsea wells and onshore facilities
  2. **Regeneration heater inspection –** tubes testing

     Requires removing a tube section for examination following 10 years in service according to ASME recommendations.
  3. **Cause & Effect Proof Tests -** More than 2 years overdue
  4. **PSVs Calibration and testing –**

     Some PSVs are no longer within the calibration period

Methods Summary - Safety Barriers Performance Review

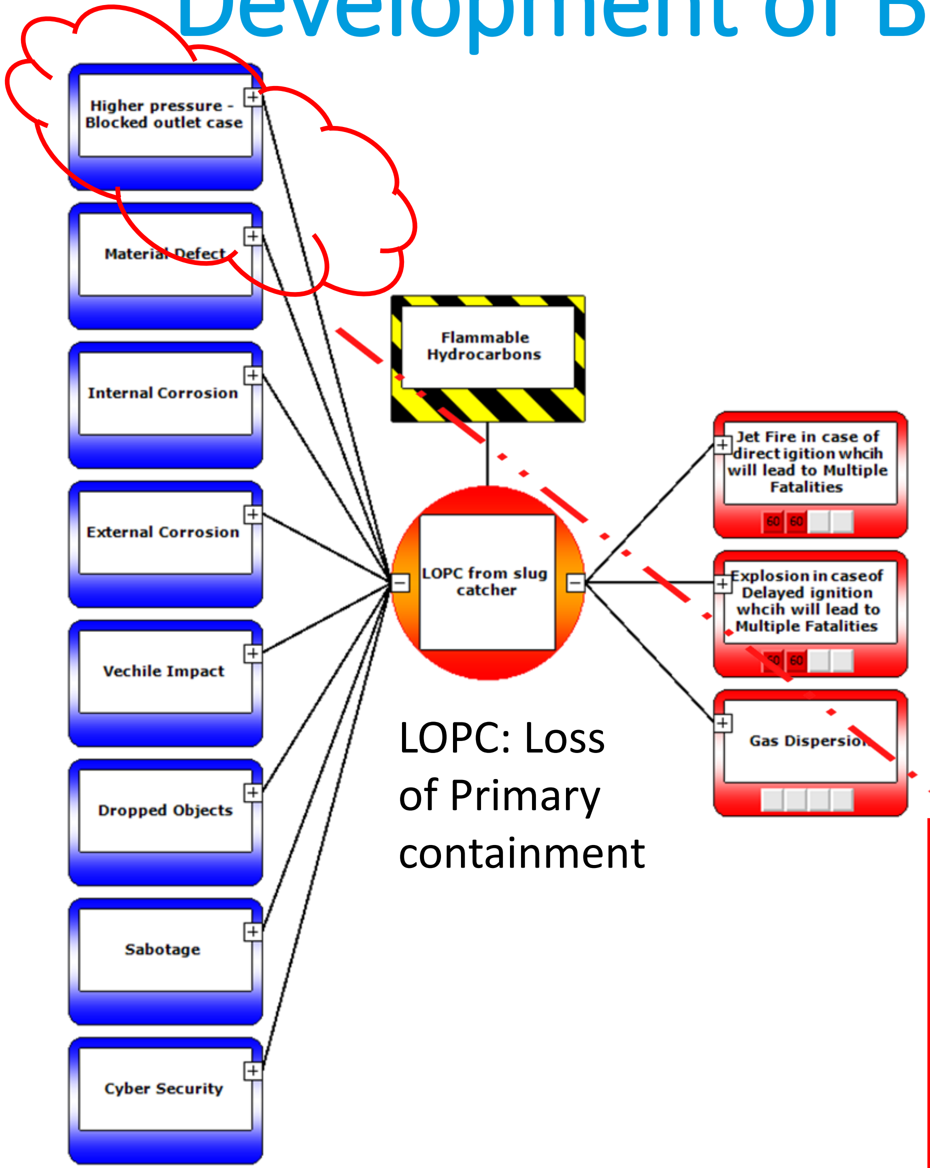
1. Identify the List of Unavailable / Impaired SCEs
2. Identification of the foreseeable MAH associated with The Unavailable / Impaired Barrier
3. Development of Bowtie Diagrams
4. Risk Assessment
5. Cumulative Risk Calculations

Development of Bowtie Diagrams - Link between BT, HAZOP and LOPA Terminologies

BT terminology	HAZOP terminologies	LOPA terminology (ies)
Threat	Deviation + possible causes	(Initiating event +Enabling event)
Barrier	Existing Safeguard / Additional Safeguard (Actions) [1]	Protection layers[1]
Consequences	Consequences	Impact event + Severity level
Hazard	Design intent	Description of the scenario

