NTNU – Trondheim
Norwegian University of
Science and Technology

MR 8406 Operational risk analysis

Modelling hazardous events for decision support

S. Lee, Y. Liu & N. Paltrinieri

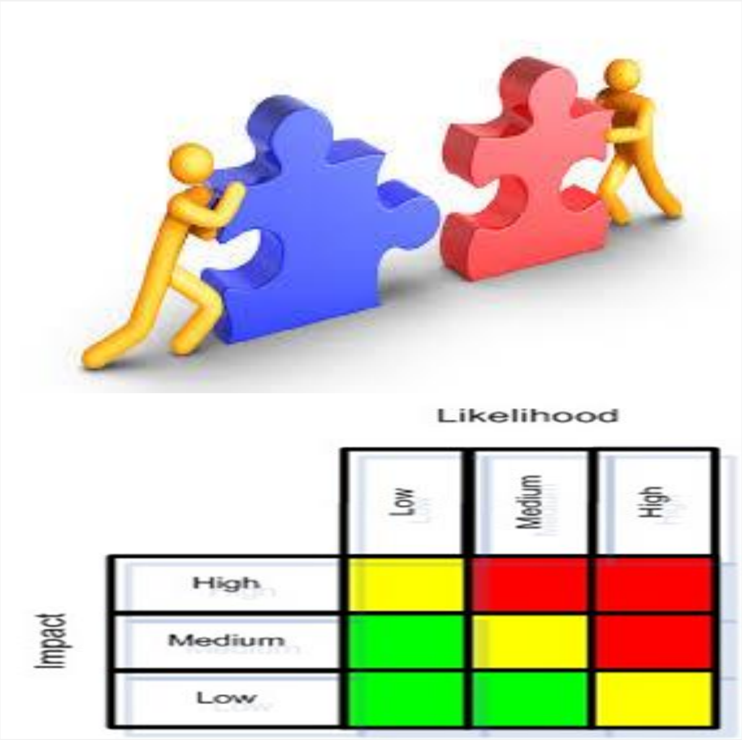
Shenae Lee
10 March 2017
(To be presented in ESREL)

Thank you to S.Haugen and X.Yang for valuable comments

The presentation is about

- A brief introduction to operational risk analysis
- Case study: modelling event scenario (storage tank overfill)
- Summary
- Q & A

Point of departure



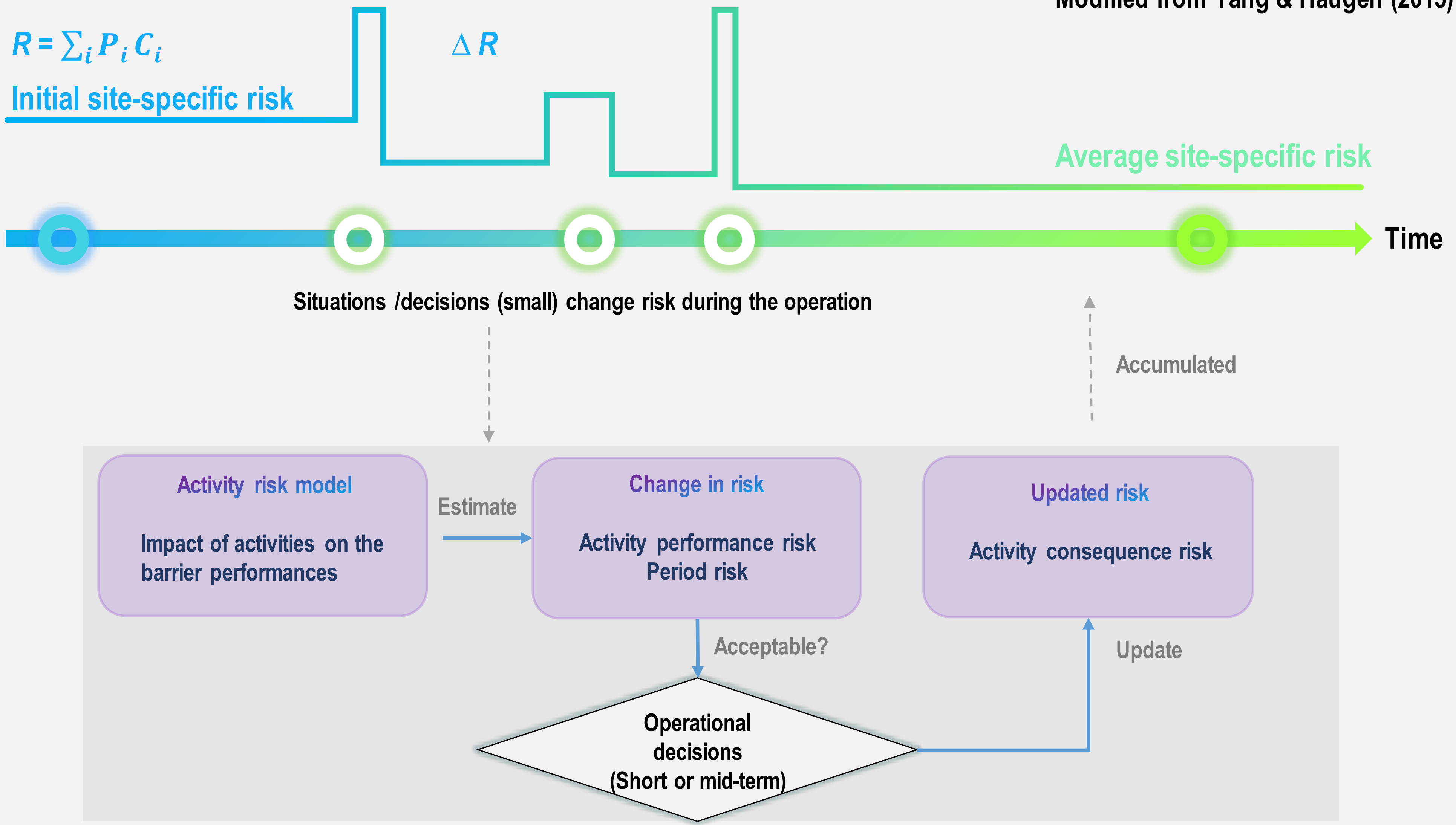
Operational risk analyses

(Vatn & Haugen, 2013)

