5th Public Webinar | 21st APRIL 2022

PRHYDE-Protocol for heavy-duty hydrogen refuelling

Call Identifier FCH-04-2-2019:
Refuelling Protocols for Medium and Heavy-Duty Vehicles

PRHYDE
Protocol for heavy-duty Hydrogen refuelling

Clean Hydrogen Partnership

This project has received funding from the Fuel Cells and Hydrogen 2 Joint Undertaking (now Clean Hydrogen Partnership) under Grant Agreement No 874997. This Joint Undertaking receives support from the European Union's Horizon 2020 Research and Innovation programme, Hydrogen Europe and Hydrogen Europe Research.

Co-funded by the European Union

WP3: Risk Assessment

Claus Due Sinding / Nel Hydrogen

Disclaimer

The PRHYDE Risk Assessment on novel fuelling concepts was done to the best of our abilities with help from external experts.

The following Risk Assessment is the first milestone in assessing the risks arising from the novel fuelling concepts

End-implementation should include separate Risk Assessment by the individual station manufacturers and OEMs for most accurate mitigation of risk.

Participants

- PRHYDE Partners
  - Nel Hydrogen
  - Shell
  - Toyota
  - Engie
  - Nikola Motor Company
  - Air Liquide
  - ITM
- External Experts
  - First Element Fuel
  - RiskTec
  - LIFTE H2
  - US DOE labs
    - SNL
    - NREL
    - SRNL

Scope of Risk Assessment

1. Define Risk Assessment Framework
2. Identify threats arising directly from the PRHYDE Fuelling Concepts
3. Assess unmitigated consequences
4. Define barriers to achieve Target Mitigated Event Likelihood (TMEL)

Scope of Risk Assessment

1. Define Risk Assessment Framework
2. Identify threats arising directly from the PRHYDE Fuelling Concepts
3. Assess unmitigated consequences
4. Define barriers to achieve Target Mitigated Event Likelihood (TMEL)

Out-of-scope: Threats that can occur regardless of the fuelling protocol

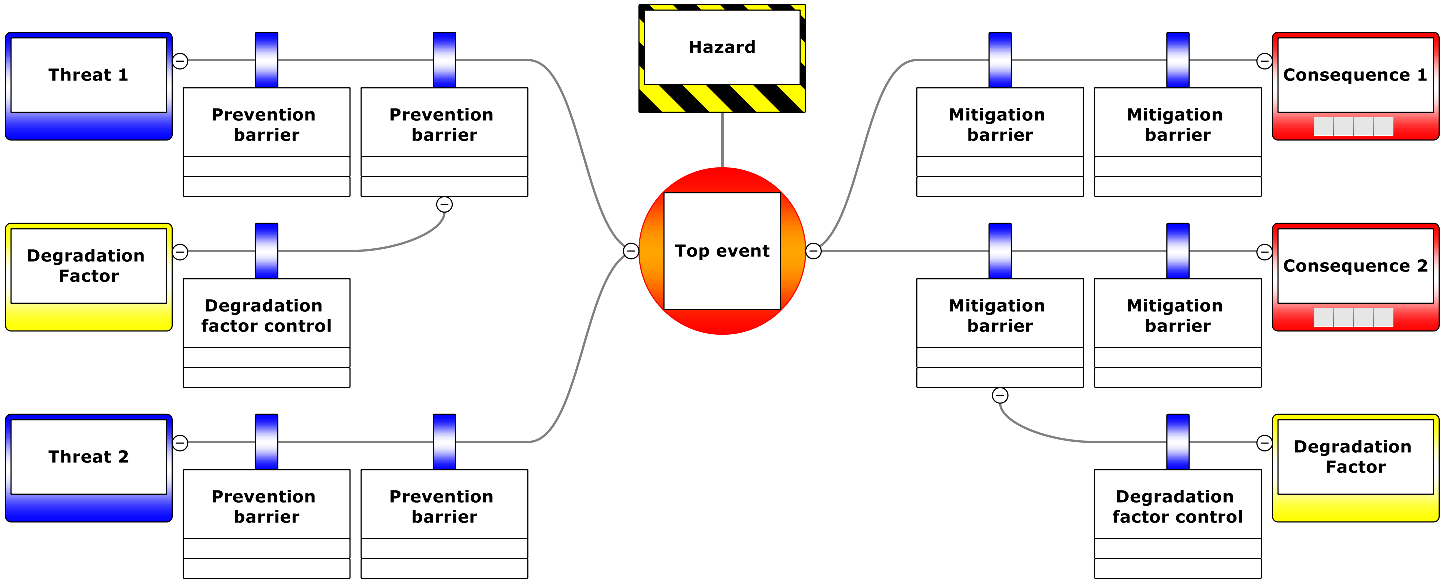
Example: Broken regulator

1. Define Risk Assessment Framework

Methodology – Bowtie-LOPA

Bowtie

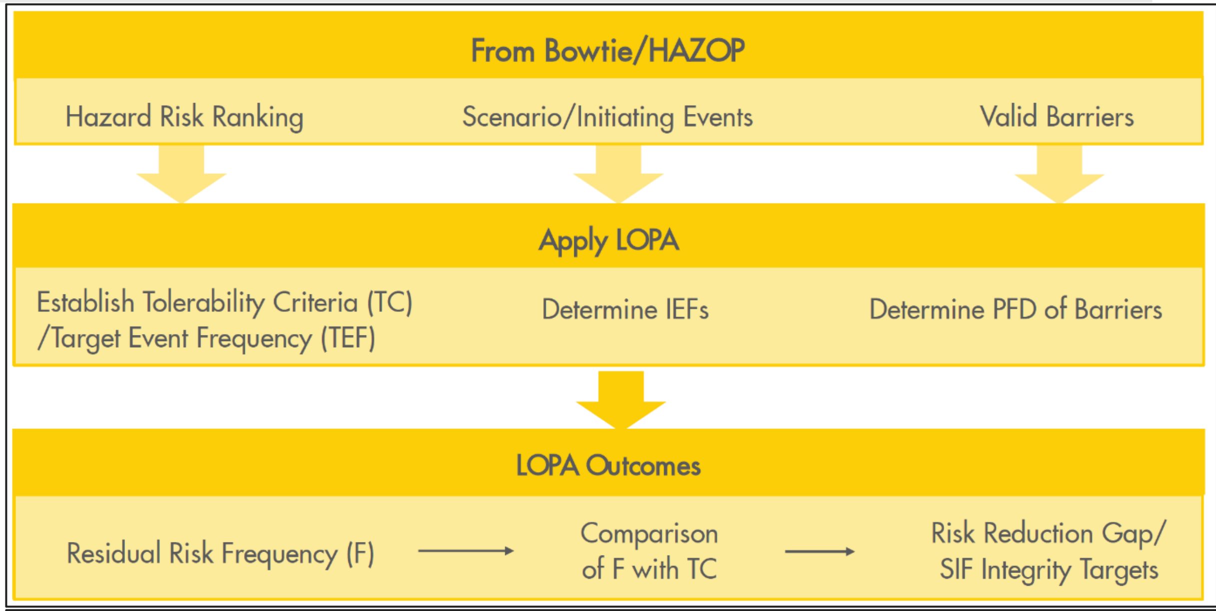
- Visually pleasant
- Separating key elements



Methodology – Bowtie-LOPA

LOPA – Layer of Protection Analysis

- Quantify frequency of event
- Quantify tolerable risk
- Quantify safeguard impact