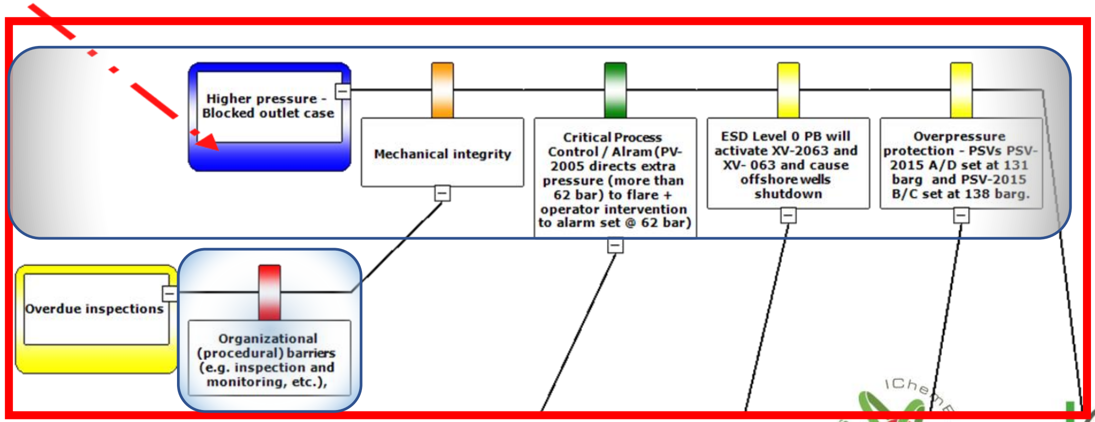
Note1: Not all safeguards are IPLs, but all IPLs are safeguards [27]

Development of Bowtie Diagrams (BTDs)



