Use Fault Tree Analysis When LOPA Fails

LOPA is Ubiquitous – but Simple…

- Most Chemical Process Industries Companies Employ Layer of Protection Analysis (LOPA)
  - Assess Process Hazards Analysis (PHA) scenario in more detail
  - High consequence scenarios
  - Complex scenarios
  - Scenarios using safeguards that require quantitative performance targets

- Originally an order-of-magnitude technique
  - More than PHA, less and quantitative risk analysis (QRA)
  - Focus on preventive safeguards that are entirely independent

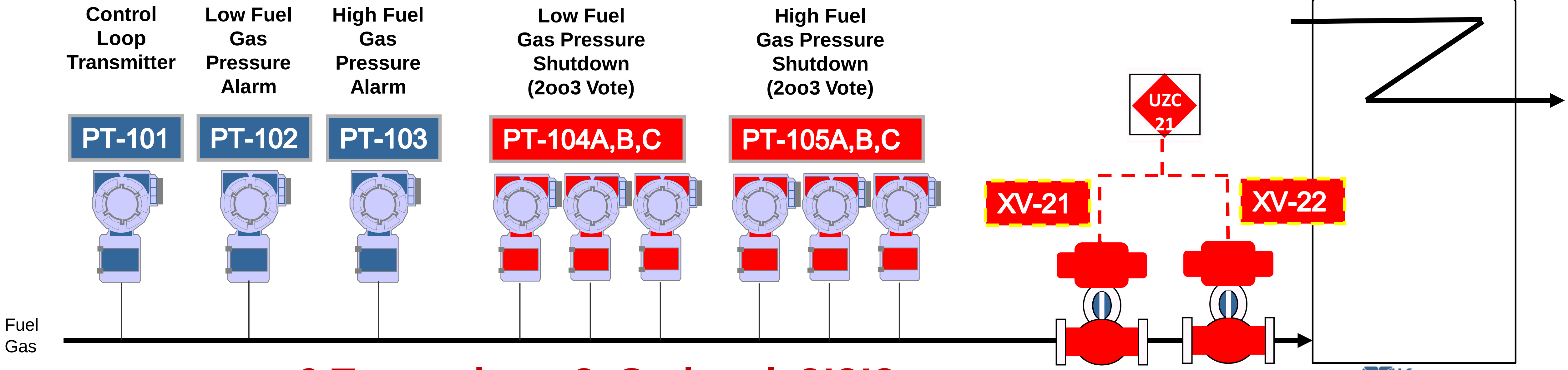
LOPA Ineffective in Some Cases

- The simplifications in LOPA result in inaccurate estimate of risk
- Common Situations where LOPA fails
  - Initiating Event IS the loss of containment
  - Use of Consequence Mitigation is Primary/Important Risk Reduction
  - Intermittent/Batch Operation
  - Protection Layers Employ Common/Shared Subsystems
  - Extensive Human Interaction in Scenario (with Shared Hardware)
  - Complex Logic / Sequences
- Oversimplifications can lead to sub-optimal design

Consider Supplementing with Fault Tree Analysis

Fired Heater Fuel Gas Pressure Safety

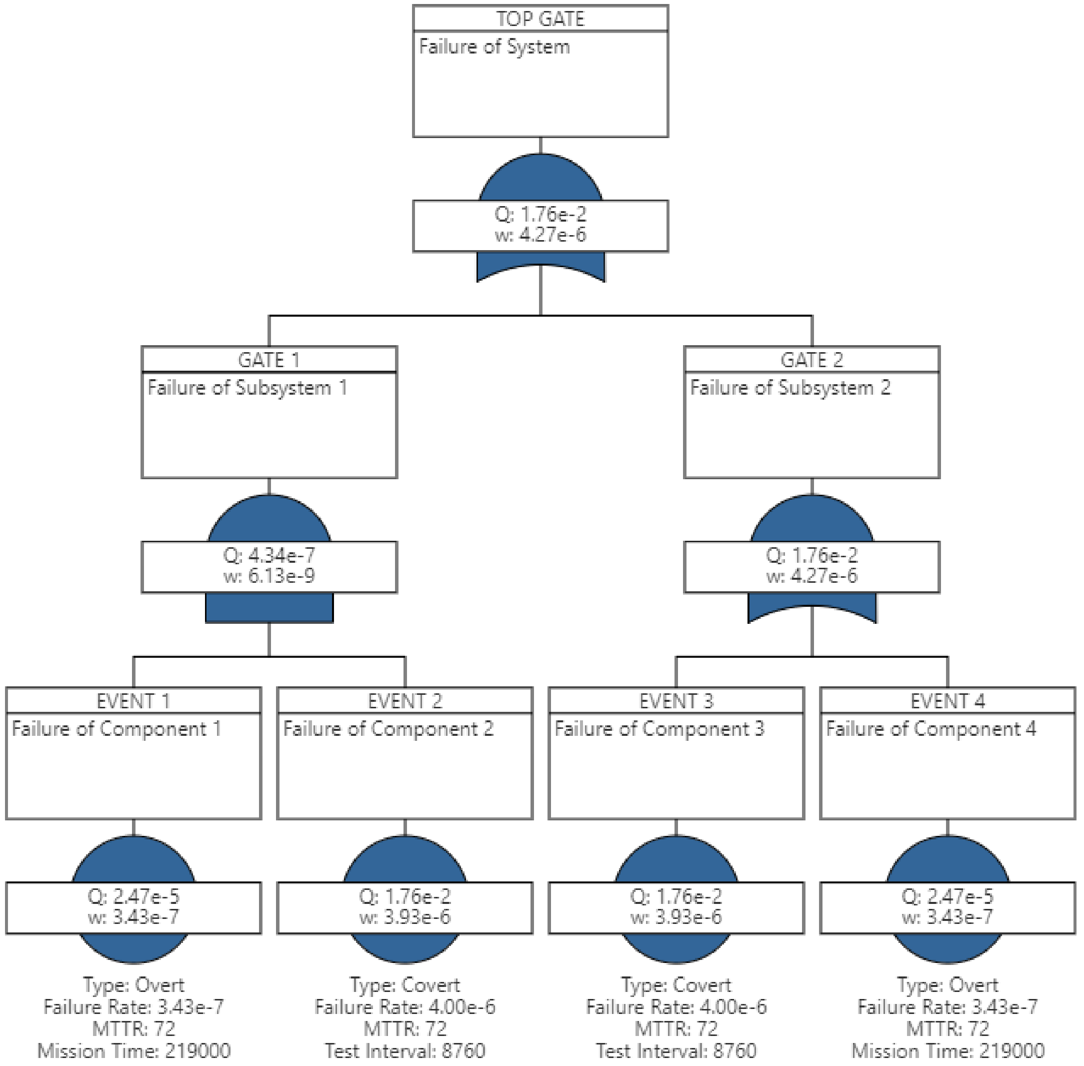
Deviation	Consequences							
	Consequence	S	TMEL Safety	Causes				RRF Safety
				Cause	Frequency	IPLs		
						IPL	PFD	
1.1 High Pressure	1.1.1 Unstable combustion. Potential Loss of Flame with Continued Introduction of Fuel Gas. If ignited, potential firebox explosion. Potential Serious Injury.	H	1E-4	1.1.1.1 Fuel Gas Control Loop Fails Valve Toward Open Position	0.1	1 Operator Intervention Based on Alarm	0.1	10
						3 High Fuel Gas Pressure SIF	0.1	
1.2 Low Pressure	1.2.1 Unstable combustion. Potential Loss of Flame with Continued Introduction of Fuel Gas. If ignited, potential firebox explosion. Potential Serious Injury.	M	1E-3	1.2.1.1 Fuel Gas Control Loop Fails Valve Toward Closed Position	0.1	2 Operator Intervention Based on Alarm	0.1	1
						4 Low Fuel Gas Pressure SIF	0.1	