$F = \Sigma(IEF \times P_e \times PFD_1 \times PFD_2 \times PFD_n) \times P_c \times PFD_{RHS}$ OR $F = \Sigma MEF \times P_c \times PFD_{RHS}$

IEF = Initiating Event Frequency
P_e = Enabling Factor
P_c = Conditional Modifier
PFD_n = Probability of Failure on Demand for Valid Barriers (n being the total number of valid barriers for each IE)
PFD_{RHS} = Probability of Failure on Demand for Valid Barriers on the right hand side of the bowtie

<u>Sources for quantitative risk assessment:</u>

- CCPS
- IEC 61511

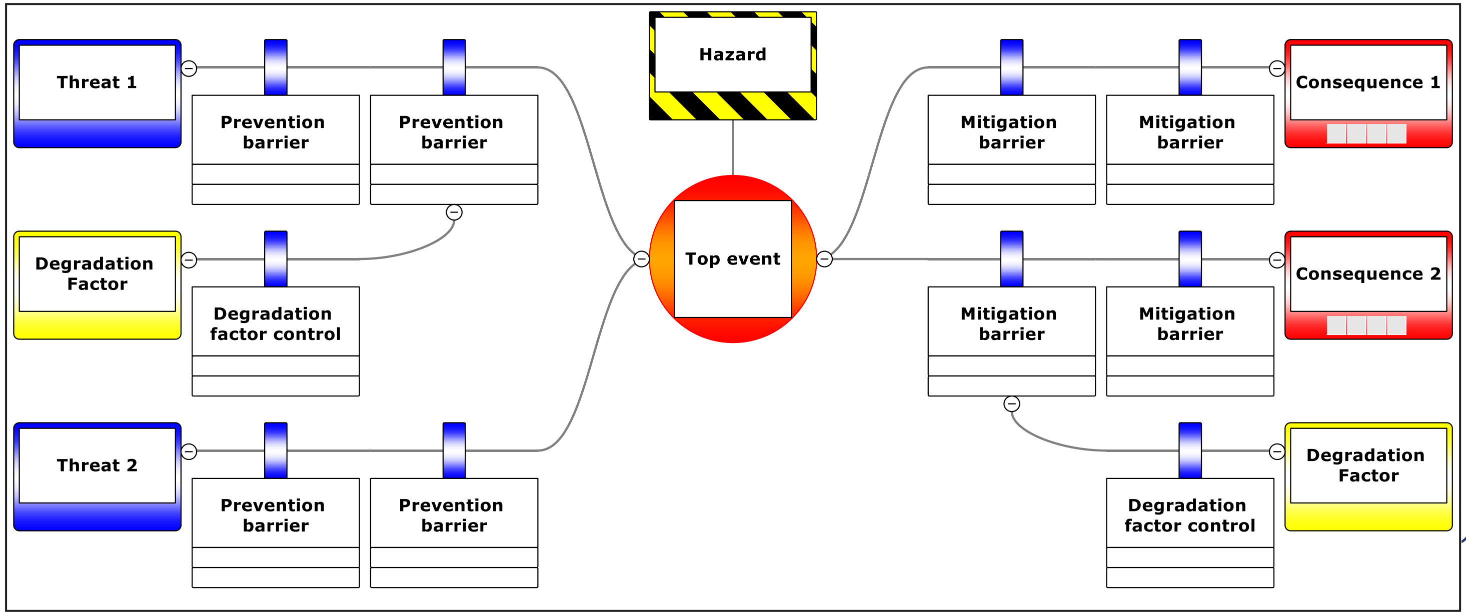
2. Identify threats from novel fuelling concepts

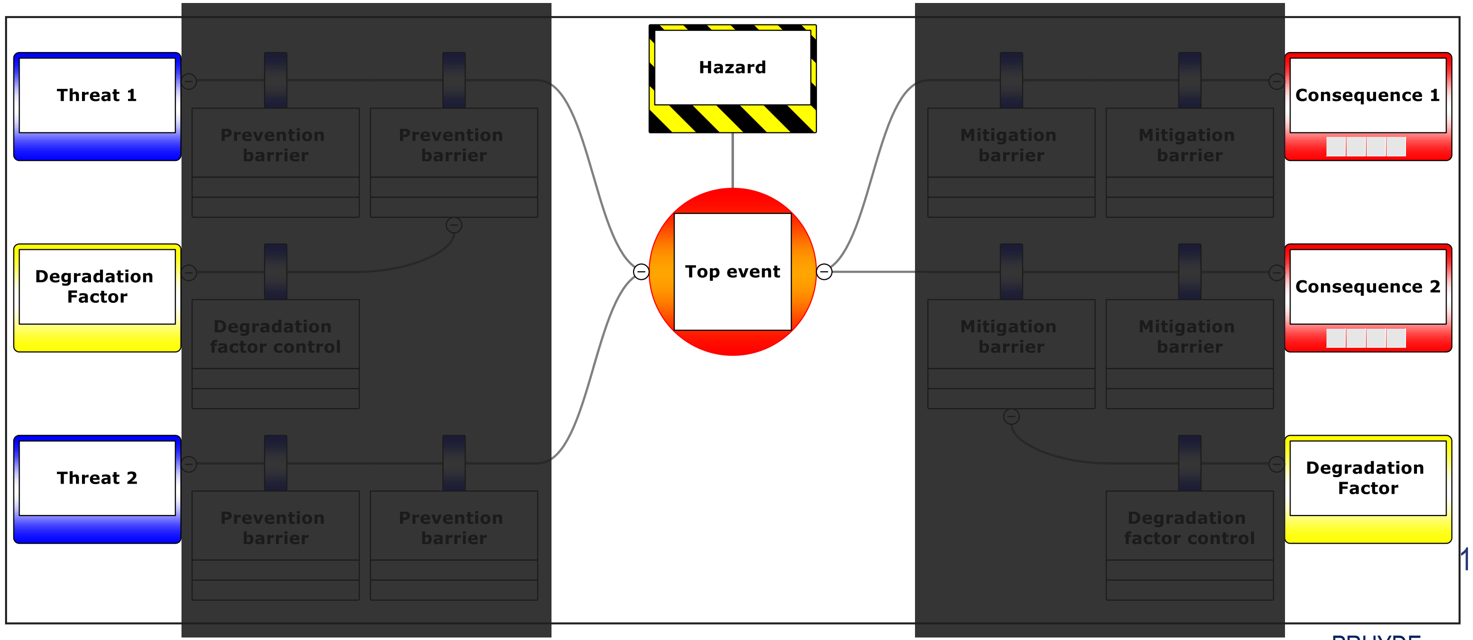
Assumptions on communication

- New protocol –> new risks

- PRHYDE Fuelling concepts are designed for faster refuelling with less pre-cooling of heavy duty vehicles
  – Trade-off: Putting higher requirements for reliable communications

- **Assumption: Safe and reliable Communication active**
  – Tgas used actively (for applicable concepts)


Hazard
Threat 1
Prevention barrier
Prevention barrier
Degradation Factor
Degradation factor control
Threat 2
Prevention barrier
Prevention barrier
Top event
Mitigation barrier
Mitigation barrier
Consequence 1
Mitigation barrier
Mitigation barrier
Consequence 2
Degradation factor control
Degradation Factor