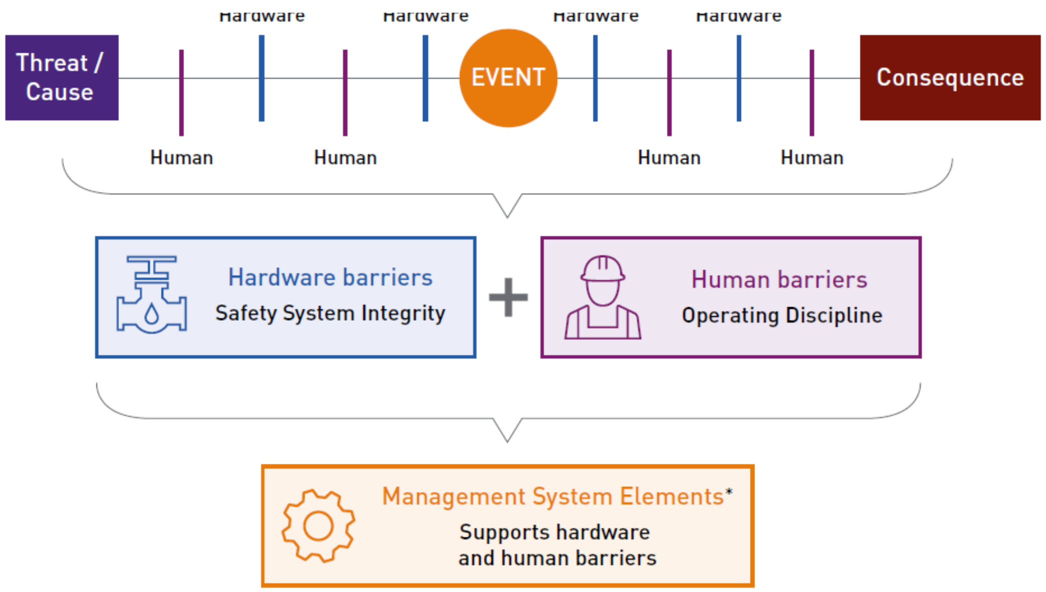
LOPC: Loss of Primary containment

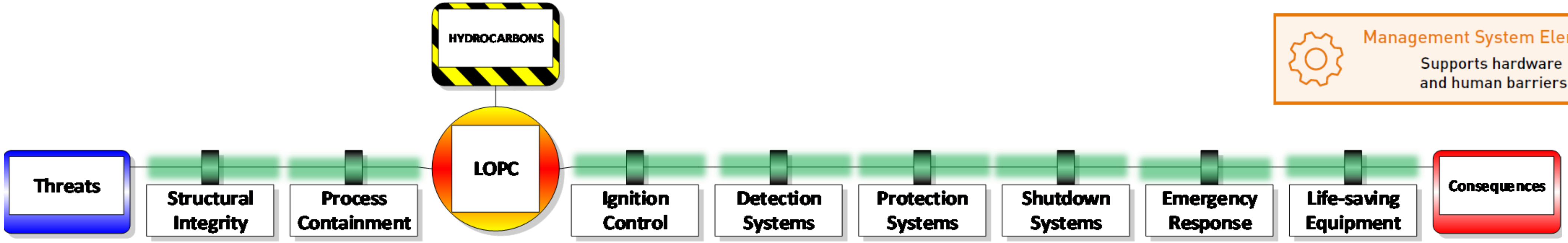
- Primary / main barriers - according to their sequence of operations in response to specific threats leading to the top event
- Barrier Decay Mechanisms which is a fault mode/malfunction mechanism that can lead to failure of the primary barrier
- Secondary barriers or barriers decay - a process or system utilized to prevent/control decay mechanisms of the primary barriers



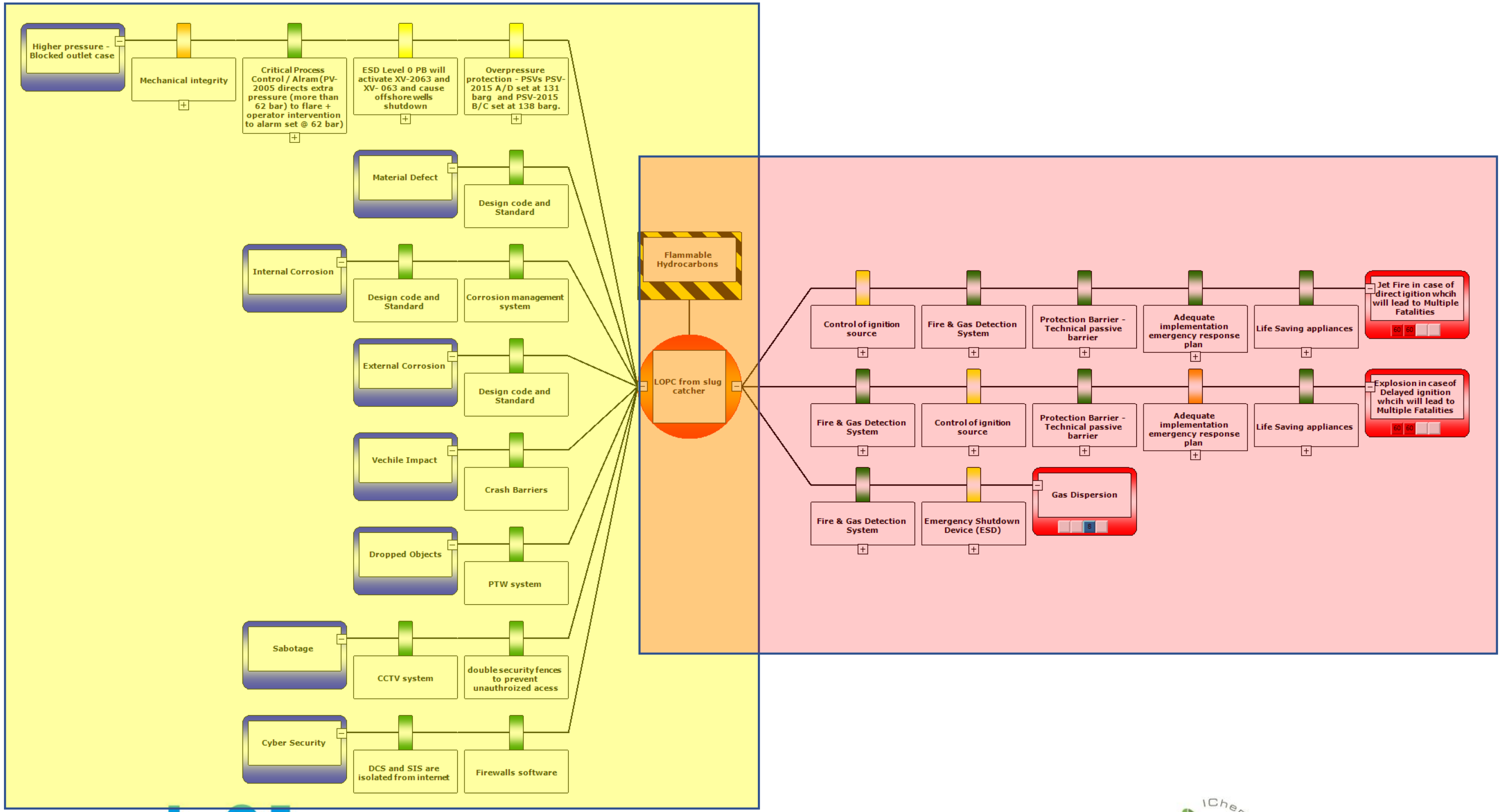
Qualitative Risk Assessment

Barriers assigned for a specific accidental event should be added to the logic trees in the sequence they will be activated (Hausand, et al., 2004)