9 Transmitters? Seriously?!?!?

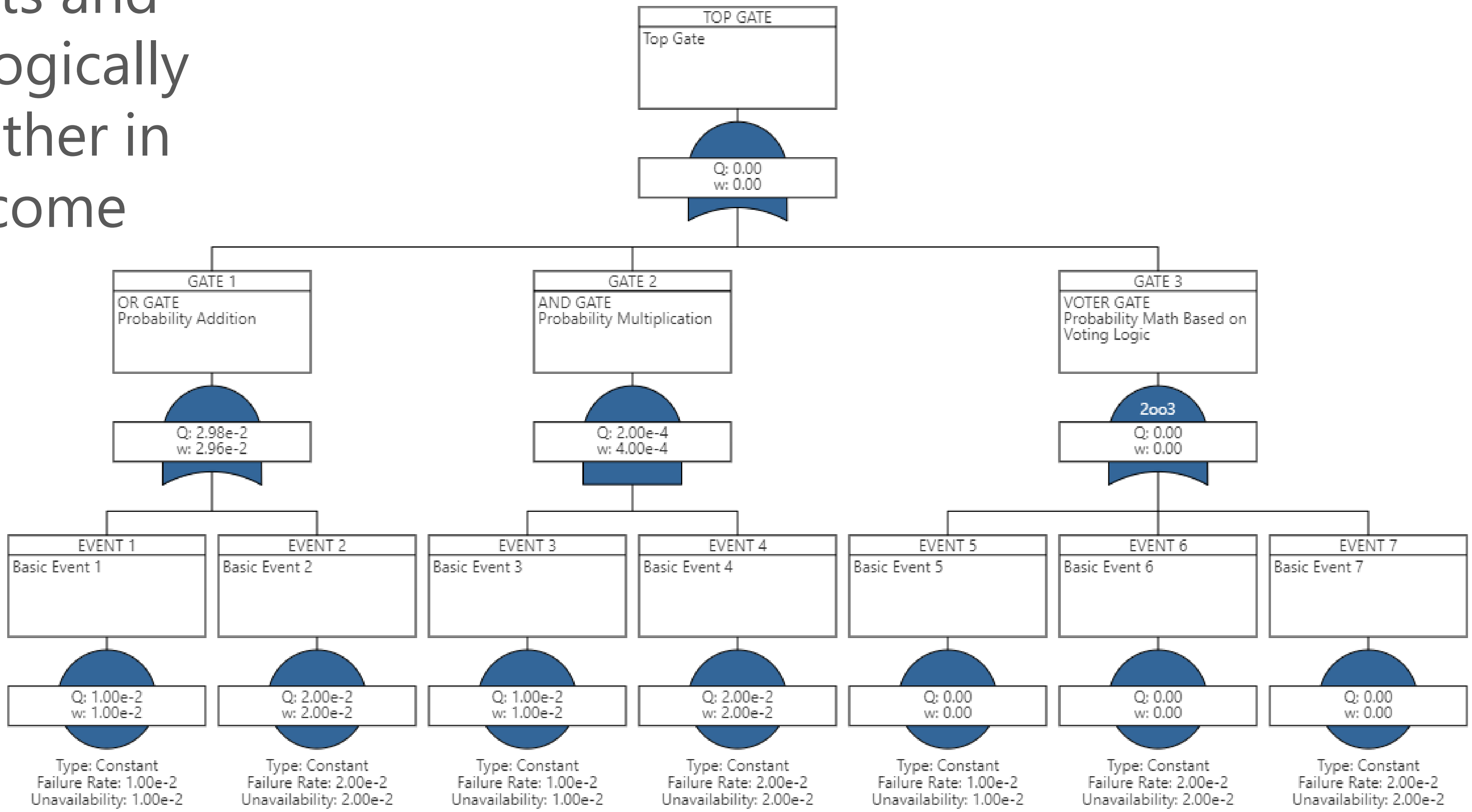
Fault Tree Analysis

- More detailed assessment of events leading to loss of containment
- Capable of complex logic
- Elegant handling of shared components
- Calculates frequency of Top Event based on basic events and logic gates



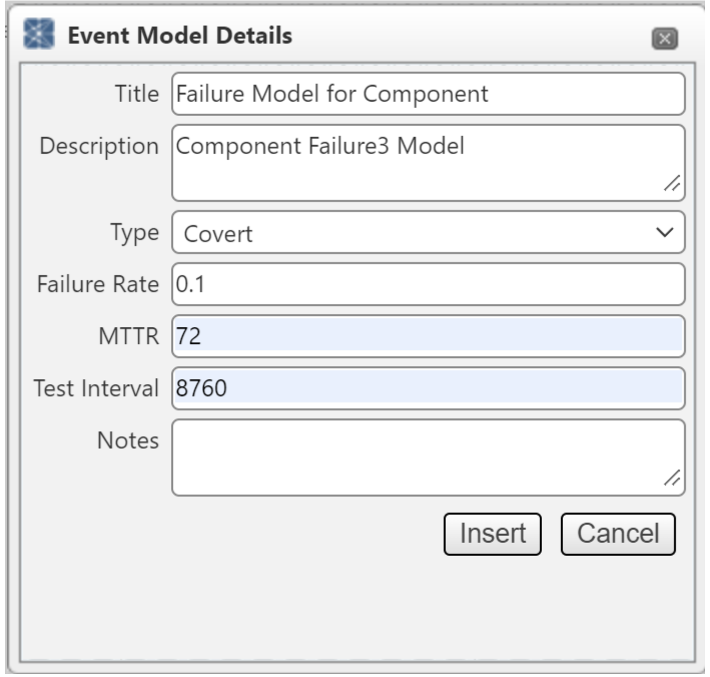
Fault Tree Gates

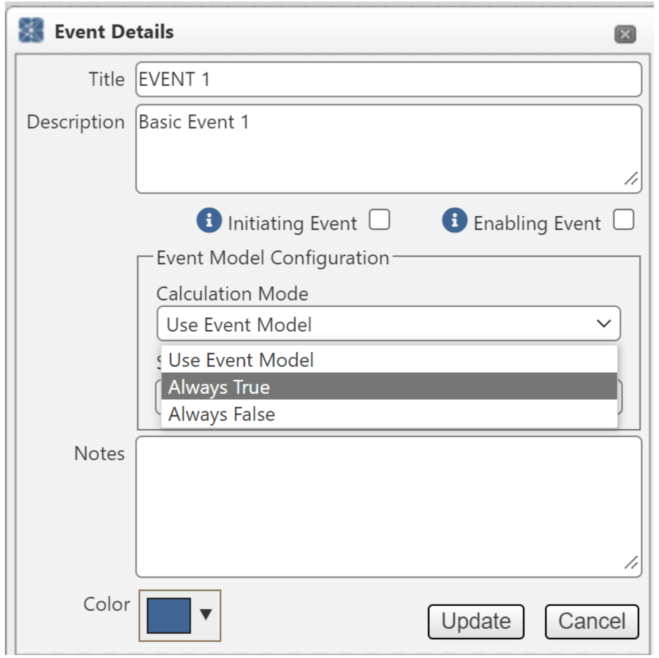
- Define how events and lower gates are logically related to each other in defining the outcome
- Common Gates
  - AND
  - OR
  - VOTE

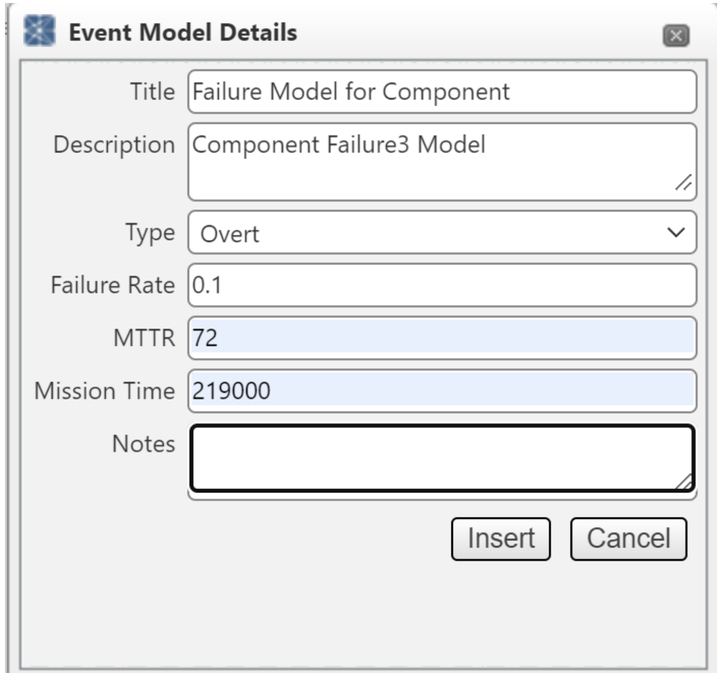


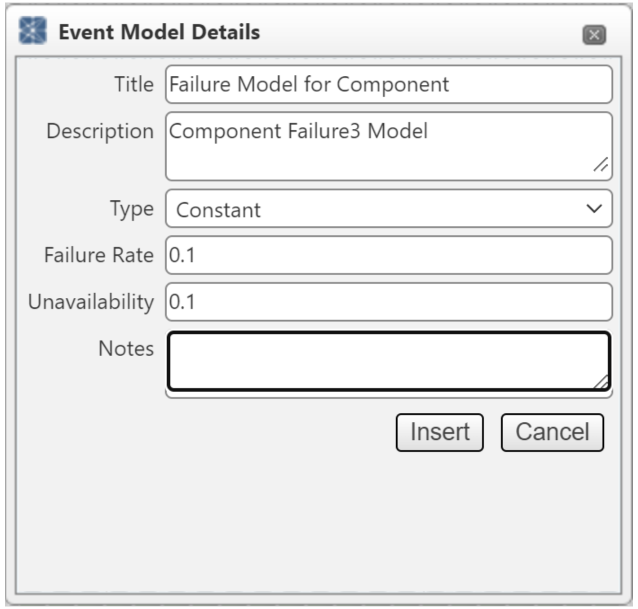
Basic Events

- Lowest Level
- Items that are not subdivided into smaller components
- Failure probabilities or failure rates are quantified
- House Events (True or False only)
- Failure Models
  - Overt
  - Covert
  - Constant