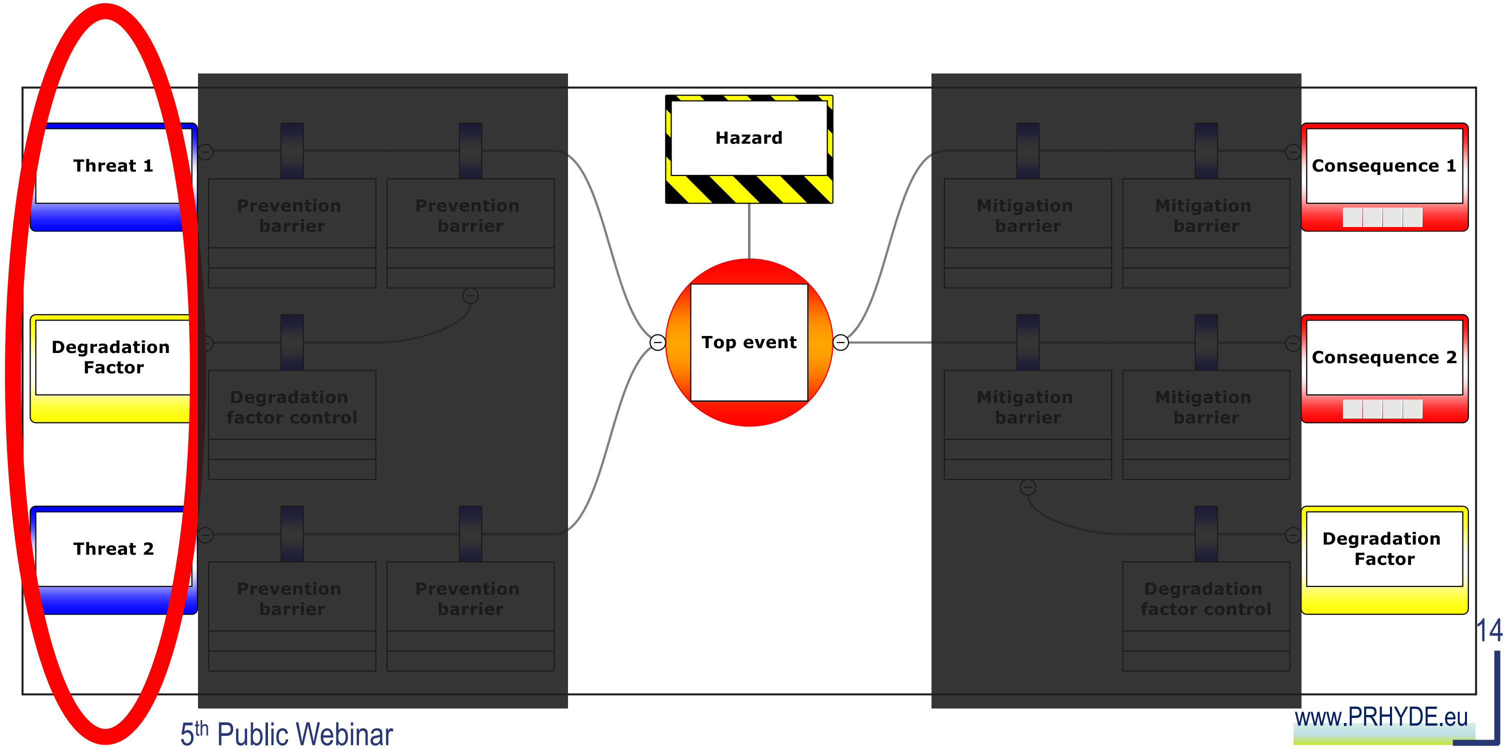

Threat 1
Degradation Factor
Threat 2
Hazard
Top event
Consequence 1
Consequence 2
Degradation Factor

Threats

- Threat: Initiating Event x Enabling Event x Conditional Modifier

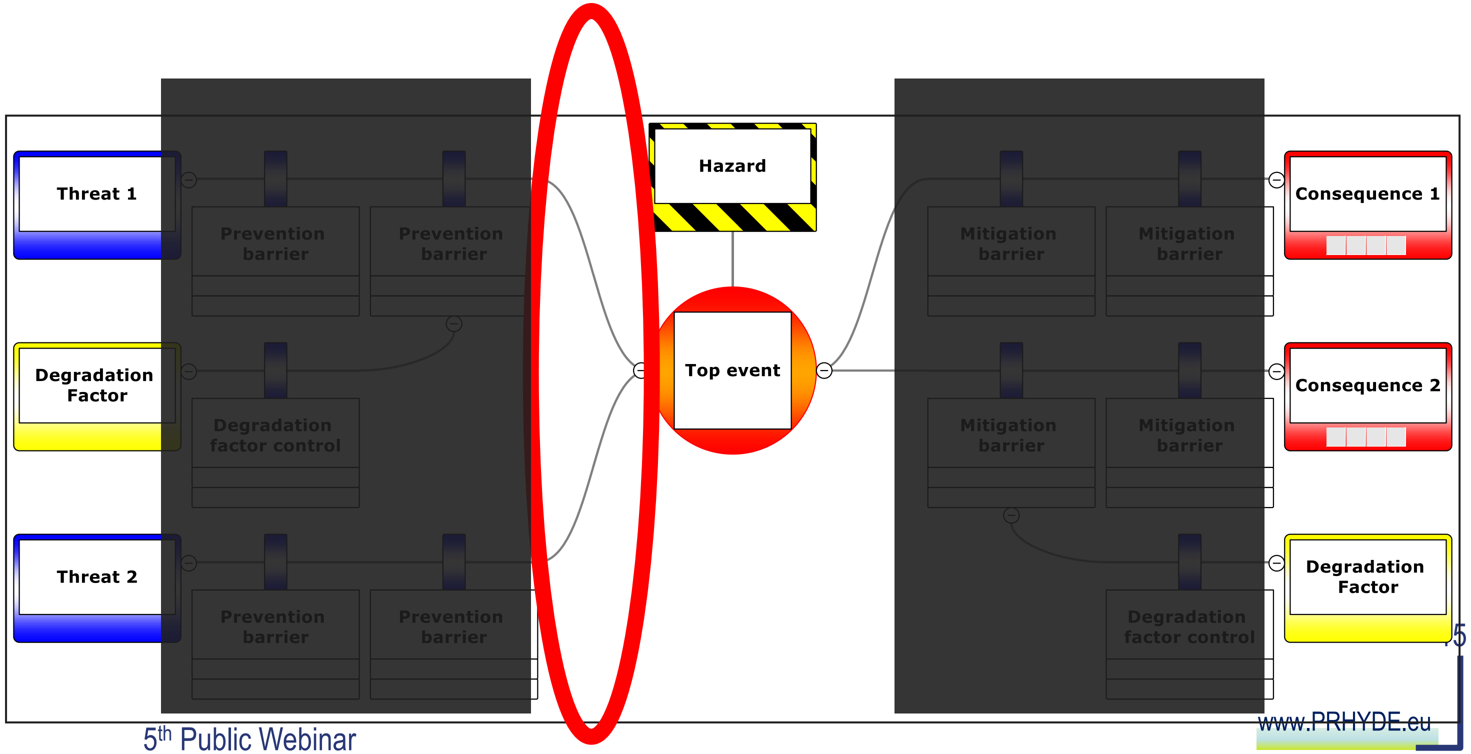
Tabel 1: Overview of applicable Initiating Events for Fueling Concepts

			Fueling Concepts			
			Type2-PR-S	Type3-PR-S		
			Static	T_{gas} Initial	T_{gas} Initial+	T_{gas} Throttle
Initiating Events	3.1.1	T_{Fuel} Error	X	X	X	X
	3.1.2	Mass Flow Error	X	X	X	X
	3.1.3	Station Pressure Error	X	X	X	X
	3.1.4	Ambient Temperature Error	X	X	X	X
	3.1.5	T_{gas} (vehicle) for fueling history Error		X		
	3.1.6	T_{gas} (vehicle) for fueling history and T_{soak} Error			X	
	3.1.7	Tgas (vehicle) Error				X