Quantitative Risk Assessment



Hazards31

IChemE Safety Centre

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

Quantitative Risk Assessment - Operational FN-Curve

A Method to develop a dynamic/live operational FN curve is presented in the following section

- In the operational FTD, The LOPC frequency is calculated based on the PFD of safety systems while QRA data mainly uses the historical failure rate data of process equipment.
- It is assumed that the calculated FTD frequency (i.e.: LOPC frequency) is equal to or replaces the process equipment failure frequency used in design QRA

Risk Calculations

PFD for the j[th] IPLs that protects against consequence C for initiating event is given by the: (Pitblado, et al., 2016)

$$PFD_{IPLs} = \prod_{j=1}^{J} = PFD_{SIB} . PFD_{PCB} . PFD_{ICB} . PFD_{DSB} . PFD_{PSB} . PFD_{SDB} \quad \text{Equation (3)}$$

PFD_{SIB} is structural integrity barrier PFD

PFD_{PCB} is the process containment barrier PFD

PFD_{ICB} is ignition control barrier PFD

PFD_{DSB} is detection system barrier PFD

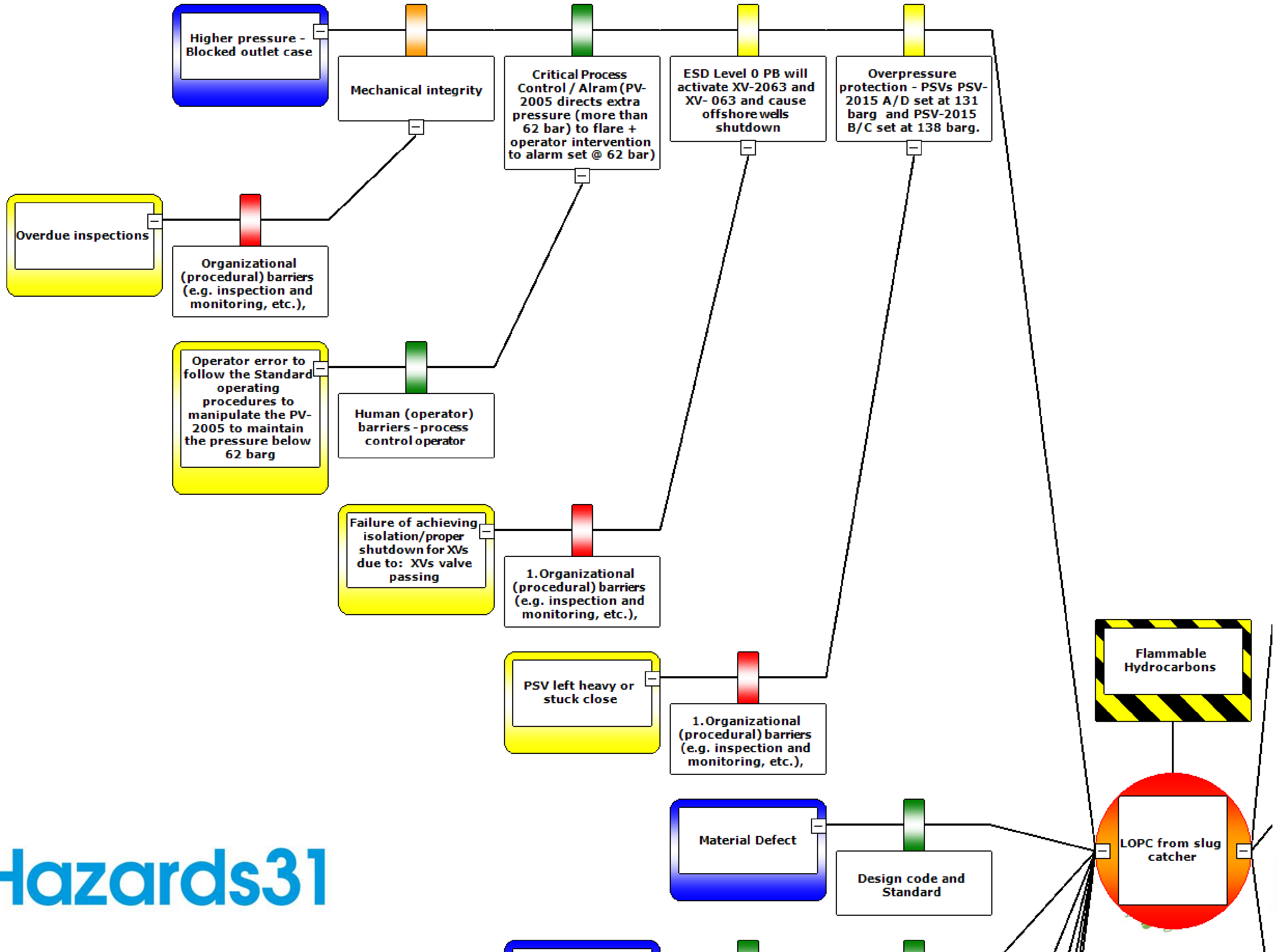
PFD_{PSB} is the protection system barrier PFD