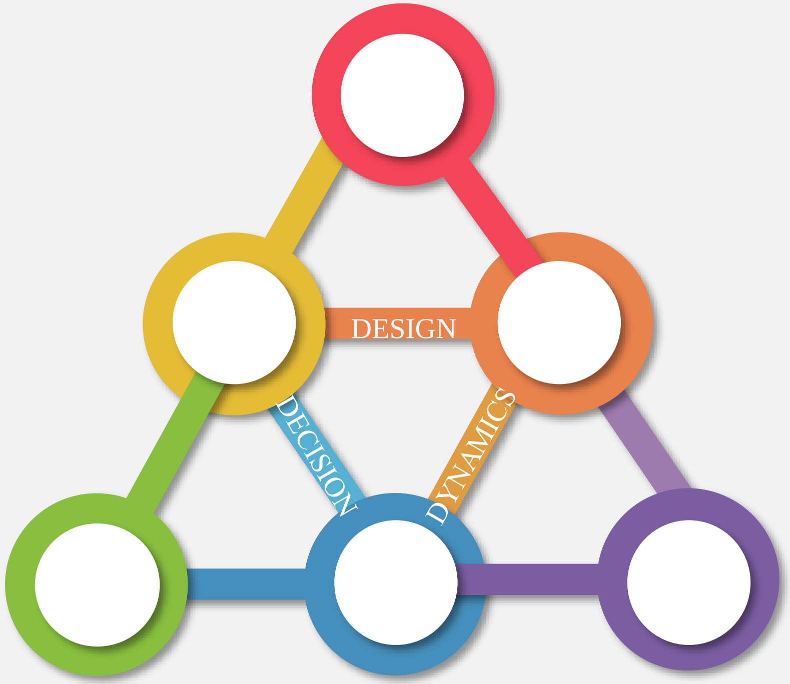
- Different from strategic risks analysis for strategic decisions
- An example of strategic risks analysis : Quantitative Risk Analysis (QRA) for safe design and procedure (risk level for the entire installation)
- QRA is not effective for operational decisions (more specific)
- An operational risk analysis is performed in limited problem area, typically decisions during planning (e.g. replace a detector)

Point of departure

Modified from Yang & Haugen (2015)



Objectives



One way to improve

- Detailed scenario analysis, make use of available information
- The need for sufficient focus on assumptions of an event scenario and a model that describes sequences of events (Aven, 2016)

Main interests

- Visualize detail event scenarios (sequence) that might be missed in quantitative risk anlysis
- Dependencies between decisions/activities and barrier failures
- Address potentials of such approach to support operational decisions

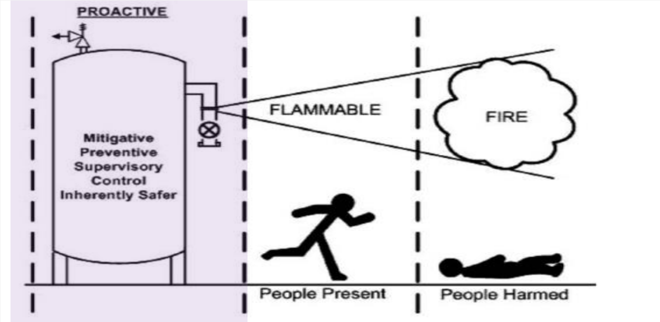
Case study

Tank overfill accidents

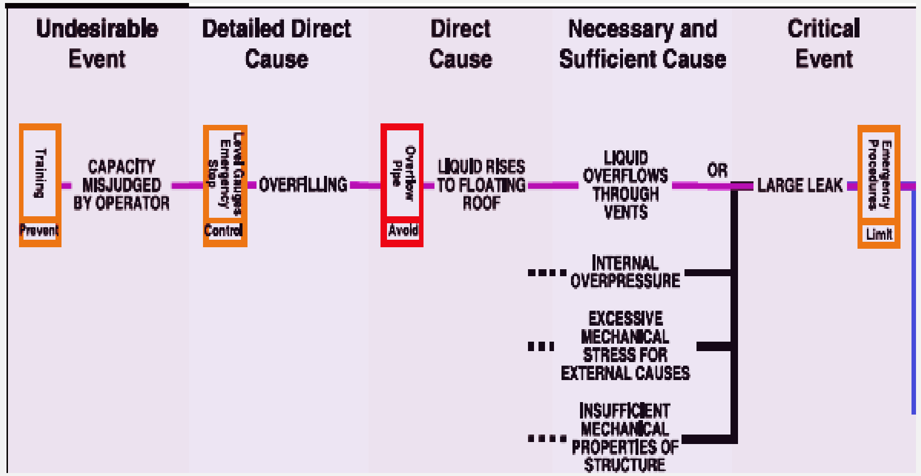
- Tank operations are similar around the world, and accidents are reoccurring (Myers & Roos, 2015).
- The overfill of atmospheric storage tanks is a common event, even with the systems for overfill prevention (Casey, 2016).
- After the Buncefield (2005), emphasis put on the use of risk analysis in design and operation