Threats

- Threat: Initiating Event x Enabling Event x Conditional Modifier
  - Enabling Event Example: Sensor fail in a certain way
  - Conditional Modifier Example: Probability of worst case heating of CHSS

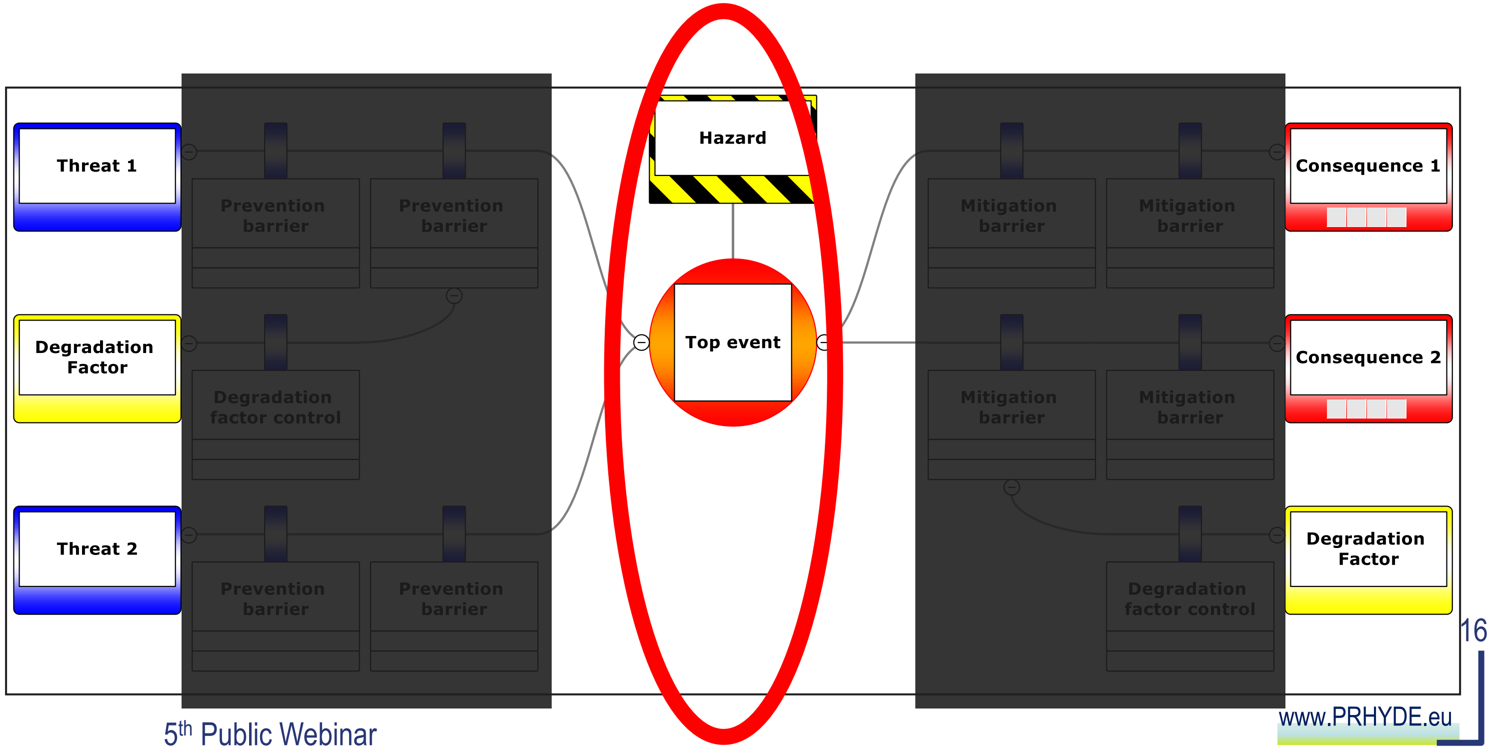


Top Event

- Top Event: Loss of Containment

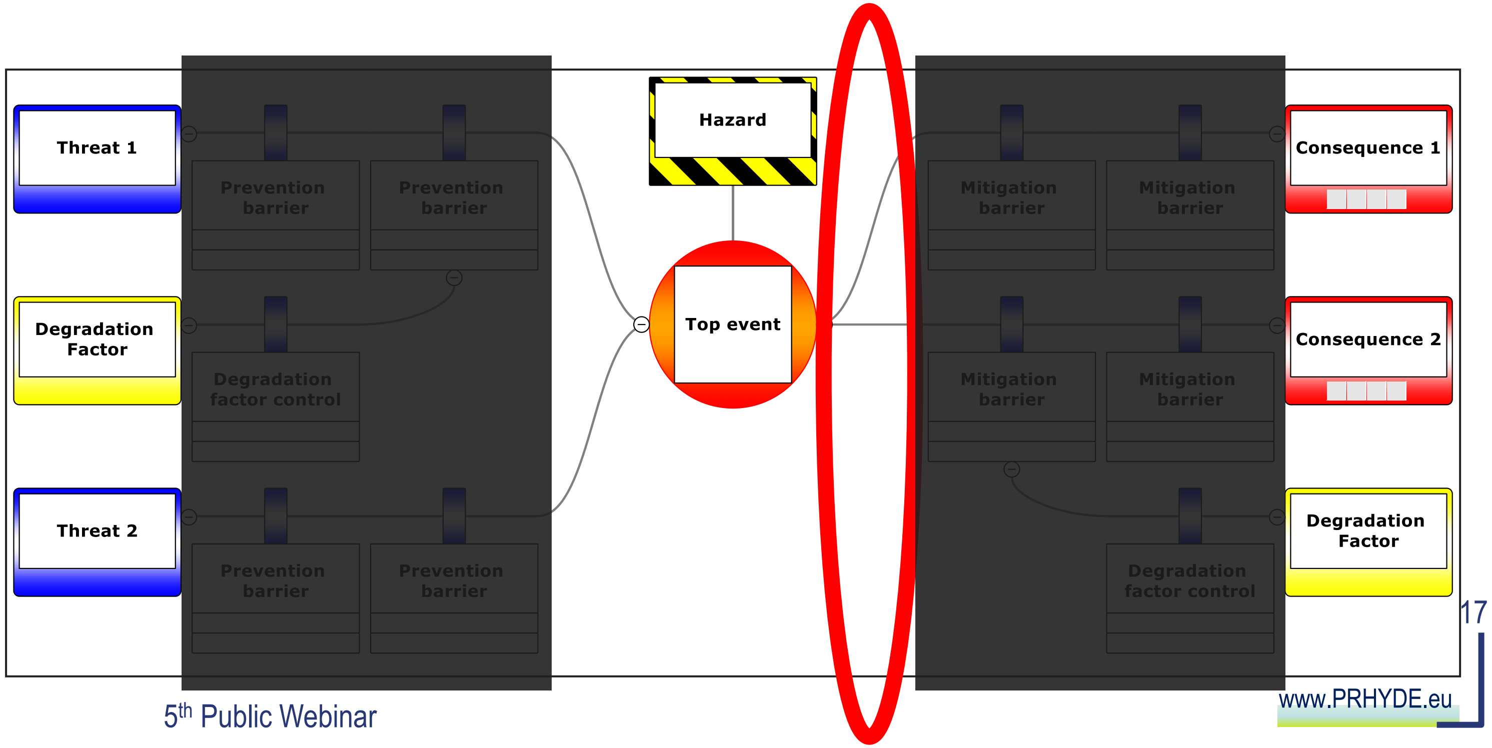
Tabel 9: Probabilities of Loss of Containment for three cases