PFD_{SDB} is shutdown barrier PFD

The Emergency response and the lifesaving barrier were excluded from the equation because both are safeguards and not IPLs.

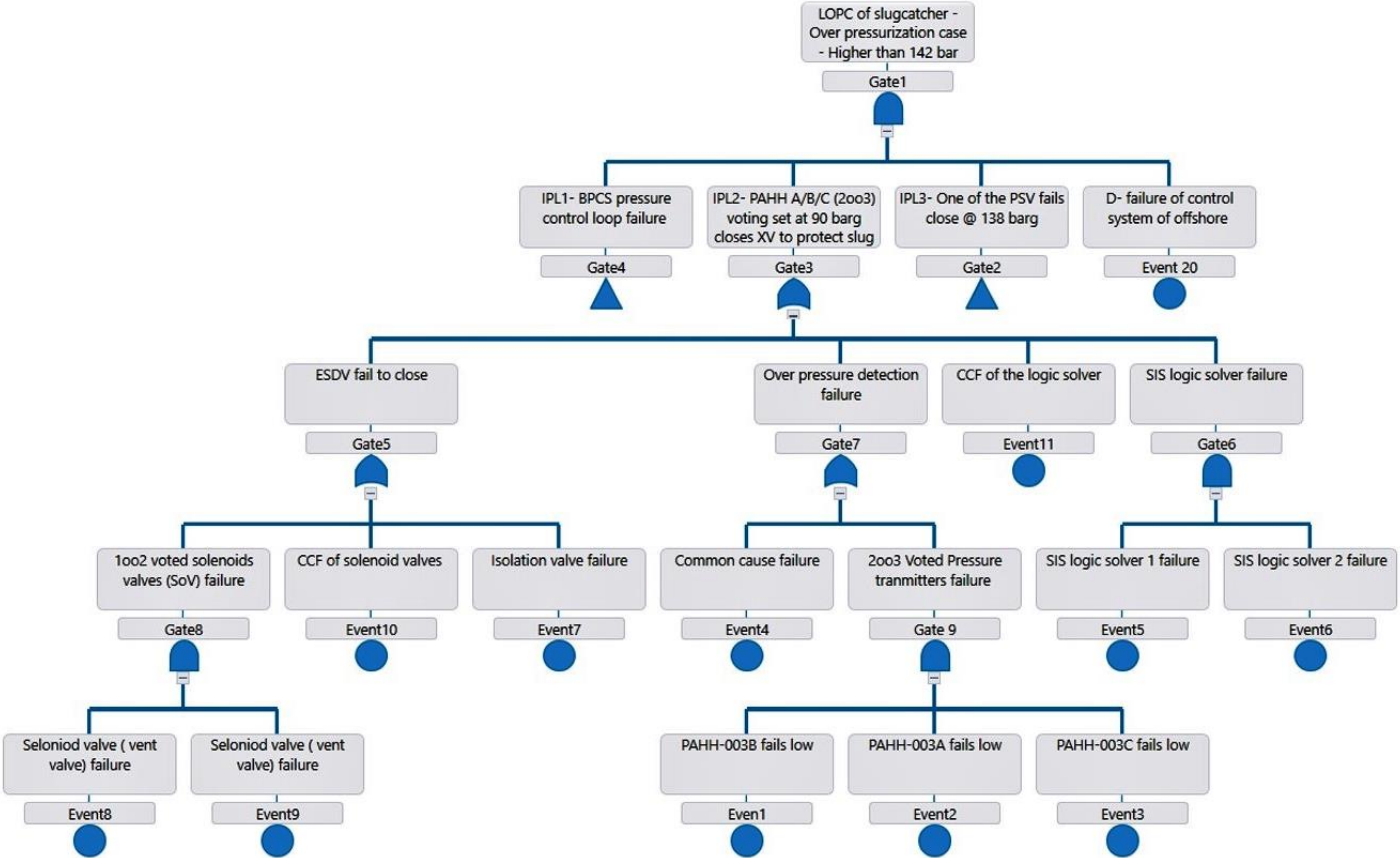
Alternative 1- Performing safety-critical maintenance
Alternative 2- Deferral of safety-critical maintenance until the next due date