Safety Barriers

Bow-tie
Hazardous event :major spill from overfill

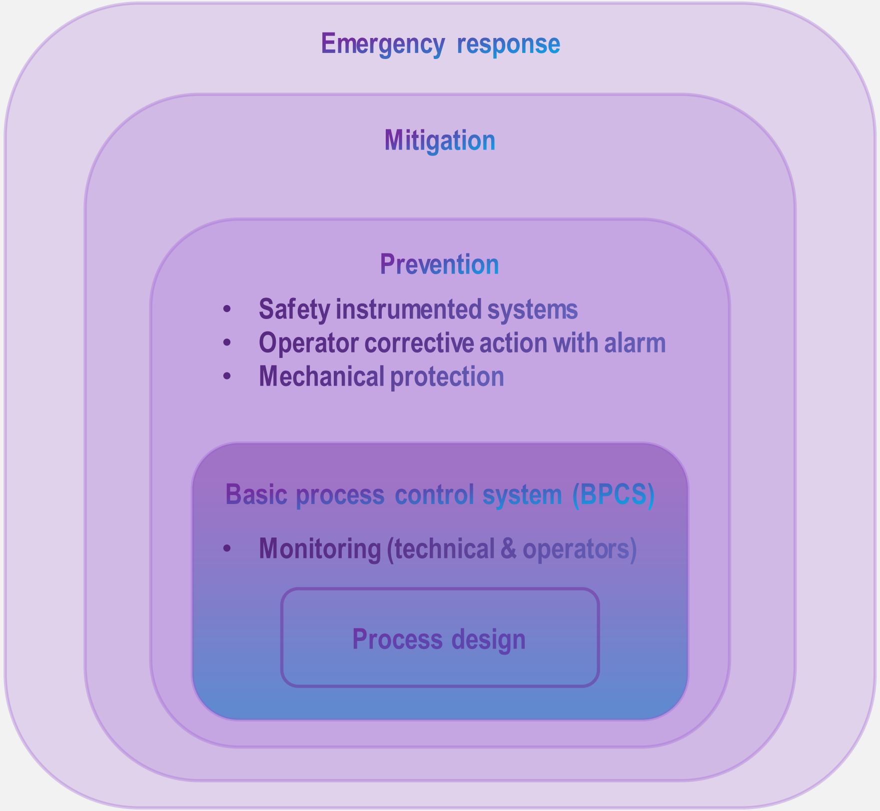


summers et al. (2012)



Left-hand side of bowtie of Buncefield case (Paltrinet al. ,2012)

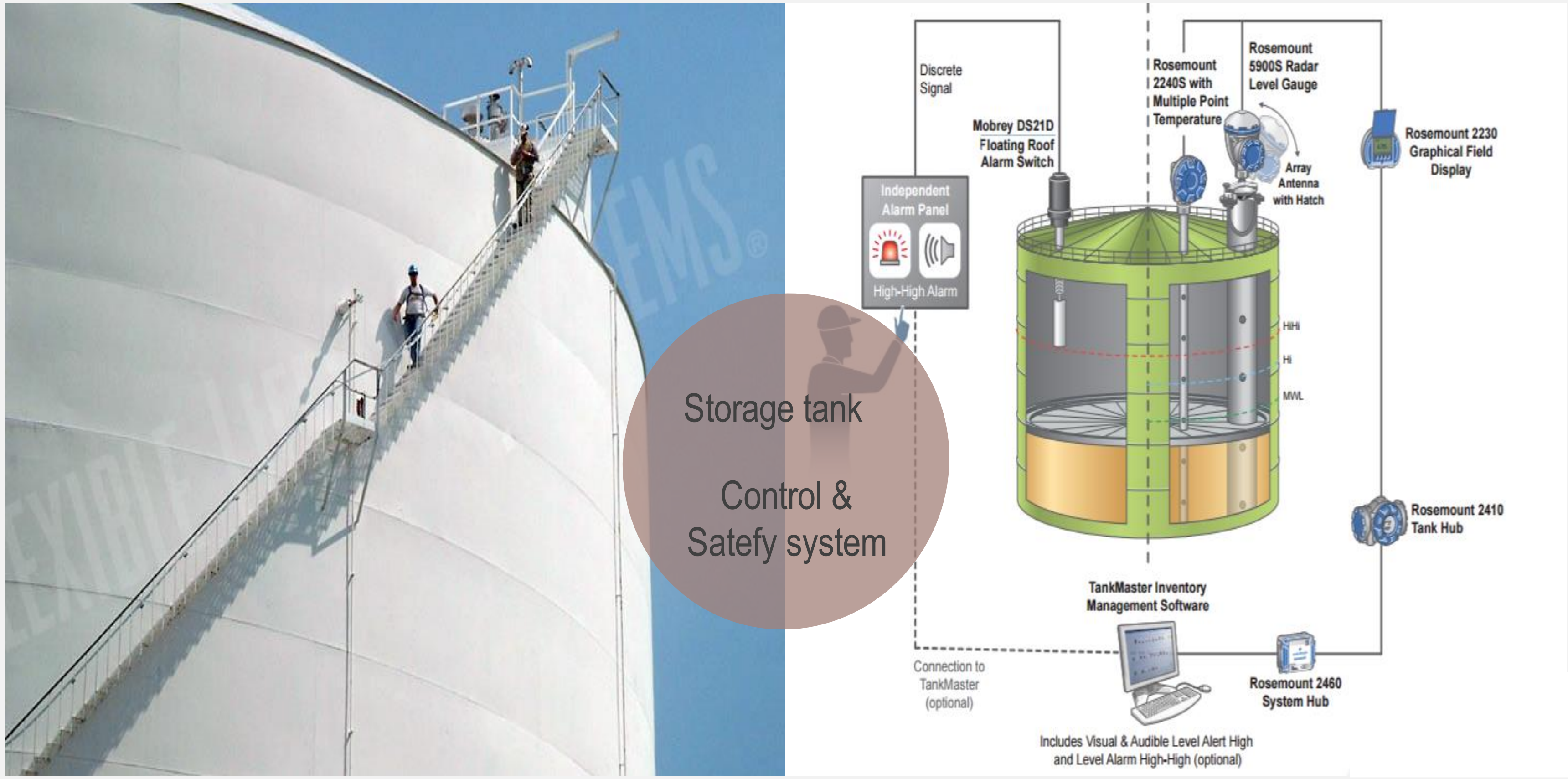
Layers of protection analysis (LOPA)