Case 1: Less Conservative		Case 2: Medium Conservative		Case 3: Very Conservative	
Temperature above Certification	Probability of loss of containment	Temperature above Certification	Probability of loss of containment	Temperature above Certification	Probability of loss of containment
0	0.0%	0	0.00%	0	0.00%
5	0.0%	5	0.00%	5	0.00%
10	0.4%	10	10.00%	10	50.00%
15	0.7%	15	20.00%	15	100.00%
20	1.2%	20	40.00%		
25	2.3%	25	60.00%		
30	4.3%	30	80.00%		
35	8.1%	35	100.00%		
40	15.2%				
45	28.5%				
50	53.4%				
55	100.0%				



Top Event Modifiers

- Modifiers of Loss-of-Containment: Ignition of hydrogen
- No references found regarding probability for ignition
- Assumption:
  - No ignition: 33.3%
  - Immediate ignition: 33.3%
  - Delayed ignition: 33.3%



Consequence

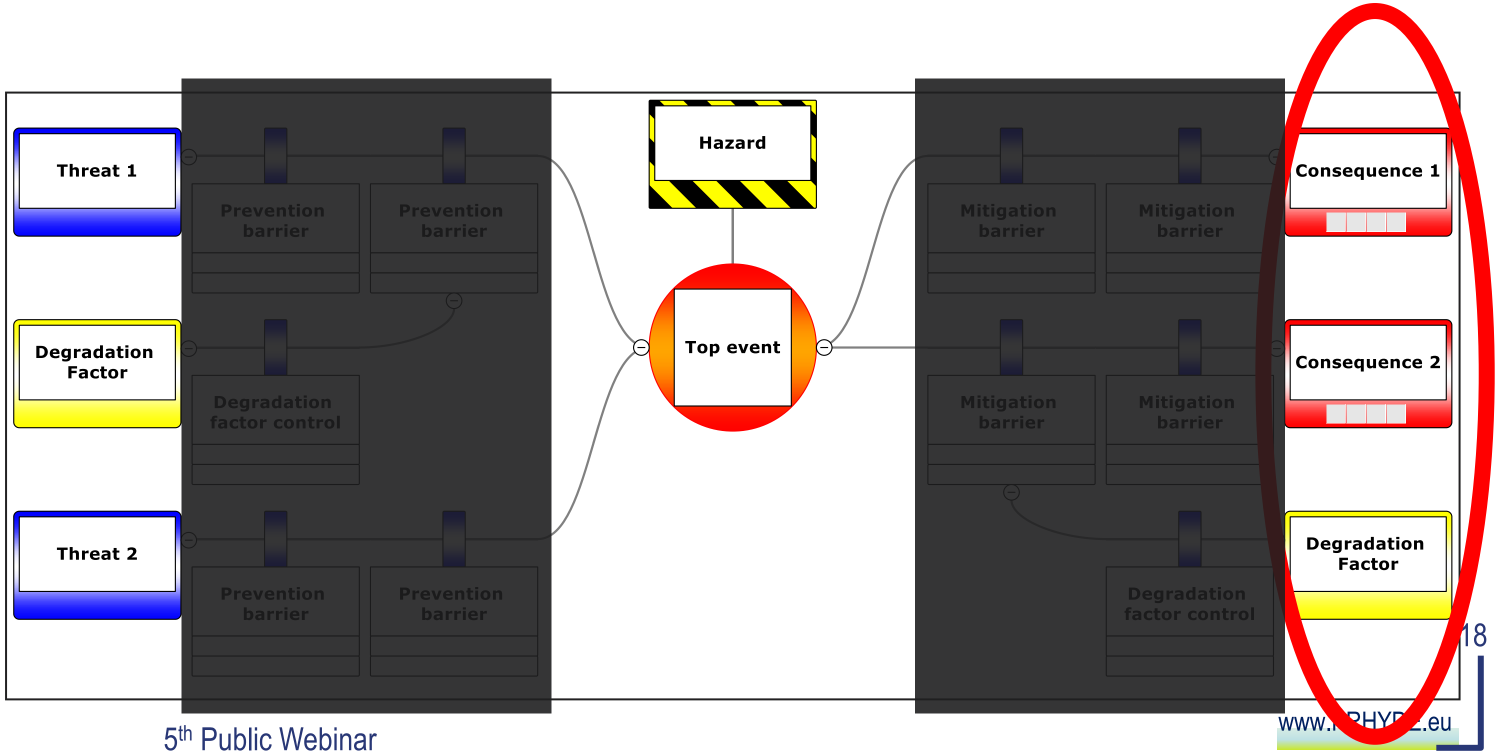
- Consequence: Outcomes of Top Event

Target Mitigated Event Likelihood (TMEL)

– Immediate Ignition
  Jet fire from vehicle tank leading to single fatality
  -> 10^-5 events pr year (once pr 100.000 years)

– Delayed ignition
  Explosion leading to multiple fatalities
  -> 10^-6 events pr year (once pr 1.000.000 years)

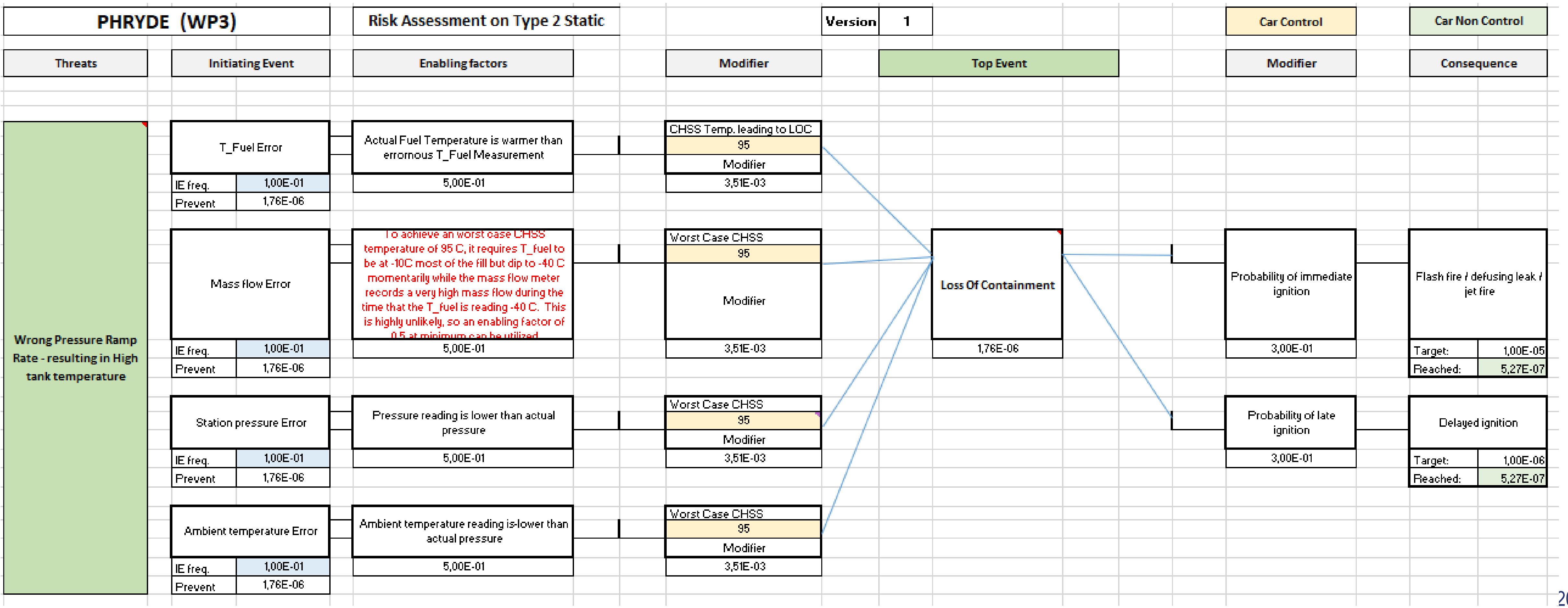
Source: UK HSE Process Safety Leadership Group Final Report