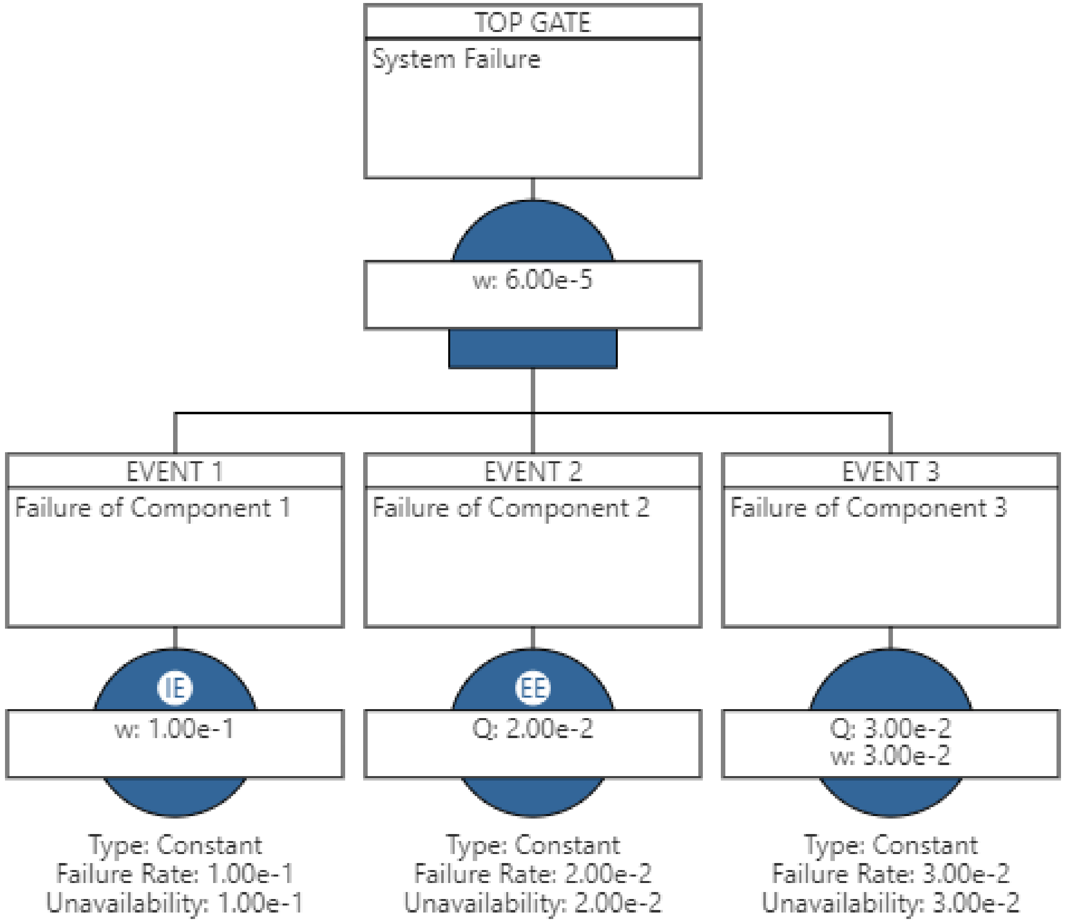




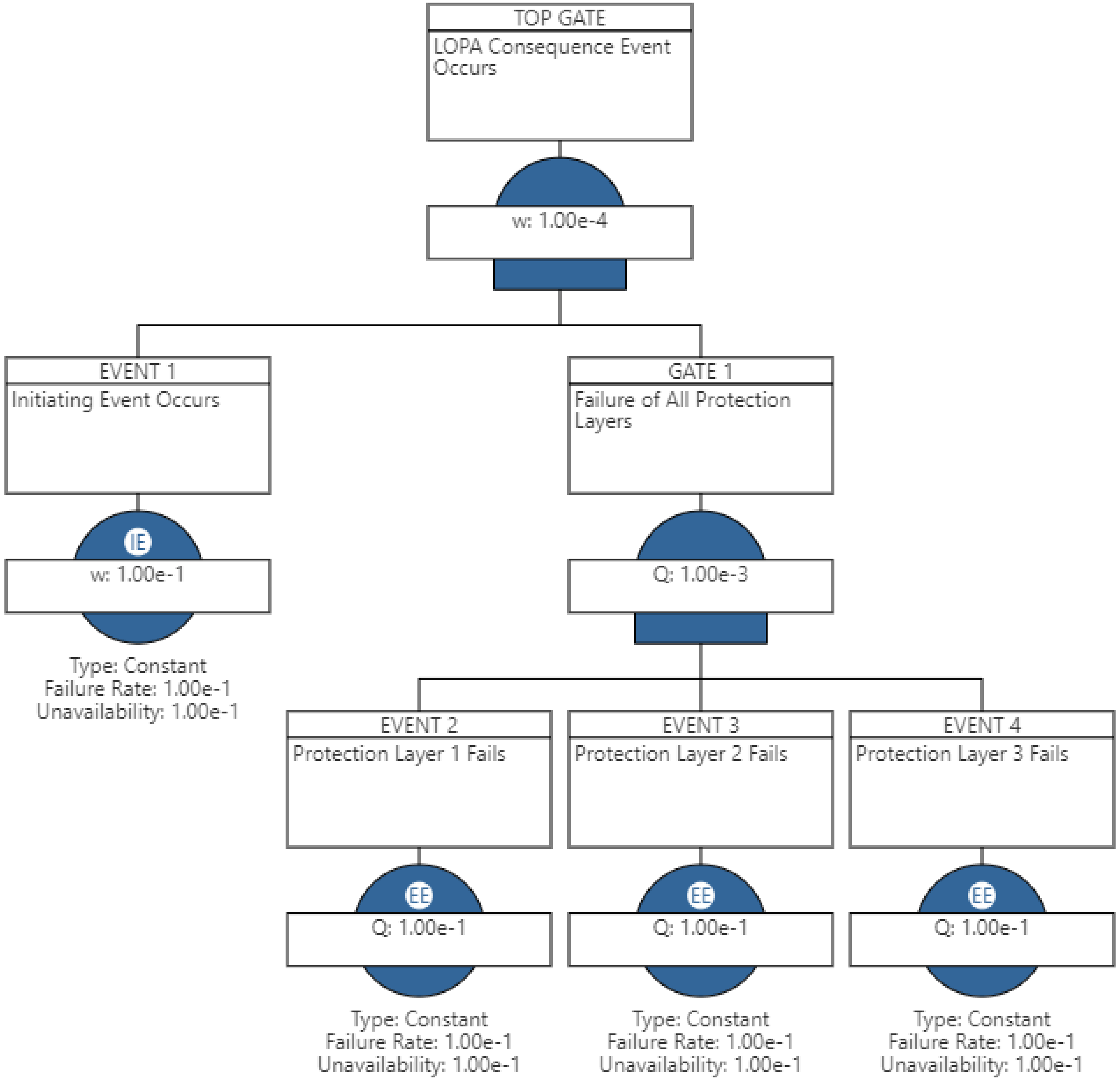


Fault Tree Sequencing

- Initiators
  - Events that start the failure chain
  - Quantified as frequencies only
- Enablers
  - Events that allow a failure chain to continue/propagate
  - Quantified as probabilities only
- Initiator or Enabler
  - Either starts or propagates failure chain
  - Frequency and Probability Quantified