IEC 61511 (2012)

Introduction
System description
Modelling
Summary
Questions

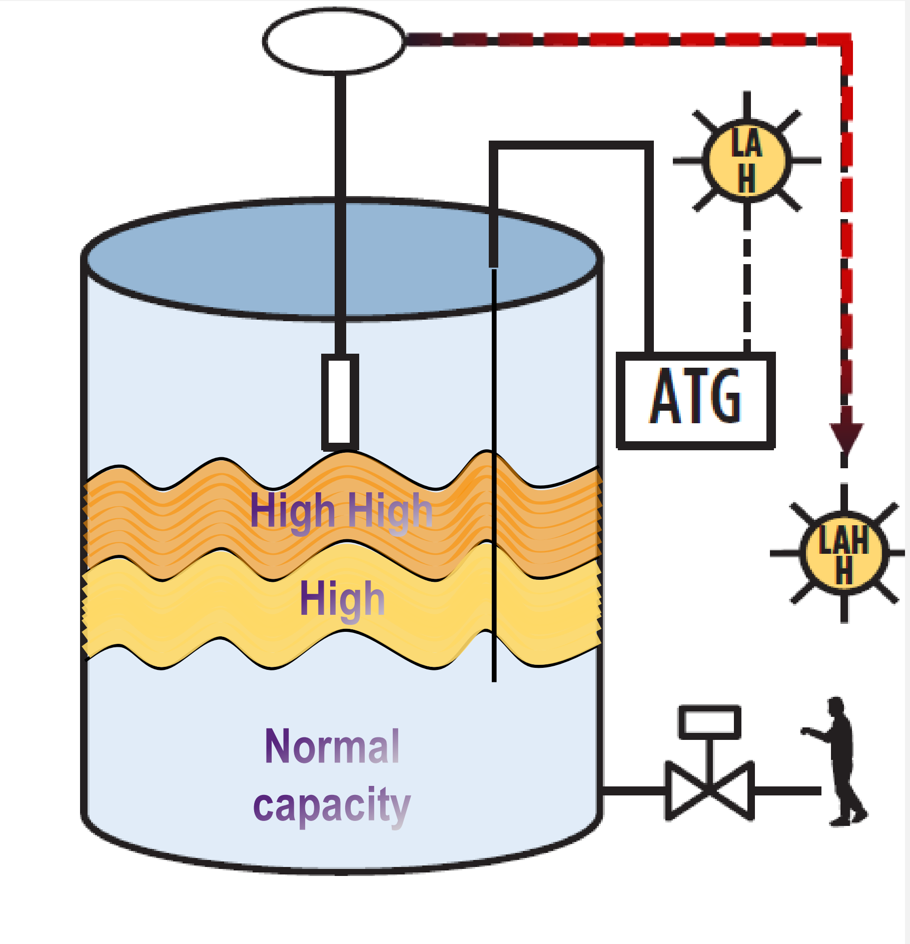
Safety instrumented system



Myers & Roos (2015)

"Many tank overfill incidents resulted from faulty instrumentation. In addition, it is common that operators did not believe the correct alarms because of past experience"

Safety instrumented system



Automatic gauging system (ATG)

- Tank levels may be read using ATG with ability to transmit a signal and/or trigger H alarm
- ATG failure - loss of information on the levels

→ H alarm is dependent on ATG

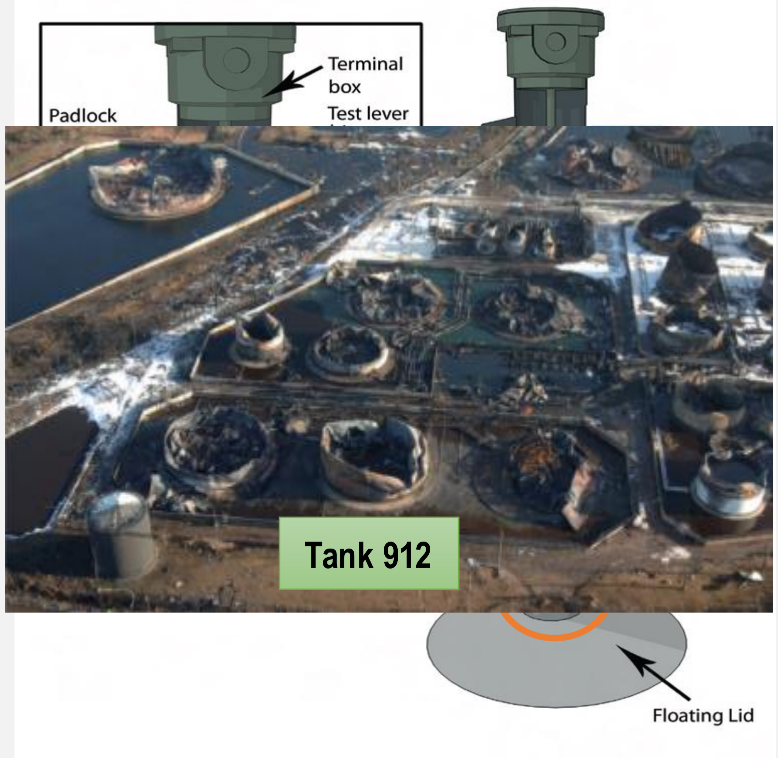
Level switch

- Independent from ATG
- Triggers H-H alarm or close the shutdown valve

Shutdown valve

- Manual intervention by local and/ or remote operator or automated shutdown

Case study



High-level switch

Buncefield (2005)