Results



Hazards31

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE



ICING
ICAL
ERING
WIDE

A	B	C	D				
Initiating LOPC Likelihood	Direct ignition Successful	Fire & Gas Detection Successful	protection system Successful	Ultimate Incident Outcome	Event Combinations	Ultimate Incident Frequency	Event Description
			0,99021	**Jet Fire**	**ABCD**	**5,14E-06**	Frequency of direct ignition given Fire and Gas system and Protection system availability
	Direct ignition	**0,985**	0,00979	**Jet Fire**	**ABCd**	**5,08E-08**	Frequency of direct ignition given Fire and Gas system availability and Protection system unavailability
	0,7		**0,99021**	**Jet Fire**	**ABcD**	**7,73E-10**	Frequency of direct ignition given Fire and Gas system unavalibility and Protection system availability
LOPC frequency	Yes	0,015	0,00979	**Jet Fire**	**ABcd**	**7,73E-10**	Frequency of direct ignition given Fire and Gas system and Protection system unavalibility
7,52E-06	No	**0,985**		**Harmless**	**AbC**	**2,22E-06**	Frequency of Harmless release given fire and gas detection system successes to detect the leak
	0,3		**0,99021**	**UNVCE**	**AbcD**	**3,35E-08**	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system success
	Delayed ignition	0,015	0,00979	**UNVCE**	**Abcd**	**3,31E-10**	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system failure

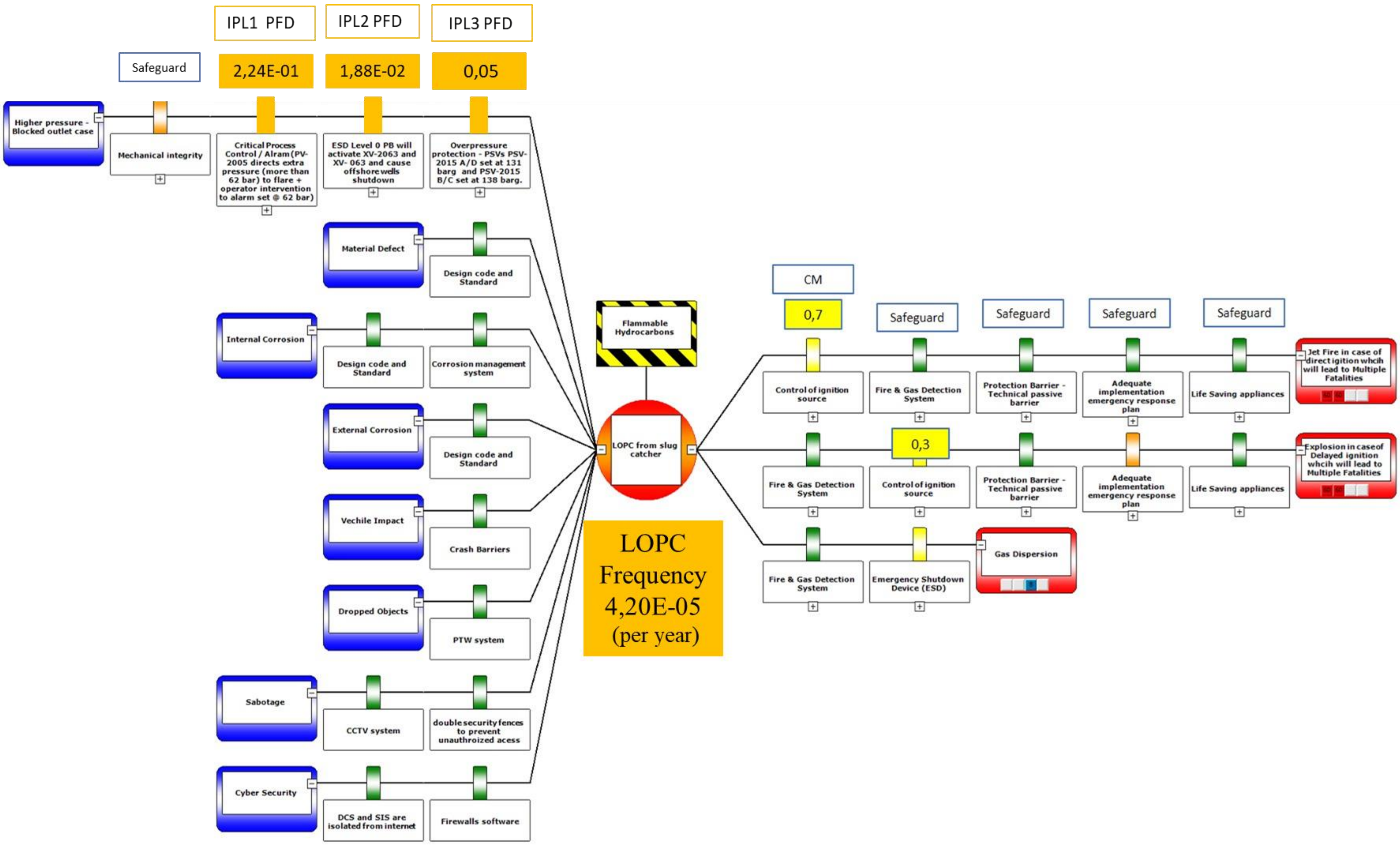
Jet fire Frequency	**5,189E-06**
UNVCE Frequency	**3,386E-08**
Harmless Frequency	**2,223E-06**
Total	**7,446E-06**