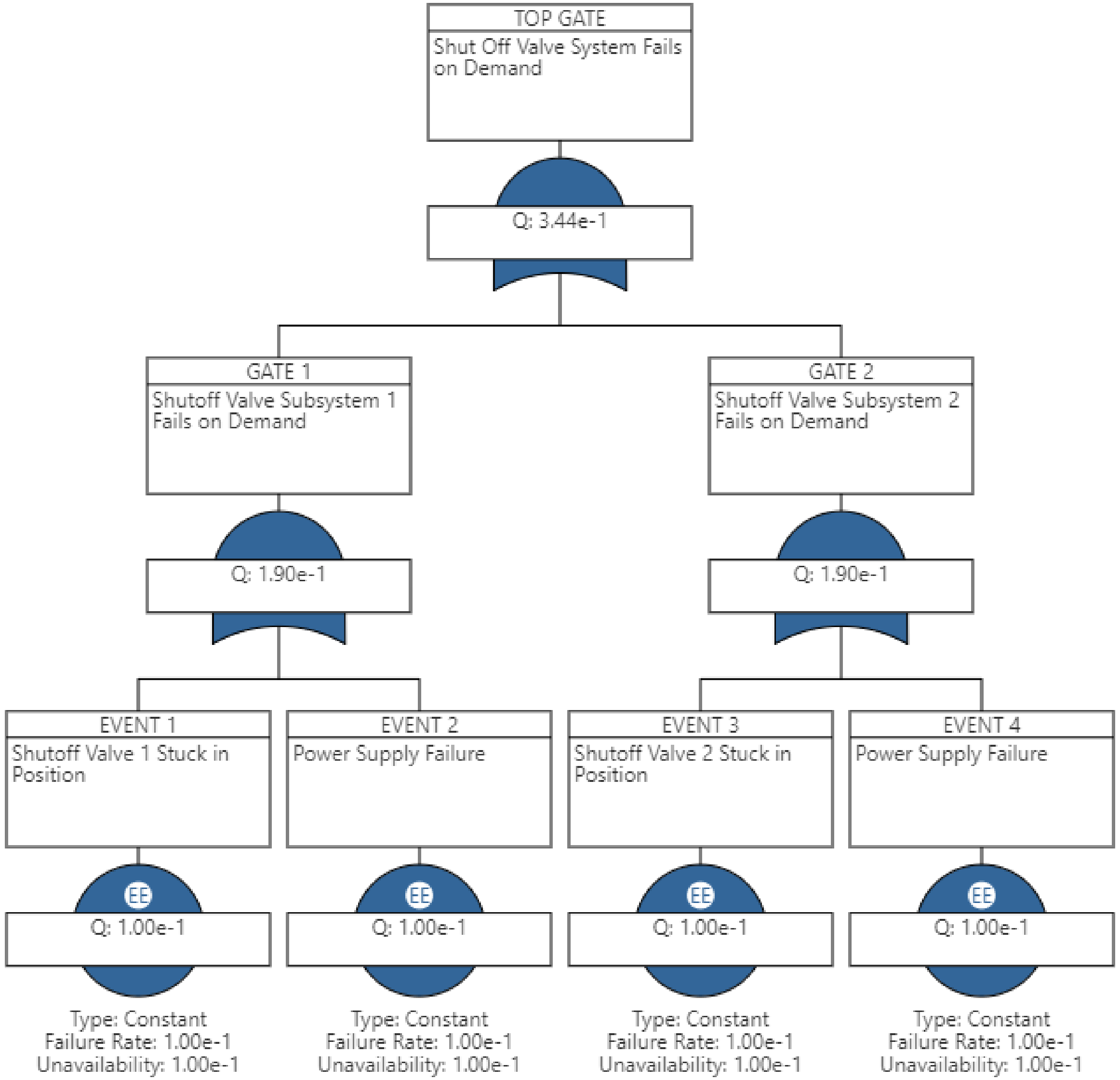


LOPA as a Fault Tree



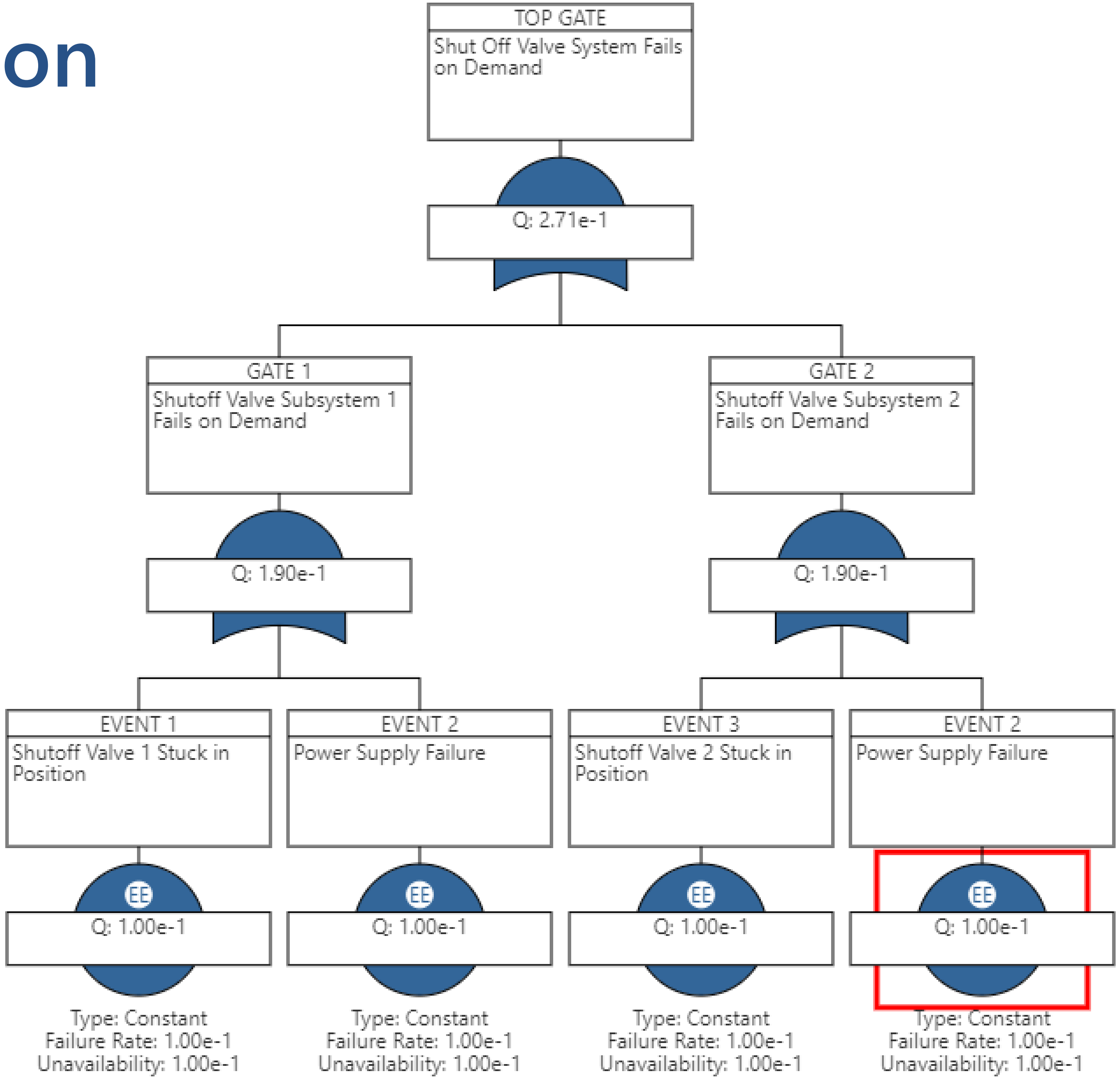
Fault Tree Solution

- Gate-by-Gate Solution
  - P(A or B) = P(A) + P(B) – P(A and B)
  - Etc.
- Cut Set Solution
  - EVENT 1 or
  - EVENT 2 or
  - EVENT 3 or
  - EVENT 4