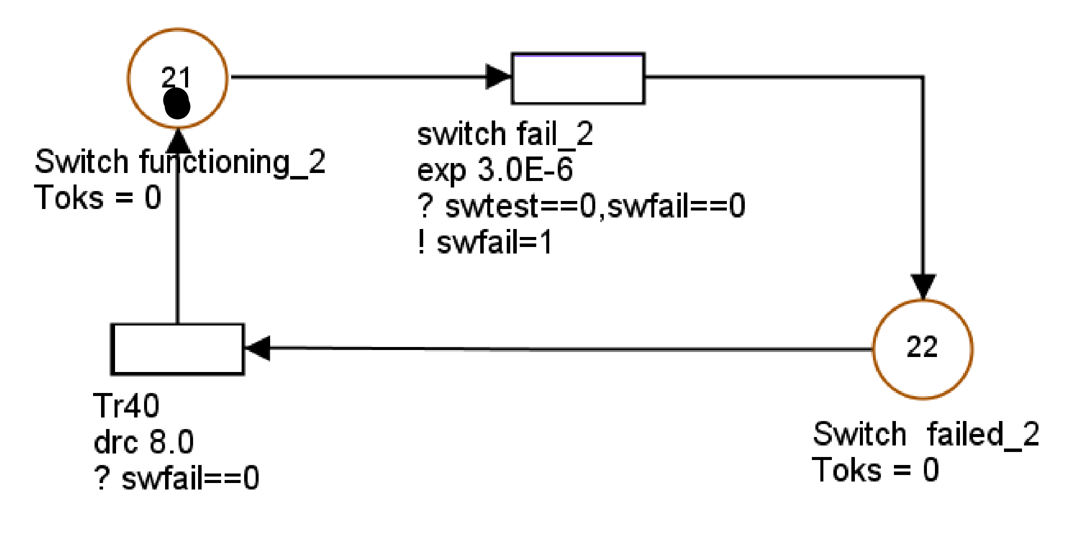
Technical barriers

- The level gauge remained the same position
  → no alarms
- High-level switch did not close the shutdown valve

Operational barriers

- No actions to repair the level gauge:
  The same problem occured 14 times in 4 months.
- The maintenance crews did not fit the padlock after testing.
- Poor communication between two companies (Designer / maintenance)

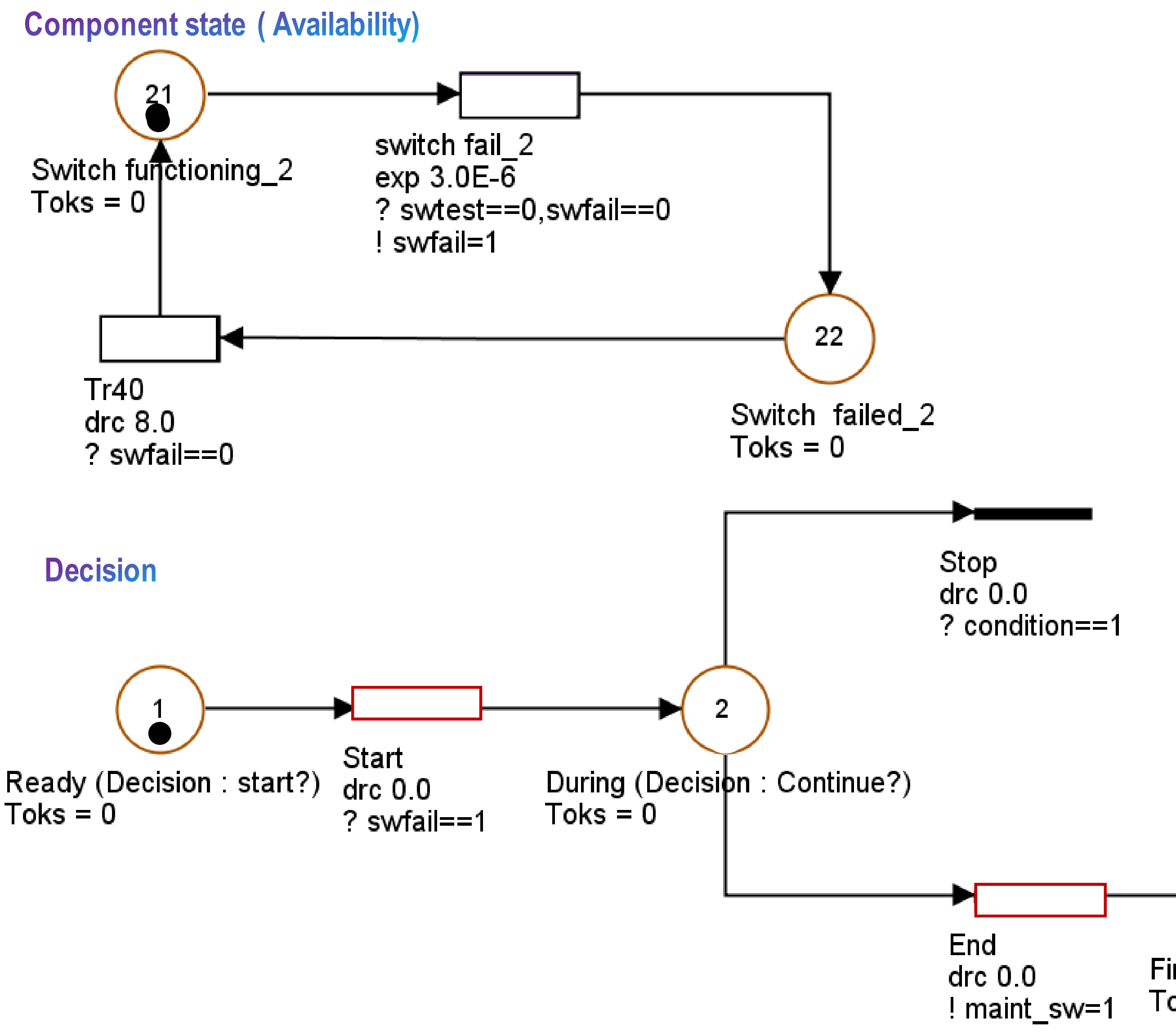
Modelling



Petri nets

- Dynamic behavior of the system in a particular state (Not limited to binary events)
- Express dependencies : support fault tree or event tree analysis
- Compact, flexible and easy to use
- Monte Carlo Simulations gives approximate value