3. Assess unmitigated consequence frequency

Example of Bowtie-LOPA in action

PRHYDE
Protocol for heavy-duty Hydrogen refuelling



Output (unmitigated)

Tabel 12: Bowtie-LOPA output for Fuelling Concept: Static

Frequency of Occurrence	Less Conservative	Medium Conservative	Very Conservative	Target
Top Event	1,76 E-6	5,00 E-5	2,50 E-4	
Jetfire → Single Fatality	5,27 E-7	1,50 E-5	7,50 E-5	1,0E-5
Explosion → Multiple Fatalities	5,27 E-7	*1,50 E-5*	*7,50 E-5*	1,0E-6

Tabel 13: Bowtie-LOPA output for Fuelling Concept: Tgas Initial

Frequency of Occurrence	Less Conservative	Medium Conservative	Very Conservative	Target
Top Event	1,76 E-6	5,00 E-5	2,50 E-4	
Jetfire → Single Fatality	5,27 E-7	1,50 E-5	7,50 E-5	1,0E-5
Explosion → Multiple Fatalities	5,27 E-7	*1,50 E-5*	*7,50 E-5*	1,0E-6

Tabel 14: Bowtie-LOPA output for Fuelling Concept: Tgas Initial+

Frequency of Occurrence	Less Conservative	Medium Conservative	Very Conservative	Target
Top Event	1,76 E-6	5,00 E-5	2,50 E-4	
Jetfire → Single Fatality	5,27 E-7	1,50 E-5	7,50 E-5	1,0E-5
Explosion → Multiple Fatalities	5,27 E-7	*1,50 E-5*	*7,50 E-5*	1,0E-6

→ Less Conservative: No extra barrier needed

Medium/Very Conservative: 1x extra barrier needed

Output (unmitigated)

Tabel 15: Bowtie-LOPA output for Fuelling Concept: Tgas throttle

Frequency of Occurrence	Less Conservative	Medium Conservative	Very Conservative	Target
Top Event	3,00 E-4	2,50 E-3	5,00 E-3	
Jetfire → Single Fatality	*9,00 E-5*	*7,50 E-4*	*1,50 E-3*	1,0E-5
Explosion → Multiple Fatalities	*9,00 E-5*	*7,50 E-4*	*1,50 E-3*	1,0E-6

