Dynamic versus static modelling of safety-critical systems for risk assessment

Markert, Frank; Kozine, Igor

Publication date:
2015

Document Version
Peer reviewed version

Link back to DTU Orbit

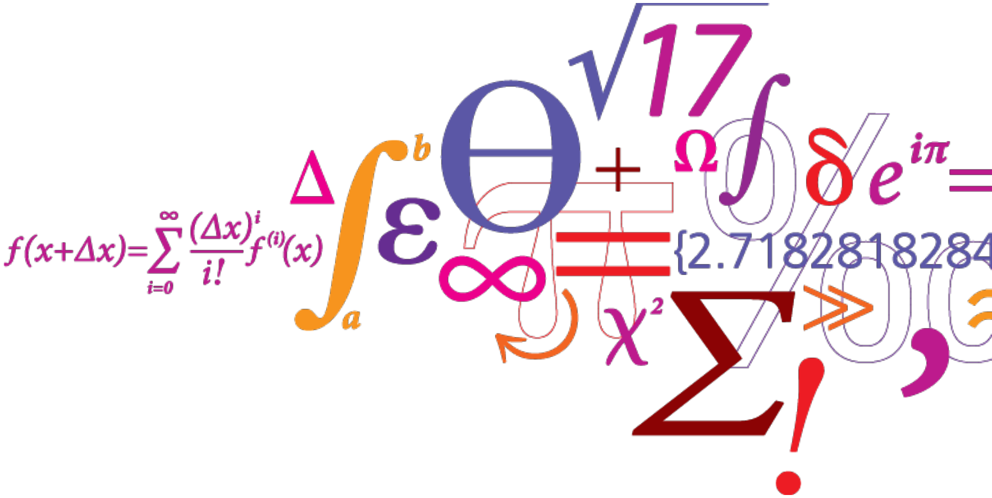
Citation (APA):
Markert, F. (Author), & Kozine, I. (Author). (2015). Dynamic versus static modelling of safety-critical systems for risk assessment. Sound/Visual production (digital)