Risk Calculations Results

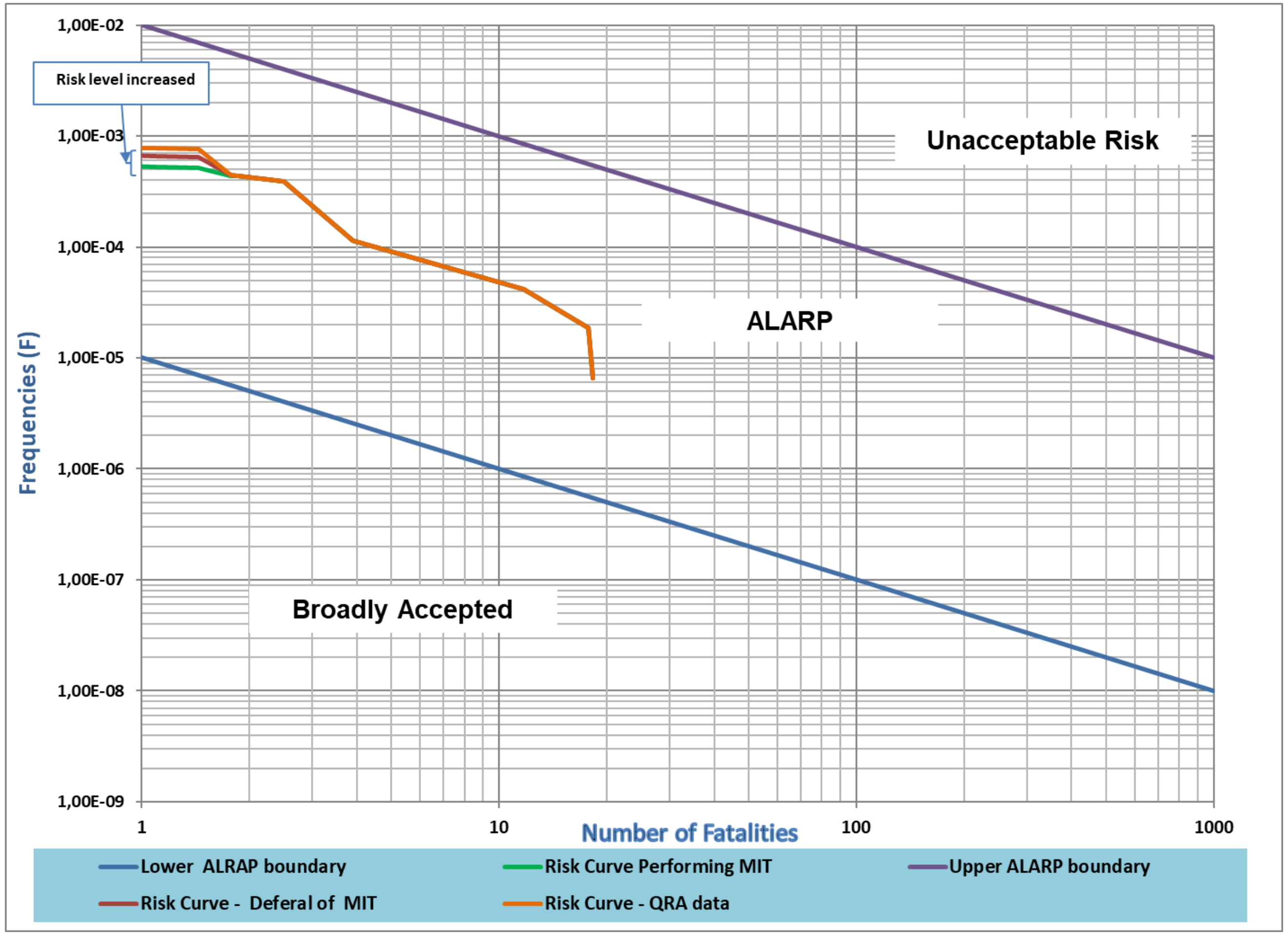
(1) Risk Evaluation Against Maximum Risk Criteria