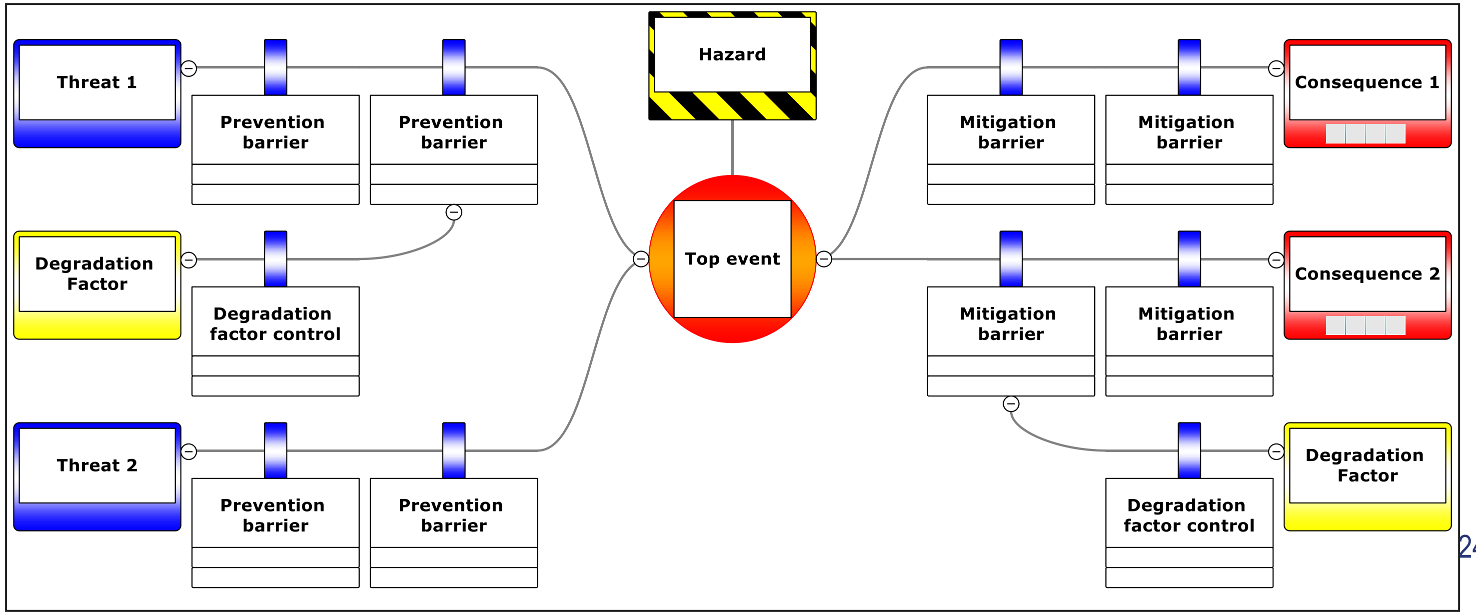
→

Less Conservative: 1x extra barrier needed

Medium Conservative: 2x extra barriers needed

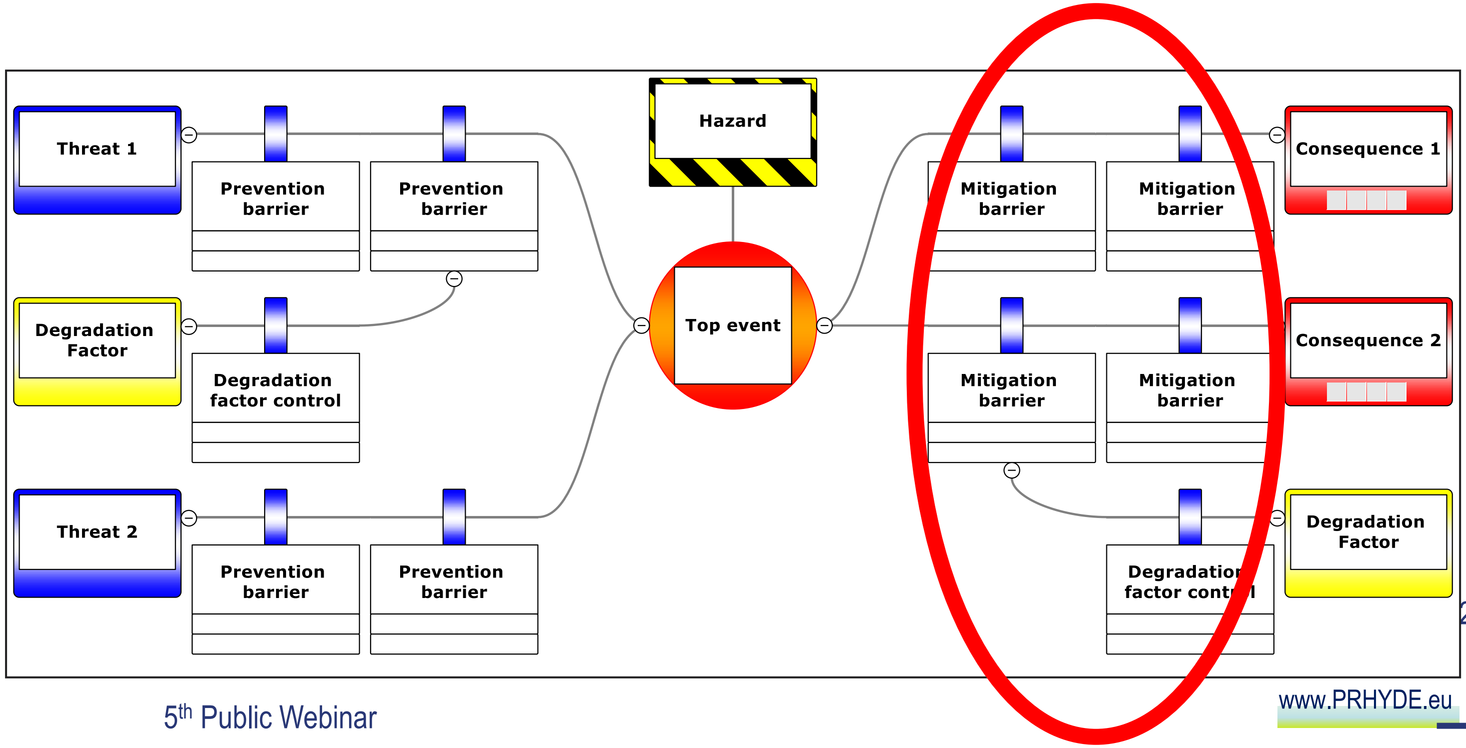
Very Conservative: 2-3x extra barrier needed

4. Defining barriers to achieve TMEL


Threat 1
Prevention barrier
Prevention barrier
Hazard
Top event
Mitigation barrier
Mitigation barrier
Consequence 1
Degradation Factor
Degradation factor control
Mitigation barrier
Mitigation barrier
Consequence 2
Threat 2
Prevention barrier
Prevention barrier
Degradation factor control
Degradation Factor

Mitigative barriers identified

- Station H2 Detector
- Vehicle H2 Detector
- Ultra-sonic Leak Detector

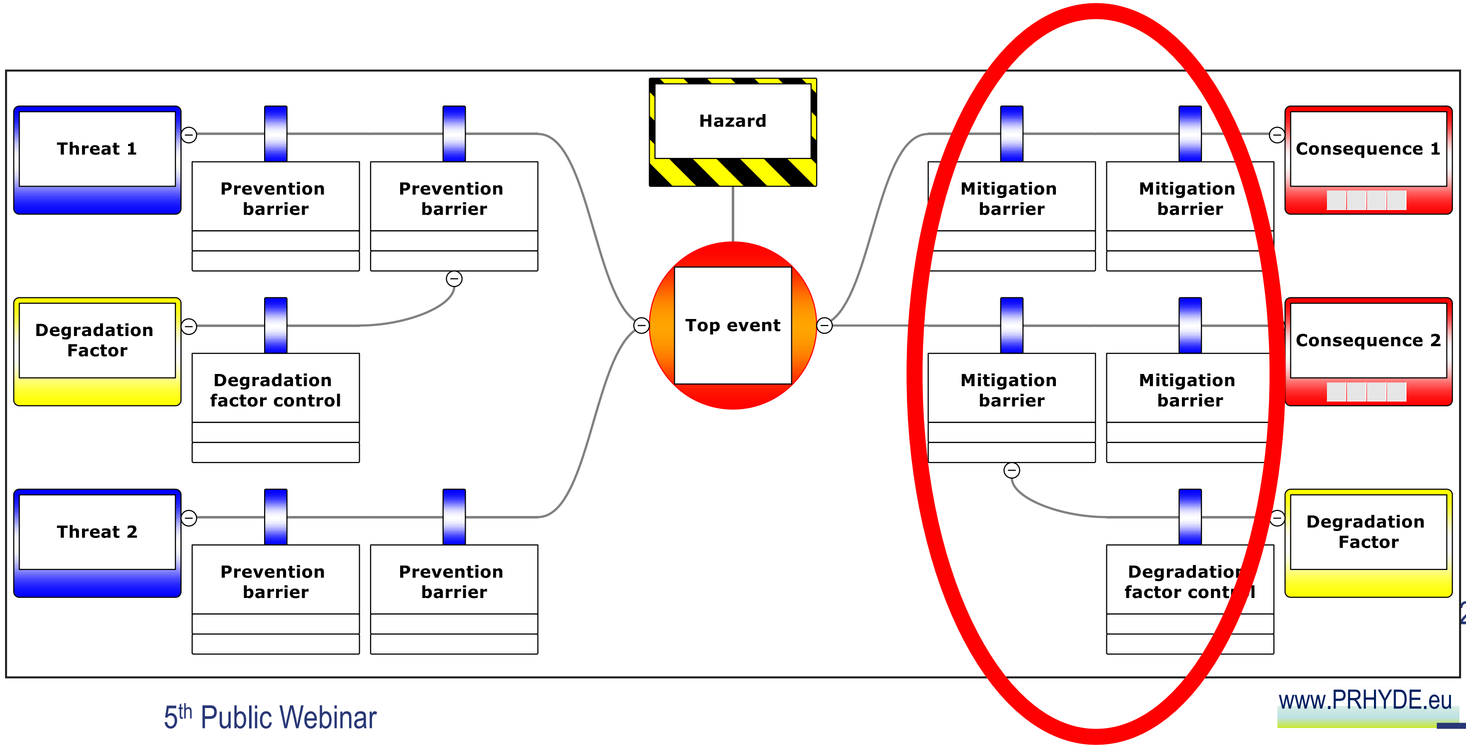


Mitigative barriers identified

- Station H2 Detector
- Vehicle H2 Detector
- Ultra-sonic Leak Detector

Top Event: Loss of Containment

Once Loss of Containment has occurred, these barriers does not mitigate much!