Dynamic versus static modelling of safety-critical systems for risk assessment

Frank Markert
fram@dtu.dk

Igor Kozine
igko@dtu.dk

Produktionstorvet byg. 424
2800 Kongens Lyngby
Danmark



DTU Management Engineering
Department of Management Engineering

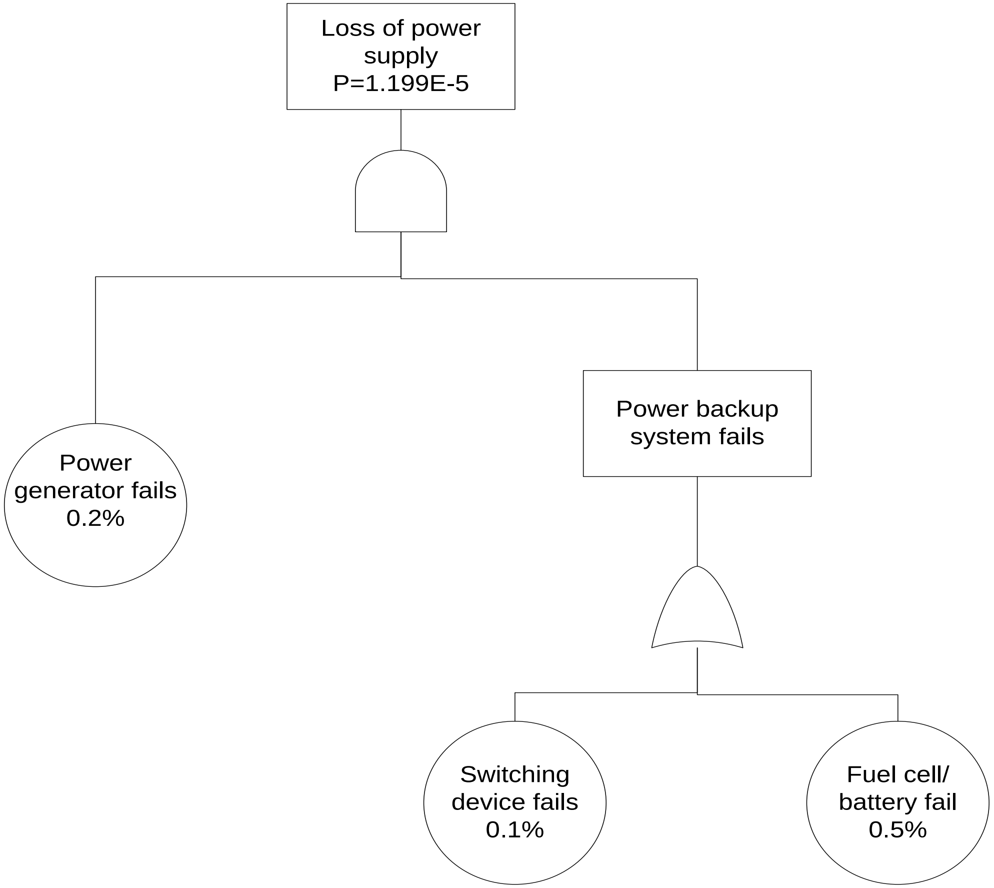
Content

- Modelling approaches of safety – critical systems
- Advantages of dynamic modelling using a discrete event simulation environment
- Overview and examples of the projects that have used this approach to derive risk and reliability assessments.
- Conclusion