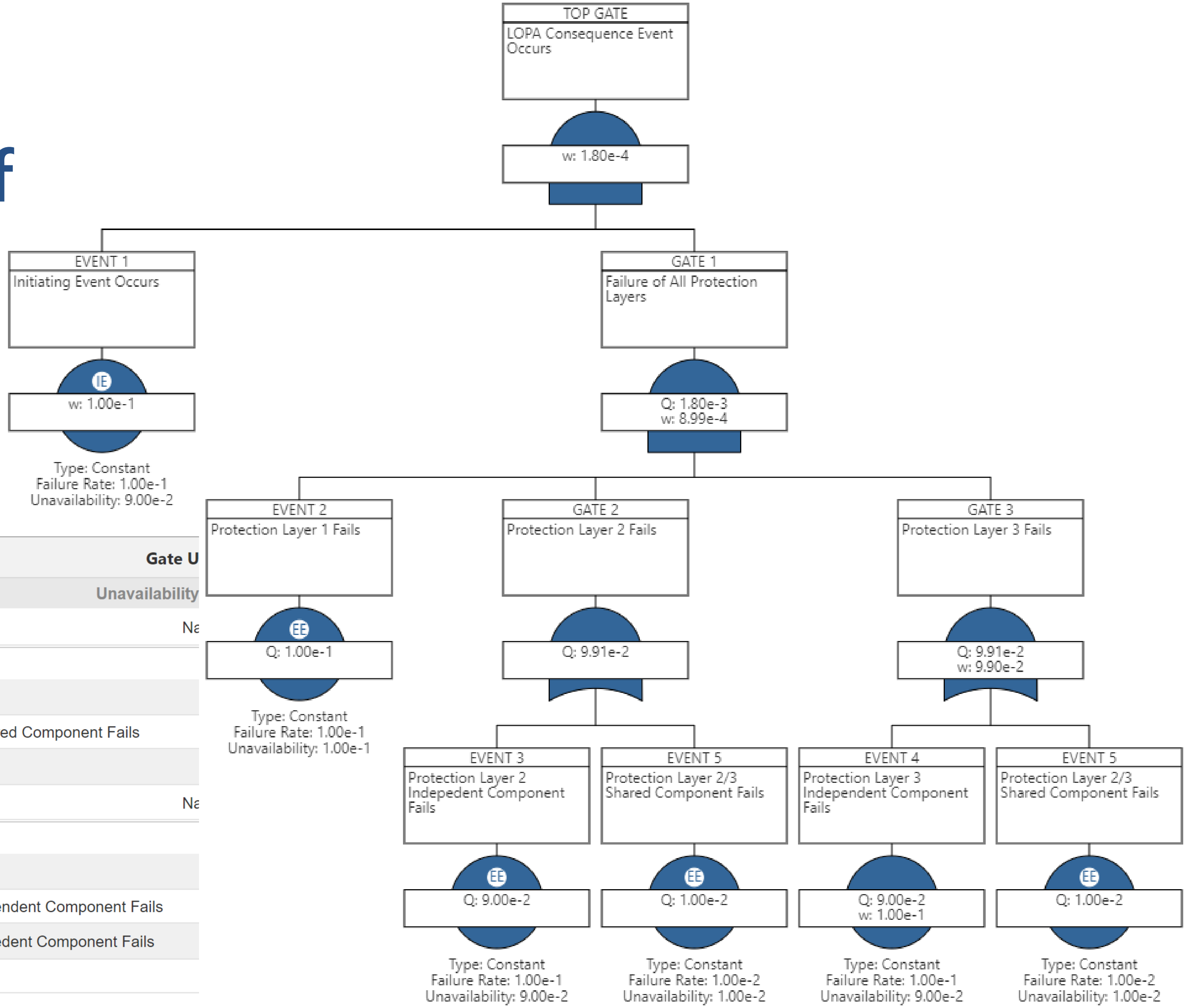


Minimal Cut Set Solution

- Generate Complete Cut Set
- Remove Duplicates
- Minimal Cut Set
  - EVENT 1 or
  - EVENT 2 or
  - EVENT 3 or
  - EVENT 2



Elegant Handling of Commonality of LOPA Scenario



Select Gate TOP GATE **Gate U**

Cut Set	Number of Events	Unavailability
Cut Set 1	3	Na

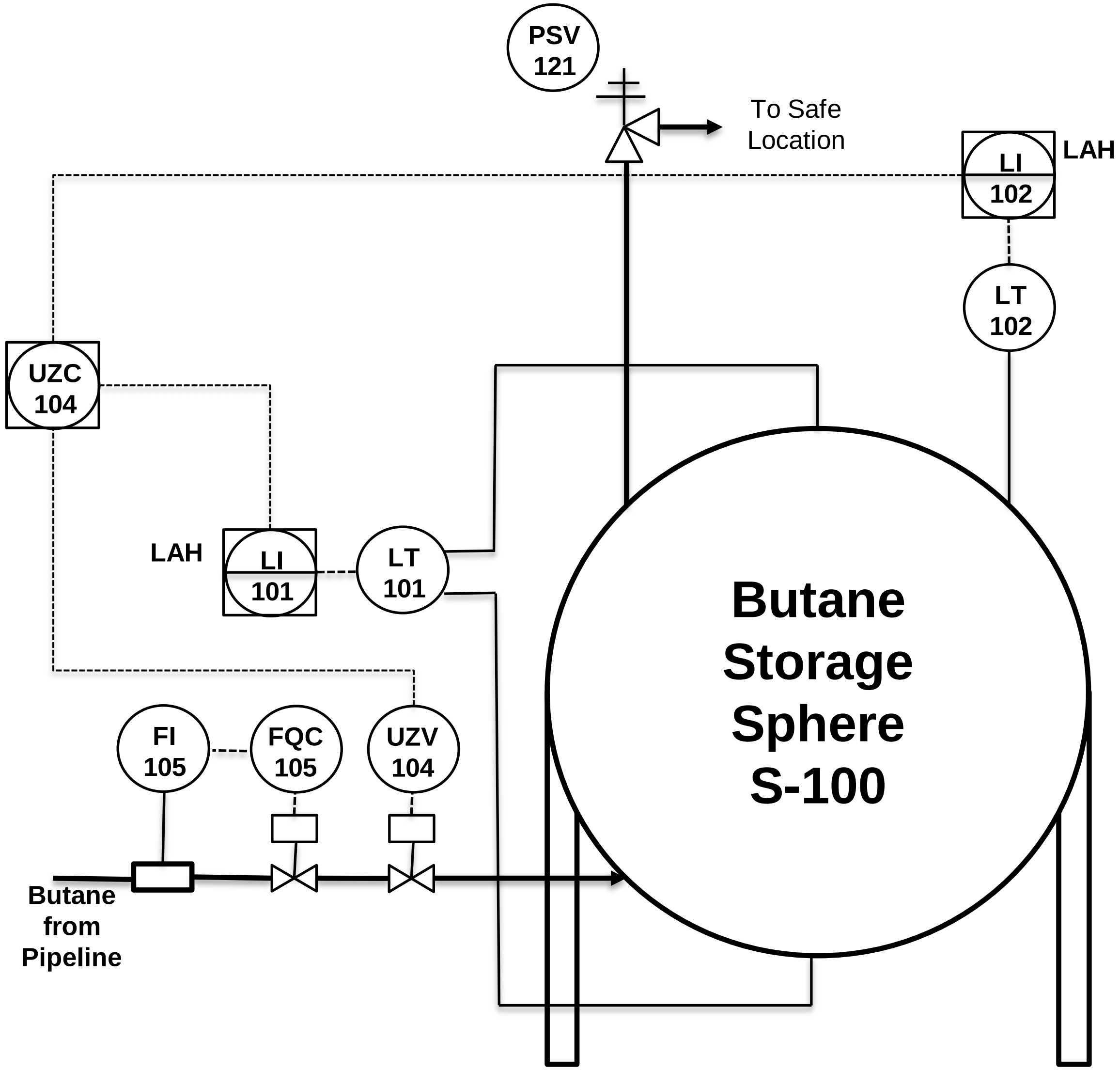
Event Title	Event Description
EVENT 2	Protection Layer 1 Fails
EVENT 5	Protection Layer 2/3 Shared Component Fails
EVENT 1	Initiating Event Occurs

Cut Set	Number of Events	Unavailability
Cut Set 2	4	Na

Event Title	Event Description
EVENT 2	Protection Layer 1 Fails
EVENT 4	Protection Layer 3 Independent Component Fails
EVENT 3	Protection Layer 2 Independepent Component Fails
EVENT 1	Initiating Event Occurs

Case Study – Butane Sphere Loading Overfill

- Butane sphere filled from pipeline
  - Amount calculated by operator based on LT-101 or LT-102
  - Amount input to totalizer controller FQC-105
  - If overfilled, alarms occur on LI-101 and LI-102
  - If LI-101 or LI-102 exceed their high-level trip point, an automatic shutoff occurs by closing UZV-104
  - PSV not sized for overfill



Case Study – First Pass LOPA Failure…

KENEXIS OPEN PHA

Signe

Study Data | Nodes | Deviations | PHA Worksheets | LOPA Worksheets | Check Lists | Recommendations | Safeguards | Parking Lot | Risk Criteria

LOPA Worksheets

1. Butane Storage Sphere S-100

Searc

Deviation	Consequences							
	Consequence	S	TMEL Safety	Causes				RRF Safety
				Cause	Frequency	IPLs		
						IPL	PFD	
1.1 High Level	1.1.1 Overpressure of Storage Sphere S-100 with Potential Loss of Mechanical Integrity and Rupture. Potential Vapor Cloud Explosion and/or Large Pool Fire	H	1E-4	1.1.1.1 Failure of Filling Control Loop	0.1	1 Operator Intervention Based on LAH-101	0.1	0
						2 Operator Intervention Based on LAH-102	0.1	
						3 High Level Shutdown Safety Instrumented Function (SIL 2)	0.01	

Case Study – First Pass LOPA Failure…

- Initiating event is more complex than control loop failure
  - Transfers are a batch operation that occur multiple times per year
  - Calculation of transfer amount is source of failure
    - Calculation error
    - Level measurement error
  - Control loop hardware failure can occur, but only an issue during transfer
  - Frequency of transfers drives the risk, more transfers = more risk
- Every protection layer shares components with other protection layers

Case Study – Second Attempt LOPA

Deviation	Consequence	S	TMEL Safety	Cause	Frequency	IPL	PFD	RRF Safety
	Consequences							
				Causes				
						IPLs		
1.1 High Level	1.1.1 Overpressure of Storage Sphere S-100 with Potential Loss of Mechanical Integrity and Rupture. Potential Vapor Cloud Explosion and/or Large Pool Fire	H	1E-4	1.1.1.1 Failure of Filling Control Loop while filling	0.1	1 Operator Intervention Based on LAH-101	0.1	260
						2 Operator Intervention Based on LAH-102 - No Credit Taken, Common Operator	1	
						3 High Level Shutdown Safety Instrumented Function (SIL 2) - No Credit Taken, Common Level Sensor	1	
				1.1.1.2 Error in Calculating Fill Amount - 8 fills per year, 0.01 probability of failure per fill	0.08	4 Operator Intervention Based on LAH-101 - No credit taken, not independent from amount calculation measurement	1	
						5 Operator Intervention Based on LAH-102	0.1	
						3 High Level Shutdown Safety Instrumented Function (SIL 2) - No Credit Taken, Common Level Sensor	1	
				1.1.1.3 Error in Entering Fill Amount - 8 fills per year, 0.01 probability of failure per fill	0.08	1 Operator Intervention Based on LAH-101	0.1	
						2 Operator Intervention Based on LAH-102 - No Credit Taken, Common Operator	1	
						3 High Level Shutdown Safety Instrumented Function (SIL 2) - No Credit Taken, Common Level Sensor	1	