Petri Net with marking



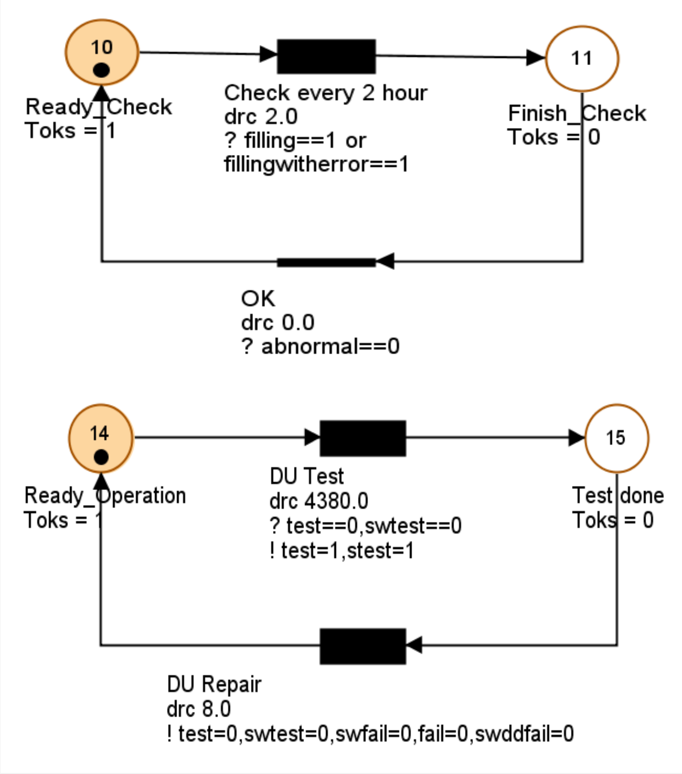
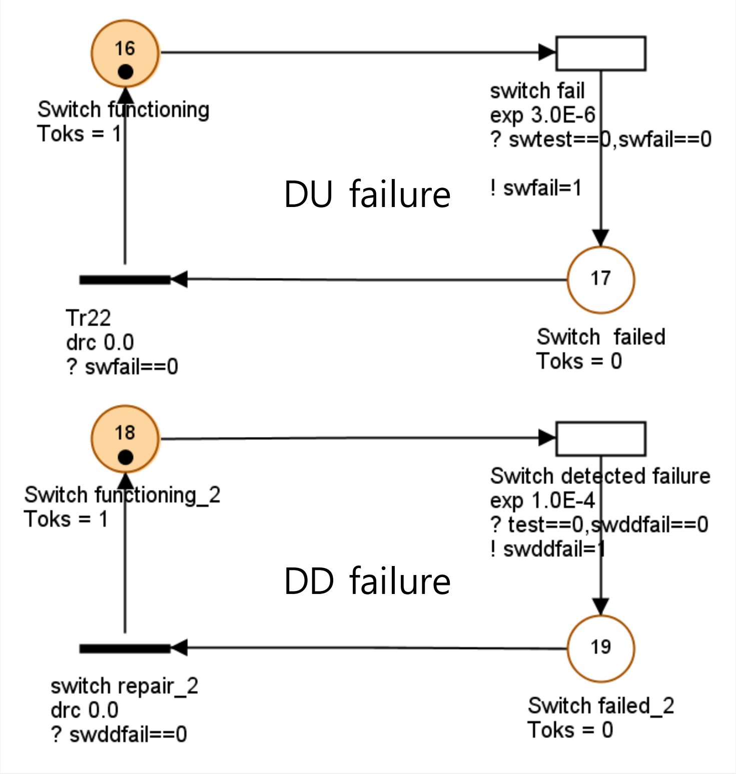
Elements of Marked Petri Nets

- Place with Token(s)
- Transitions
- Arc
- Predicate, assertions

'Petri Net is static network but a token is dynamic (Rausand, 2011)'