Preventive Barriers Identified

a) Redundant sensor monitoring

b) Vehicle Abort Signal

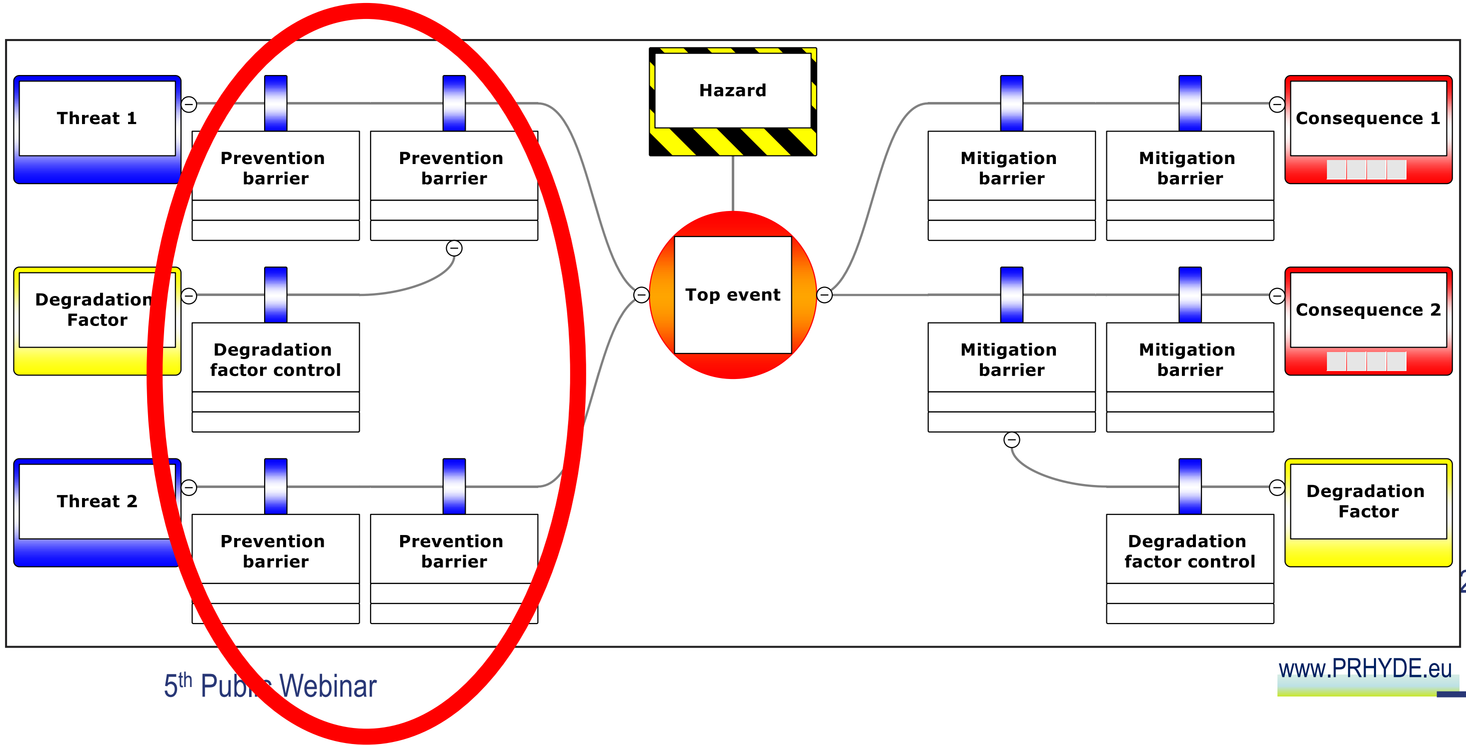
c) Vehicle Shut-off Valve

d) Safety Max PRR Limit

e) Vehicle record last refueling

f) Integrity barrier

g) Qualifying CHSS to 95°C



Redundant Sensor Monitoring

- Description
  - A means to double-check if sensor measurements (Station Pressure, Fuel Temperature, Mass Flow) are correct
- Challenges
  - Additional station components
  - SIL rating on mass flow meters

Vehicle Abort Signal

- Description
  - A means for vehicle to observe danger and tell station to terminate flow of hydrogen
- Challenges
  - Safety critical: Abort signal treated as Emergency Stop (ISO 12100)
  - Safety critical: Heartbeat required

Vehicle Shut-off Valve

- Description
  - A means for vehicle to terminate flow of hydrogen
- Challenges
  - Not implemented in industry today

Safety Max PRR Limit

- Description
  - A secondary t-final table stored in the station process PLC (or safety PLC) using reference CHSS design. Safeguard to overheat.

- Challenges
  - Needs further inspection
  - Rebuilds headroom that we are trying to narrow

Vehicle record last refueling

- Description
  - A means for vehicle to determine if there has been fuelling history or not.
- Challenges
  - Added requirement for vehicle

Integrity barrier

- Description
  - A means to detect a fault in the mass flow measurement or station pressure measurement
- Challenge
  - Although defined in SAE J2601-1 2020, this barrier has not been sufficiently evaluated

Qualifying CHSS to 95°C

- Description
  - Qualifying CHSS up to 95C
  - If implemented, many of the identified risk scenarios are obsoleted!

- Challenges
  - Current UN GTR 13 provides requirements for 85C

Which barriers to implement?

- Redundant sensor monitoring
- Vehicle Abort Signal
- Vehicle Shut-off Valve
- Safety Max PRR Limit
- Vehicle record last refueling
- Integrity barrier
- Qualifying CHSS to 95°C

Which barrier to implement to cover for residual risk?

Which barriers to implement?

- **Risk Assessment Team has selected some favorite recommendations**

A. Redundant sensor monitoring

B. Qualify CHSS to 95C

- **Further work to be done towards end of PRHYDE Project**

Thoughts on non-scored threats

Non-scored threats – Incorrect Fuelling Parameters

PRHYDE
Protocol for heavy-duty Hydrogen refuelling

Tabel 17: T-final implementation - Potential Threats and Potential Mitigative Barriers

Potential Threats	Potential Mitigative Barriers
t-final values are derived incorrectly	• Use of a validated and industry accepted fuelling model, ideally with the automatic generation of t-final tables built into its functionality ✓ NREL's H2FillS fuelling model is one such candidate • Validation testing – testing should be defined in the fuelling protocol standard and should be conducted at defined conditions to ensure that: A) Flow rate constrained t-final values do not exceed the mass flow limit defined in the fuelling protocol standard (e.g. 300 g/s) B) Temperature constrained t-final values do not exceed the maximum T_{max} temperature utilized to derive the t-final values in the fuelling model
t-final vector or t-final tables are implemented or communicated incorrectly	• t-final vector verification ✓ A testing regimen / validation process may be defined in the fuelling protocol standard which provides guidance and recommendations to the vehicle OEM for validating that the vehicle communicates the appropriate t-final table and/or calculates and communicates the correct t-final vector based on a set of inputs. This should be done in a comprehensive manner to verify the calculation logic, table selection, and stored table values over the range of possible inputs.
Incorrect CHSS parts replaced during repair or maintenance	• OEM to require replacement with original equipment parts. • Communication ECU requires connections to each tank in the CHSS to confirm it is the correct specification. ✓ Tank could have an IC (for wired connection) or RFID chip (for wireless connection) integrated into the outer layer of the tank winding during manufacturing. ✓ ECU needs signal from each chip to function

Non-scored threats – Wrong station/vehicle pairing

PRHYDE
Protocol for heavy-duty Hydrogen refuelling

Wrong Station/Vehicle pairing

Tabel 18: Station/Vehicle pairing - Potential Threats and Potential Mitigative Barriers

Potential Threats	Potential Mitigative Barriers
Different Pressure Classes	• Mechanical interlock via the connector (nozzle and receptacle) • Communication of pressure class from station to vehicle and vehicle to station
Tank Volume out of Dispenser scope	• Communication of the CHSS volume from the vehicle to the dispenser • Application of an independent volume measurement by the station • Application of error checking methodology such as the Integrity Check described in Appendix L of SAE J2601

Non-scored threats – Programming error, PLC/ECU failure

PRHYDE
Protocol for heavy-duty Hydrogen refuelling

- Factory Acceptance Testing of Station / Vehicle
- Recommendation to use practices of IEC 61508 / 61511 and ISO 26262
- Recommendation to have Management of Change system in place upon modifications of software

Next Steps

Next Steps

- Further work on barrier recommendations
- "No down-selection"
- Wrapping up Protocol Development

Contact

Website: www.PRHYDE.eu

E-Mail: info@PRHYDE.eu

Coordinator:

Ludwig-Bölkow-Systemtechnik GmbH
Daimlerstr. 15
85521 München/Ottobrunn
Web: http://www.lbst.de