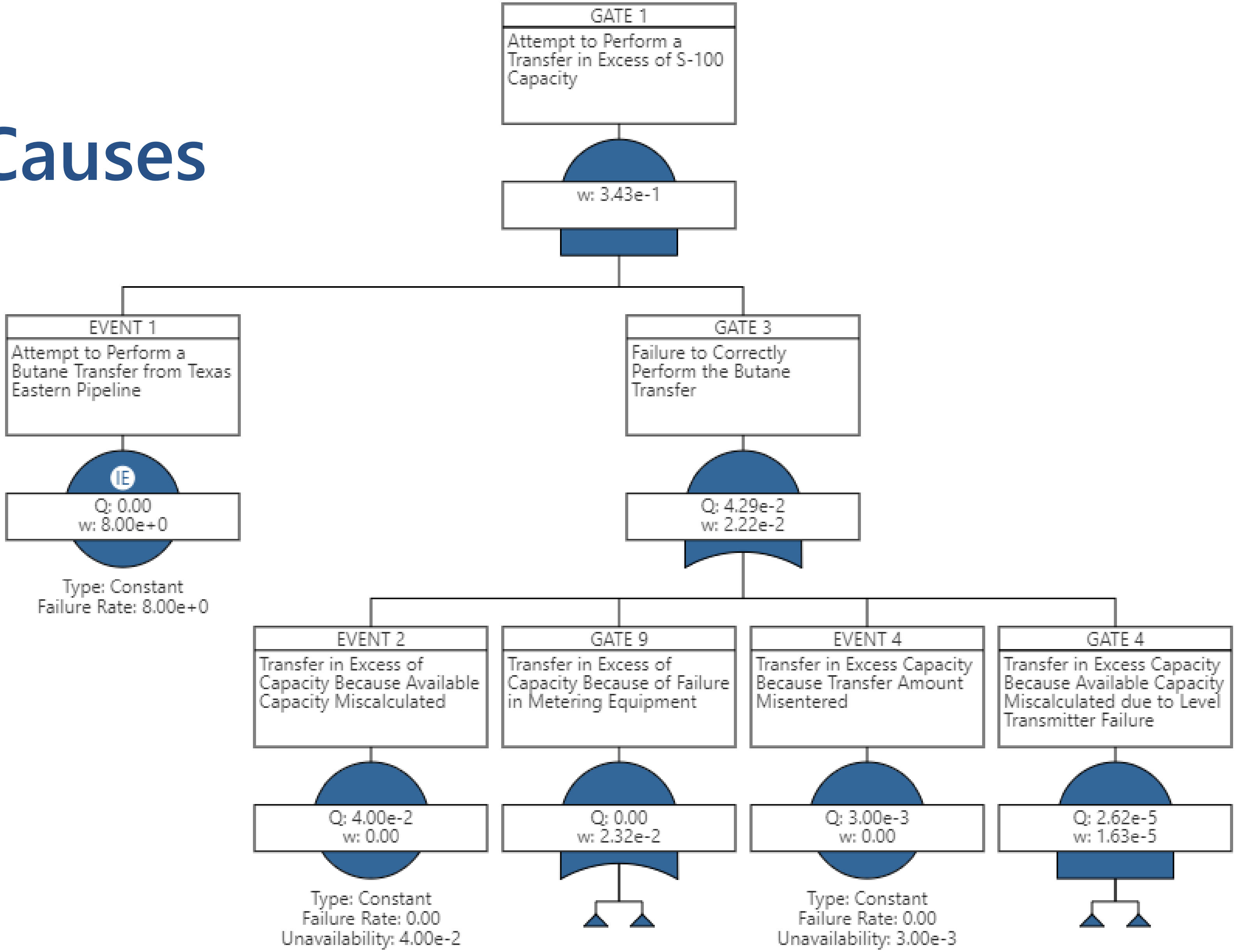
KENEXIS

Case Study – Second Attempt LOPA

- Better, but still not good
- Analysis shows that more than two orders of magnitude of risk reduction are still required
- Recommendations might include
  - Include a dedicated measurement of level for control/calculation purposes
  - Include two new dedicated level measurements for the Safety Instrumented Function
  - This could result in 5 different level measurements on the vessel… Is 5 transmitters that much better than two???

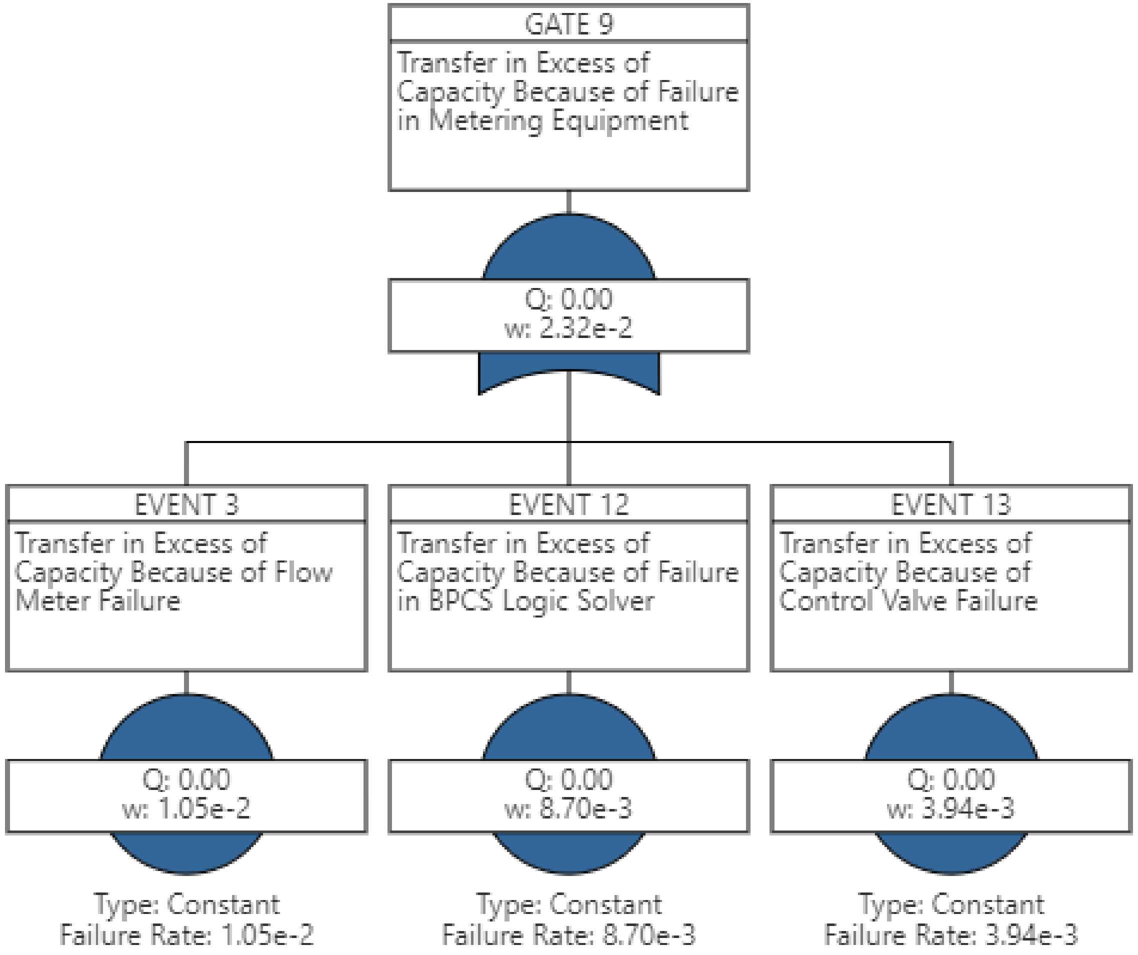
Case Study FTA – Initiating Events/Causes

- Consider all causes of overfill
- Initiator is attempt to perform transfer, given frequency
- Causes of failure must be conditional probabilities "per transfer"