Modelling

Event/activity influence barriers

Maintenance/operation	Technical barrier
	

Introduction
System description
Modelling
Summary
Questions

Modelling

States of the storage tank

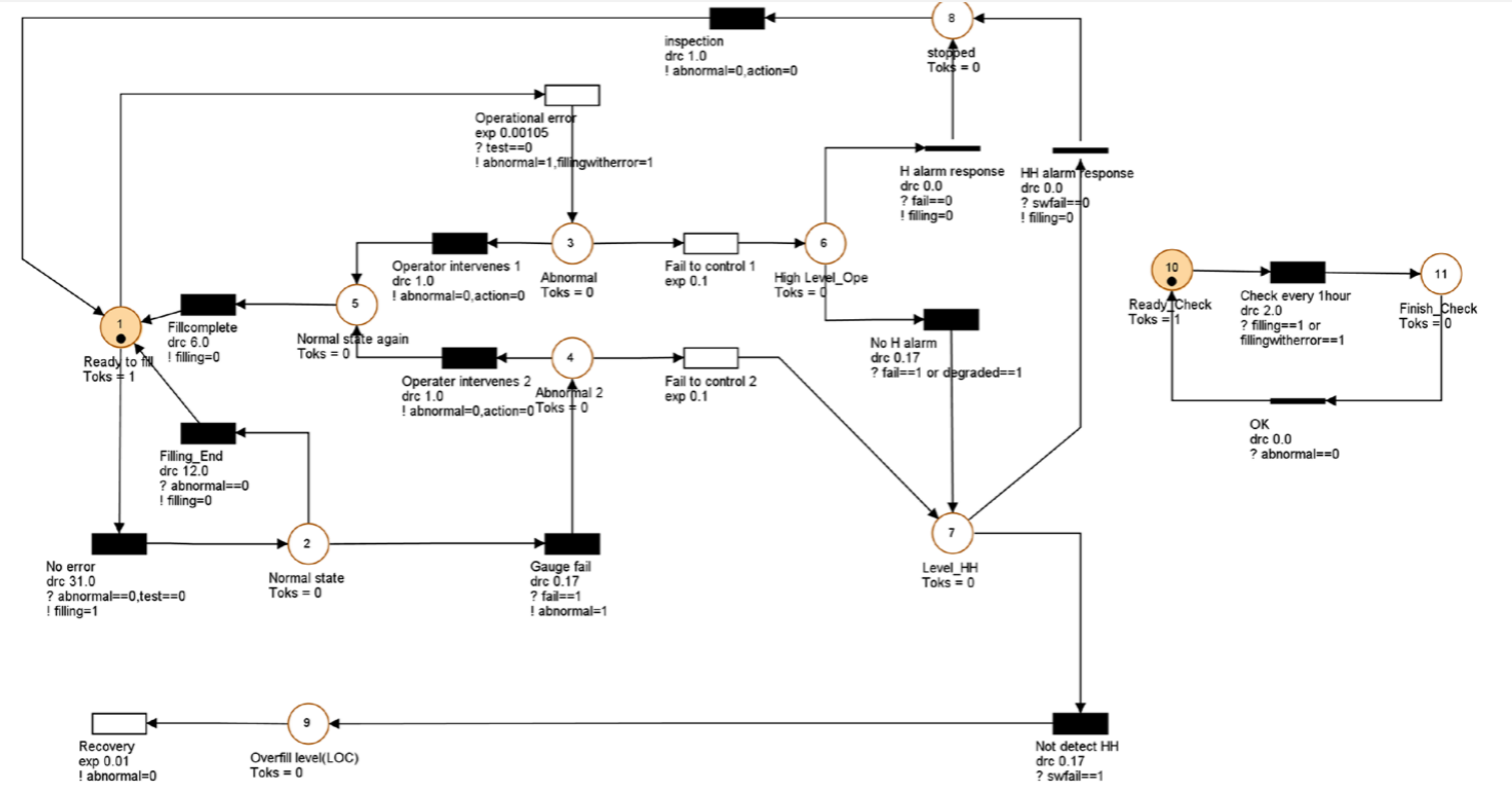


Figure 5 The petri net modelling of the tank filling level

- Introduction
- System
- **Modelling**
- Summary
- Questions

Simulation result

What and when are the events triggered during 3 months?

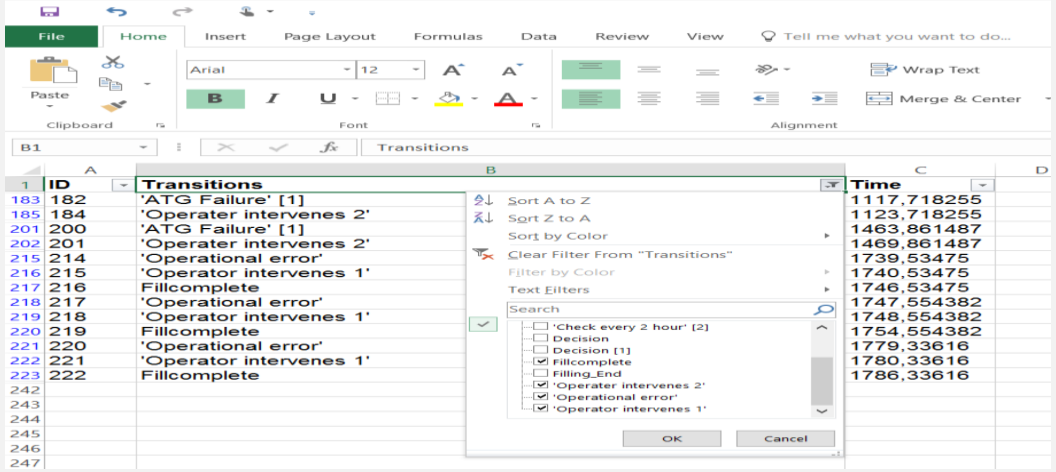
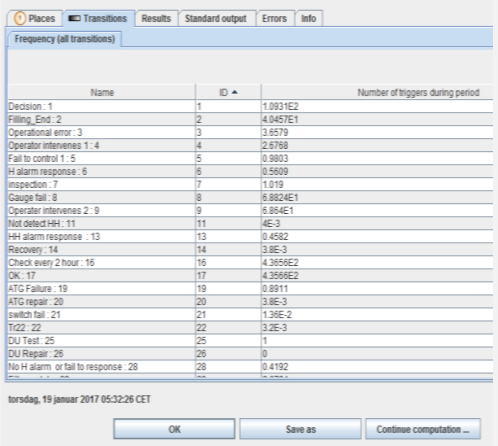


Figure 1

- What are probabilities of each state?