(2) Risk Evaluation Against Individual-Specific Individual Risk

(3) Risk Evaluation Against Target Risk Frequency
(Occurrences Per Year, Per Event)


IPL1 PFD
IPL2 PFD
IPL3 PFD
Safeguard
2,24E-01
1,88E-02
0,05
Higher pressure - Blocked outlet case
Mechanical integrity
Critical Process Control / Alram (PV-2005 directs extra pressure (more than 62 bar) to flare + operator intervention to alarm set @ 62 bar)
ESD Level 0 PB will activate XV-2063 and XV- 063 and cause offshore wells shutdown
Overpressure protection - PSVs PSV-2015 A/D set at 131 barg and PSV-2015 B/C set at 138 barg.
Material Defect
Design code and Standard
Internal Corrosion
Design code and Standard
Corrosion management system
External Corrosion
Design code and Standard
Vechile Impact
Crash Barriers
Dropped Objects
PTW system
Sabotage
CCTV system
double security fences to prevent unauthroized acess
Cyber Security
DCS and SIS are isolated from internet
Firewalls software
Flammable Hydrocarbons
LOPC from slug catcher
LOPC Frequency 4,20E-05 (per year)
CM
0,7
Safeguard
Safeguard
Safeguard
Safeguard
Control of ignition source
Fire & Gas Detection System
Protection Barrier - Technical passive barrier
Adequate implementation emergency response plan
Life Saving appliances
Jet Fire in case of direct igition whcih will lead to Multiple Fatalities
Fire & Gas Detection System
0,3
Control of ignition source
Protection Barrier - Technical passive barrier
Adequate implementation emergency response plan
Life Saving appliances
Explosion in case of Delayed ignition whcih will lead to Multiple Fatalities
Fire & Gas Detection System
Emergency Shutdown Device (ESD)
Gas Dispersion

Update FN-Curve



- **Design FN Curve**
- **Operational FN Curve**

Hazards31

IChemE Safety Centre

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

Conclusion

Conclusion

- The results of qualitative risk assessment showed that the cumulative risk is no longer ALRAP, and immediate actions need to be taken to shut down the facility and perform the safety-critical task of the impaired SCEs
- In the quantitative risk analysis approach, the logical relationships between safety barriers and MAHs were described and analysed using BT, FT, and ET analysis

Conclusion

The cumulative notion of risk was described and assessed in two forms

- The first form of cumulative risk representation is the traditional safety barrier model using the James Reason Swiss cheese model and IOGP standard - multiple failures in the safety-critical systems can cumulatively impact the risk profile of the whole industrial facility.
- A second form is a new approach which is the operational FN-Curve that represents long-range accidents in one curve – the curve can be dynamic updated when the cumulative frequencies of having multiple incidents are changed with the change in the SCE performance…

Conclusion

Operational FN Curve

- Having a full operational FN curve will represent the live/ dynamic cumulative risk profile of industrial facility where Any change in the PFD of the SCEs (due to impairment, deferment, or unavailability/ isolation) will lead to change in the incident rate and subsequently will change in the safety barriers performance and the operational FN-Curve.

- The method used in this paper can be expanded to cover all hazard scenarios of industrial facilities and can be used to generate a concise and representative picture of the cumulative risk profile for one or more facility (i.es)

Thanks

Q&A

Yasser Fathy

Yasser.Fathy@Rashpetco.com

https://www.linkedin.com/in/yasserfathy