Case Study FTA – Failed Metering Equipment

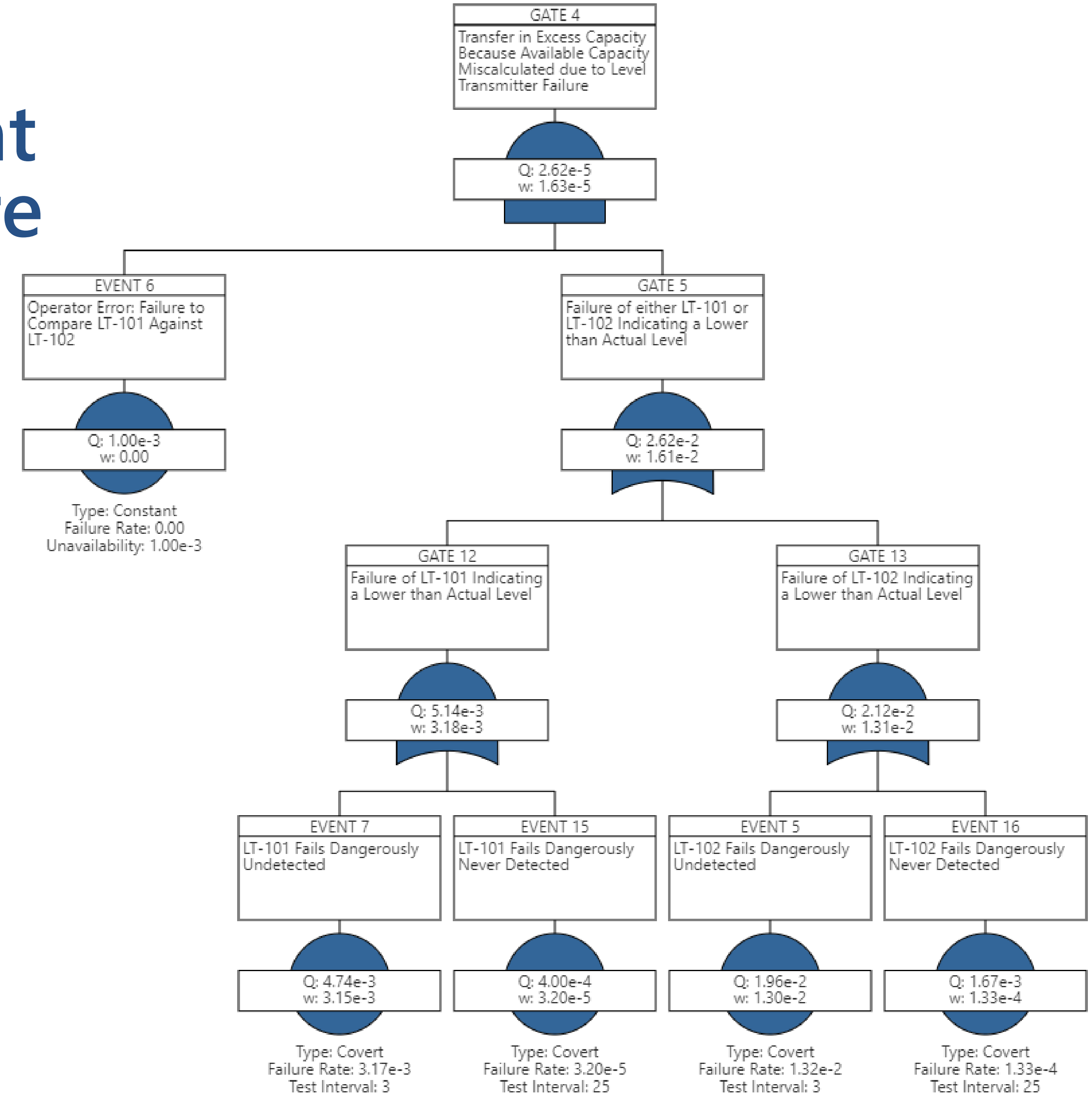
- Calculation of Failure Probability Must Consider Testing
  - Is the control loop testing before each transfer?
  - If so, the "mission time" is only the duration of the transfer, not the test interval
  - Otherwise, use traditional test interval



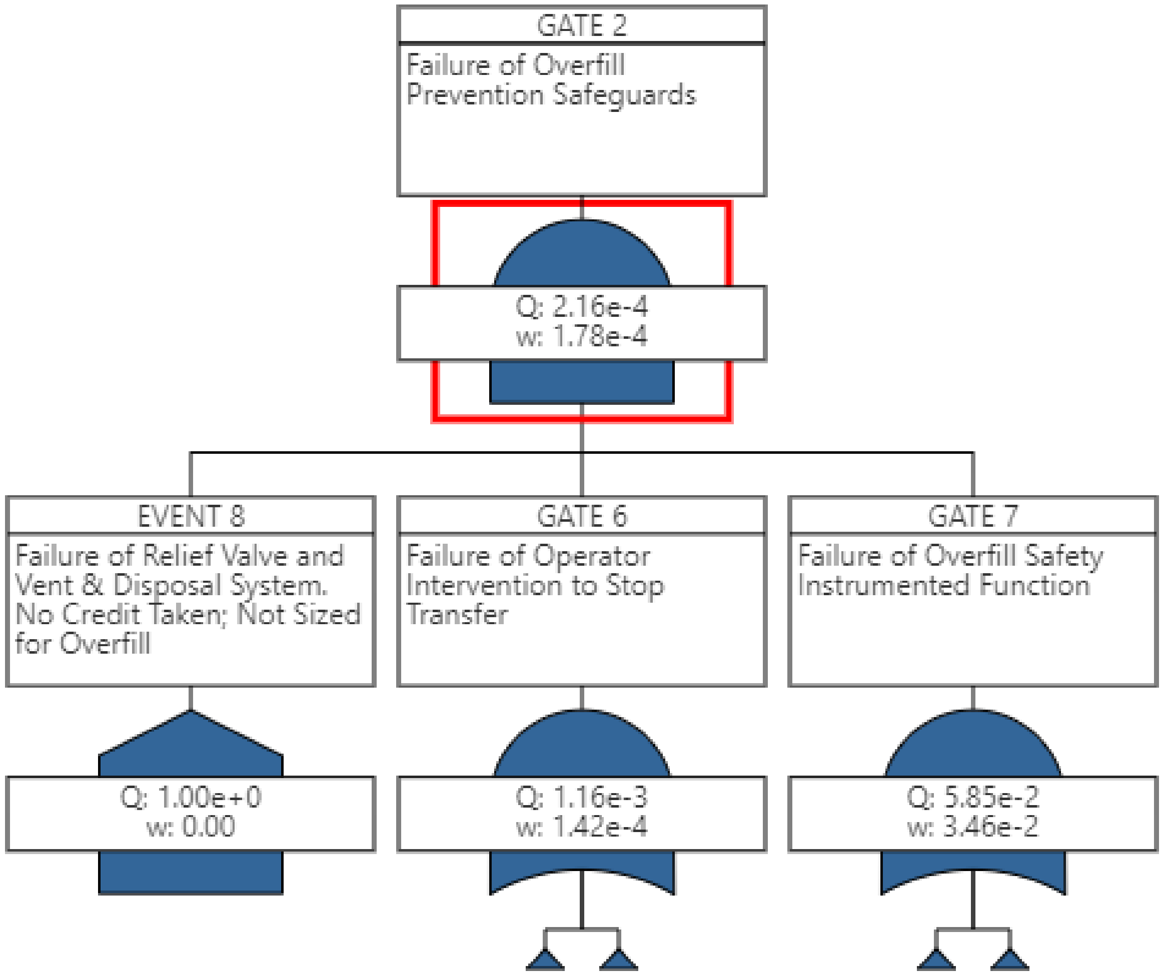
KENEXIS

Case Study FTA – Miscalculation of Amount Due to Transmitter Failure

- Transmitter failure events are considered in multiple locations
  - Measurement for calculation of transfer amount (shown here)
  - Operator response to alarm
  - Safety instrumented function effectiveness