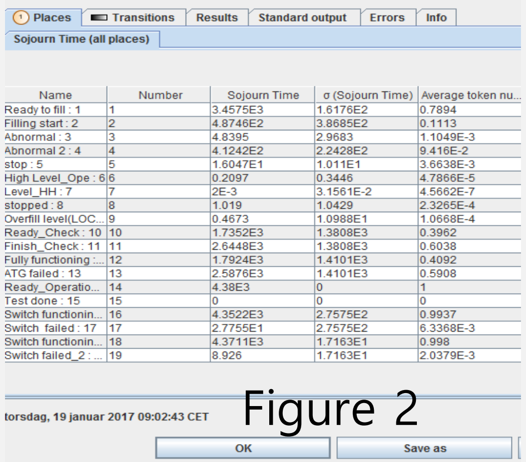
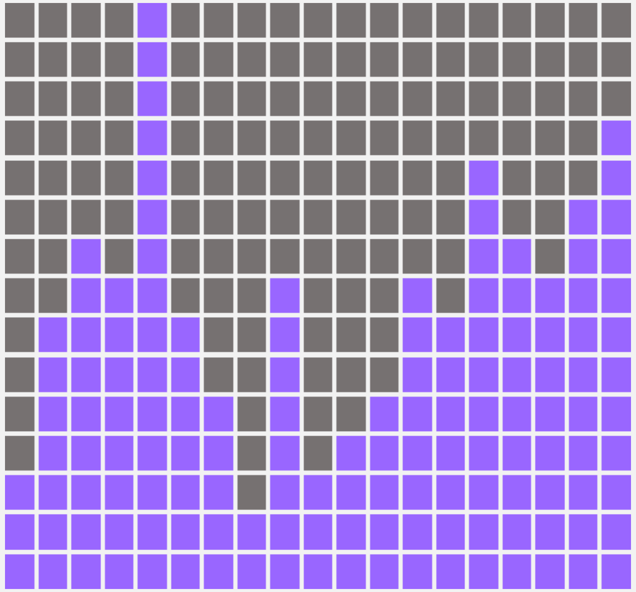


Figure 2

Provide a piece of information for decision support

Data

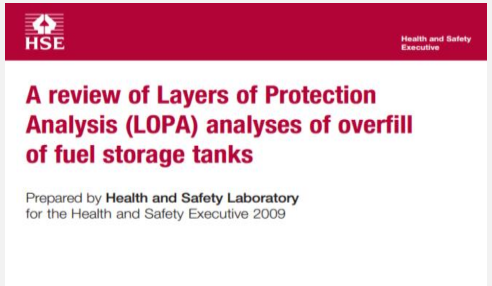


Operational barrier	Technical barrier
Generic values Operator error probability • Response time	•Tank filling frequency •Failure rate of components •Demand rate

Table F.4 – Typical protection layer (prevention and mitigation) PFDs

Protection layer	PFD
Control loop	$1,0 \times 10^{-1}$
Human performance (trained, no stress)	$1,0 \times 10^{-2}$ to $1,0 \times 10^{-4}$
Human performance (under stress)	0,5 to 1,0
Operator response to alarms	$1,0 \times 10^{-1}$
Vessel pressure rating above maximum challenge from internal and external pressure sources	10^{-4} or better, if vessel integrity is maintained (that is, corrosion is understood, inspections and maintenance is performed on schedule)

IEC 61511 (2012)

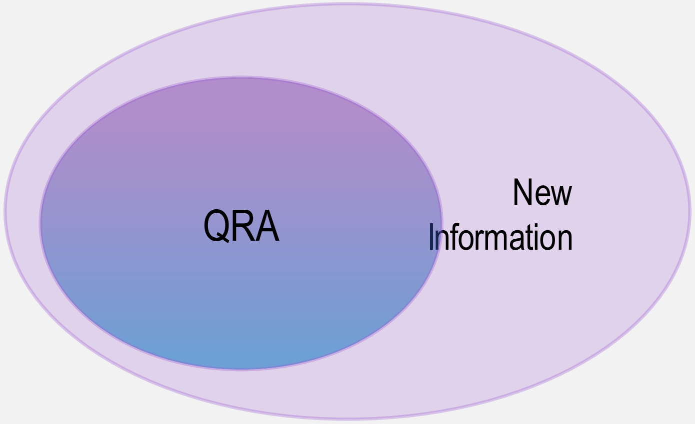

HSE
Health and Safety Executive
A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks
Prepared by Health and Safety Laboratory for the Health and Safety Executive 2009

Chambers et al., (2009), COMAH (2011)

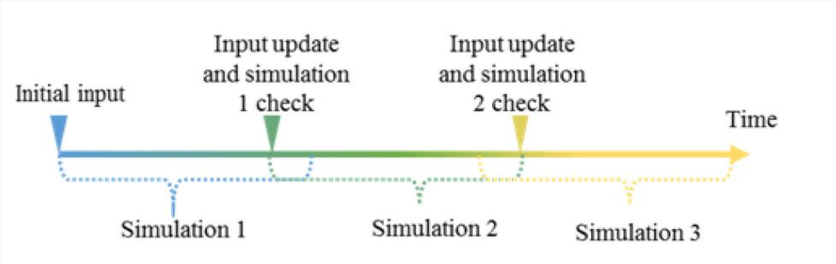
Summary

- The purpose of a risk analysis is not to address each and every possible chain of events. (Factors that influence are more focused)
- However, we try to pay attention to sequence of events sets that are considered to be safety-critical
- Select a specific path in a bow tie
- Illustrate how to use Petri nets to model the states of components or operators
- Visualize assumptions behind the events

Changes in risk over time



Summary and conclusion



Decision support

- **Support understanding of operational situations**
- Modify the elements of Petri net based on work orders, maintenance activities, work permits
- **Practical value : when we have identified possible event sets, the model gives a realistic probability value to avoid unnecessary precaution measures**

Summary and conclusion

Limitations and potential improvements

Limitations	Improvements
• Requires good understanding of both technical systems and operational situations • Weak links to the severe accident • Does not embrace risk influencing factors • Big Petri nets are not good in communication	• Include risk influencing factors by using Bayes rule to update the parameter in a stochastic distribution (e.g. failure rates)

Questions

Thank you ☺