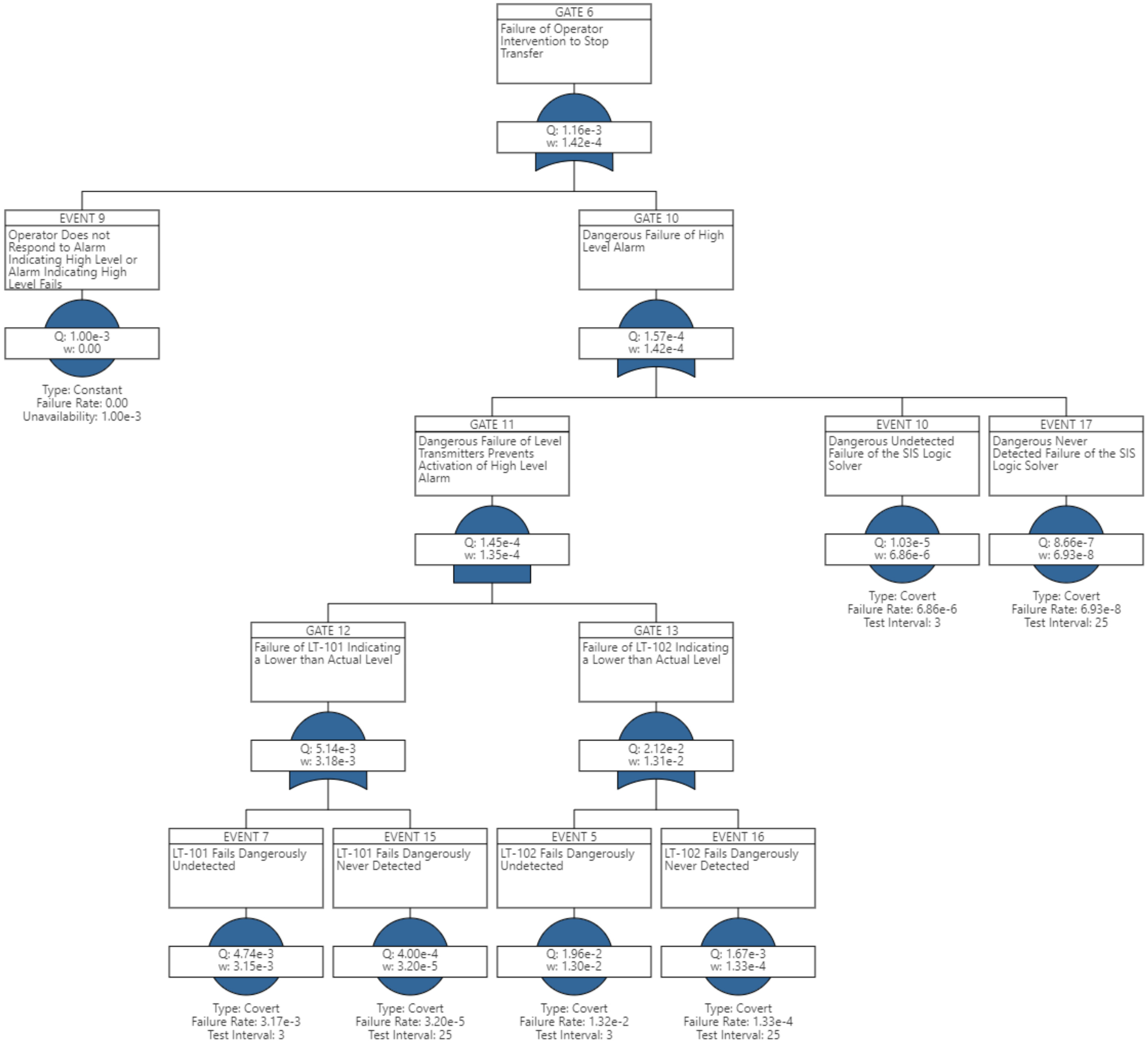


Case Study FTA – Failure of Safeguards

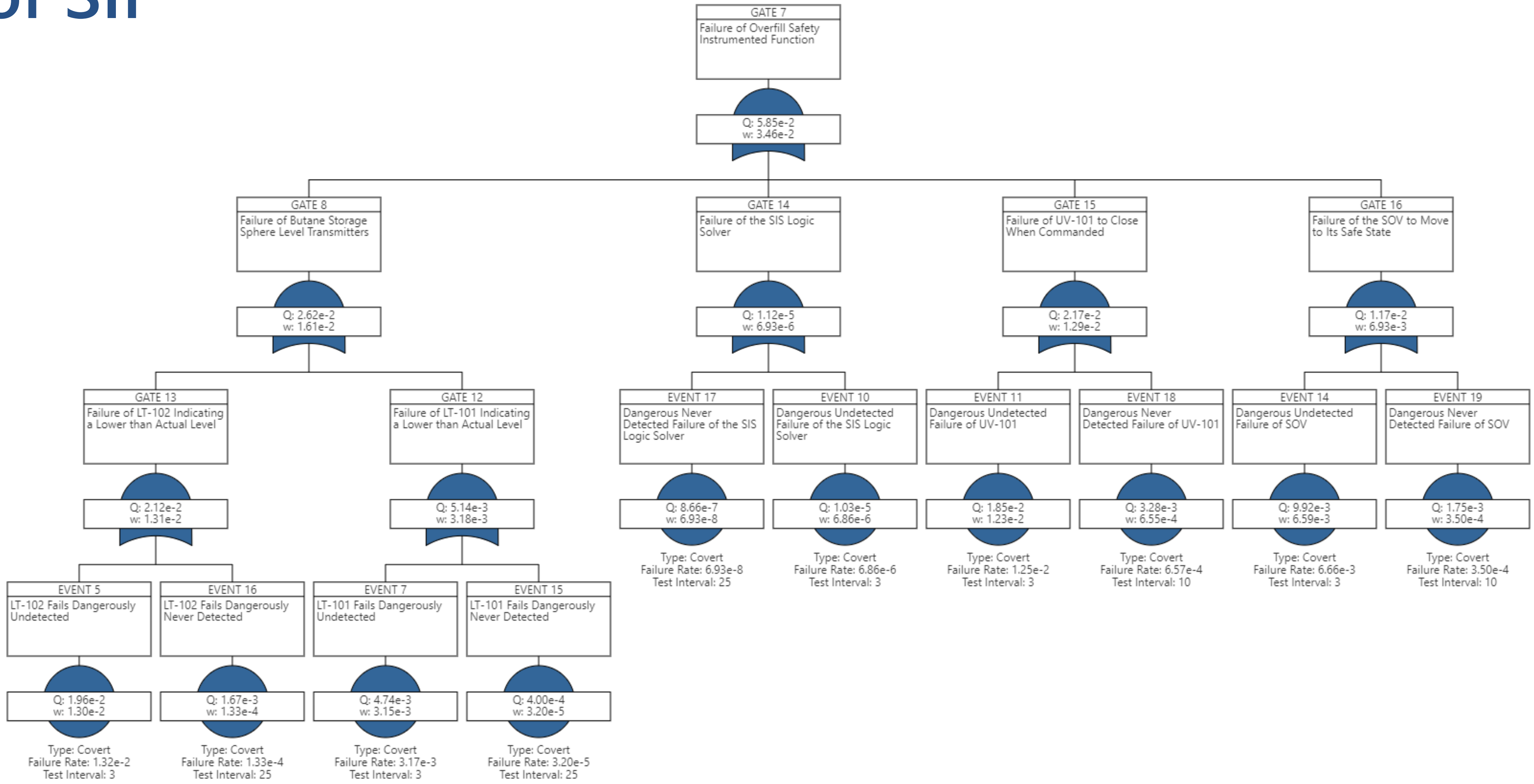


Case Study FTA – Failure of Operator Intervention

- Separation of operator action from equipment failure
- Equipment failure is the same event structure as for miscalculation for sensors

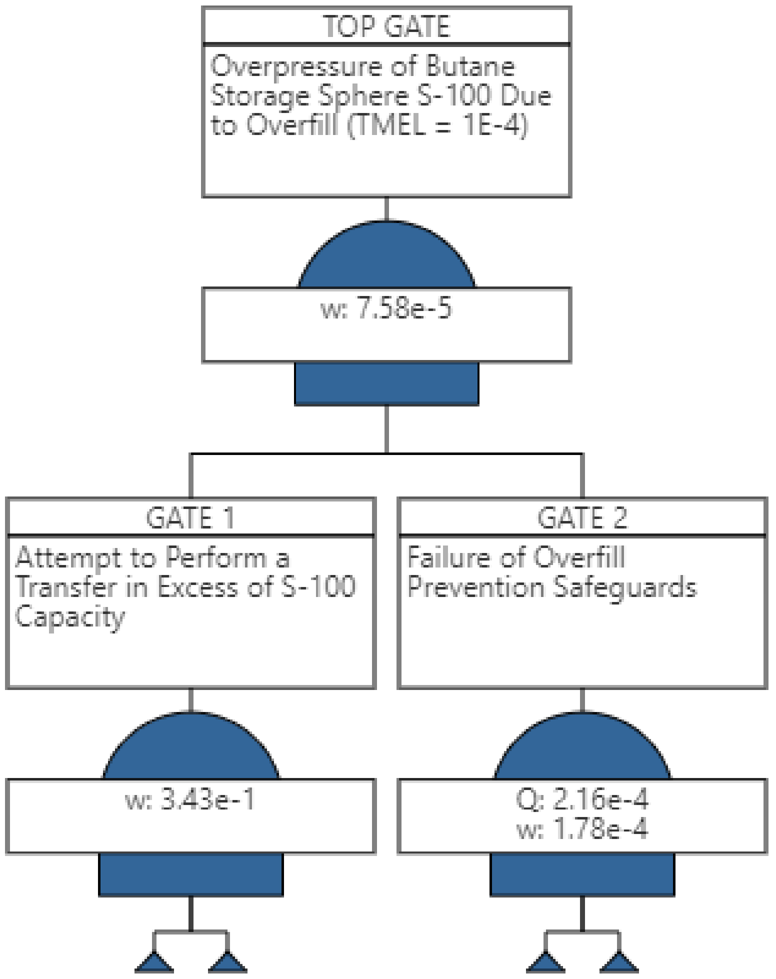


Case Study FTA – Failure of SIF



Case Study FTA Overall Results

- Overpressure (top event) occurs if excess butane is attempted to be transferred and all safeguards fail
- Tolerable risk is achieved with existing design after more sophisticated analysis



Summary

- LOPA is ubiquitous, but simplifications sometimes prevent accurate calculation of actual risk
  - Potential for poor design recommendations
  - Potential for overdesign and high cost (CAPEX and OPEX)
- When LOPA provides questionable results investigate cause
  - Inability to consider protection layers with common equipment
  - Complexity of scenario requires simplification
- Supplement LOPA with FTA to address identified shortcomings

Thank you…

Figures created using Kenexis Open PHA and Kenexis Arbor Software…