Modelling approach practised in risk analysis

Example power backup system

- **Fault tree**



Loss of power supply P=1.199E-5

Power generator fails 0.2%

Power backup system fails

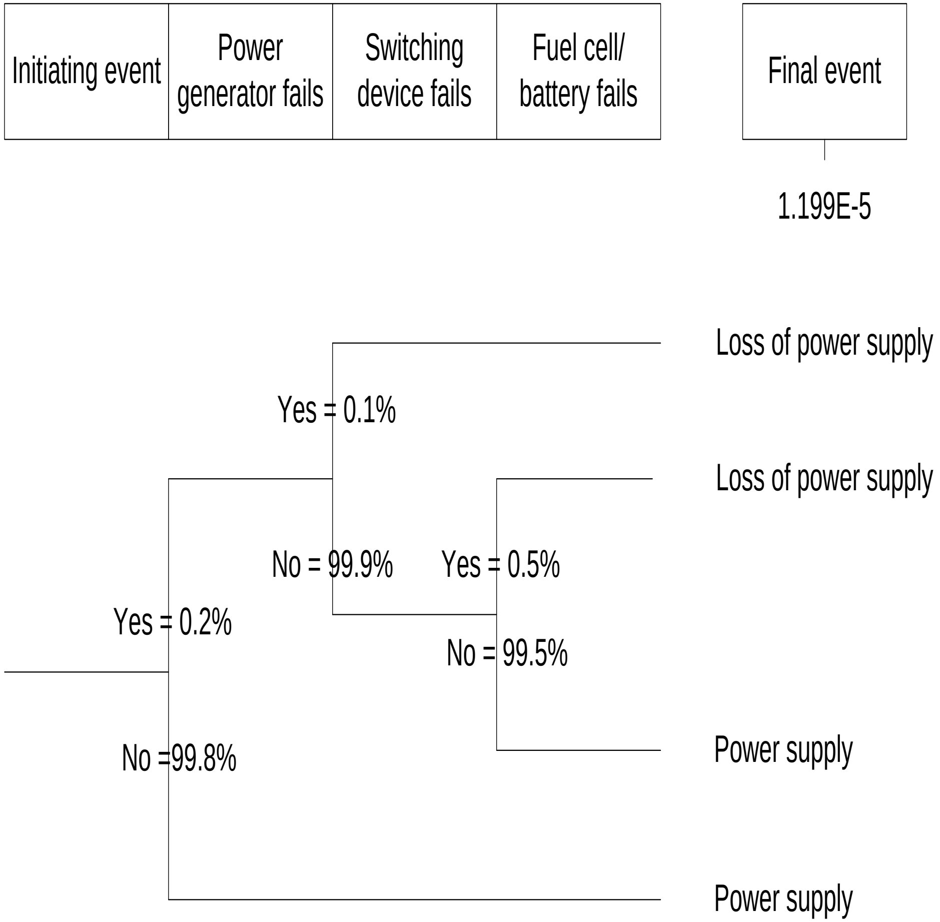
Switching device fails 0.1%

Fuel cell/ battery fail 0.5%

Modelling approach practised in risk analysis

- Fault tree
- **Event tree**

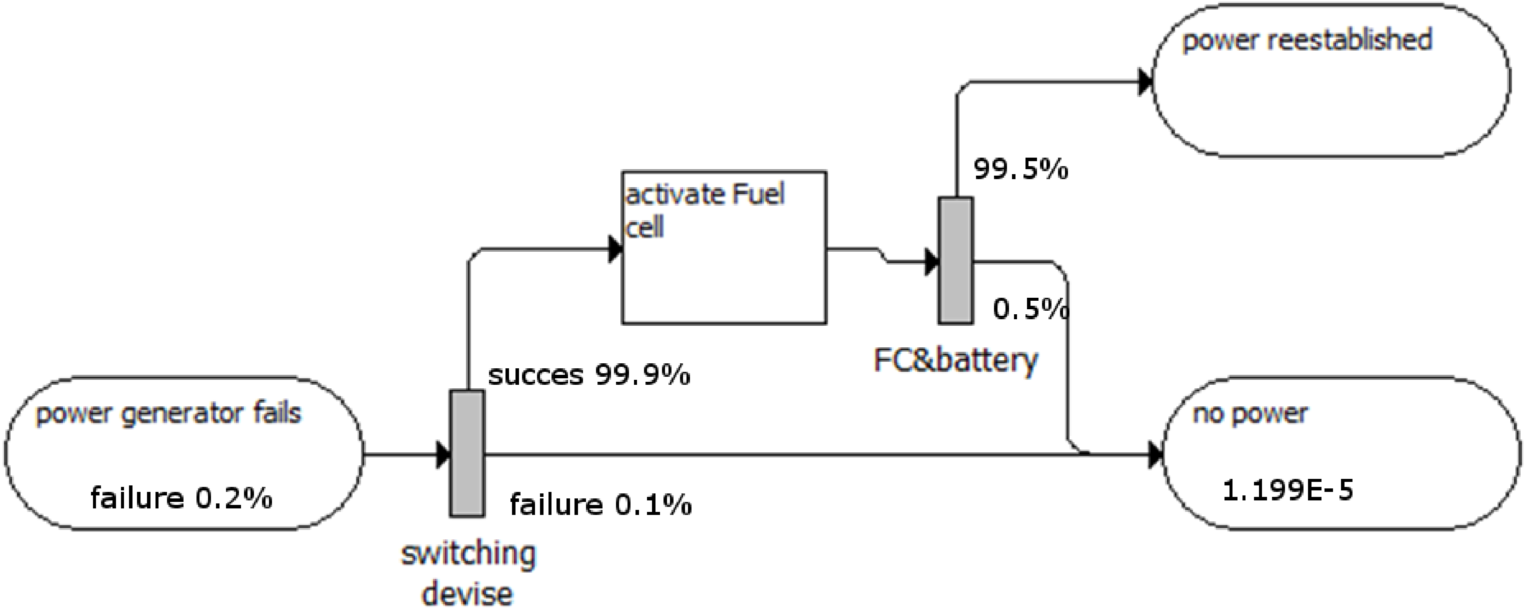
Example power backup system



Modelling approach practised in risk analysis

Example power backup system

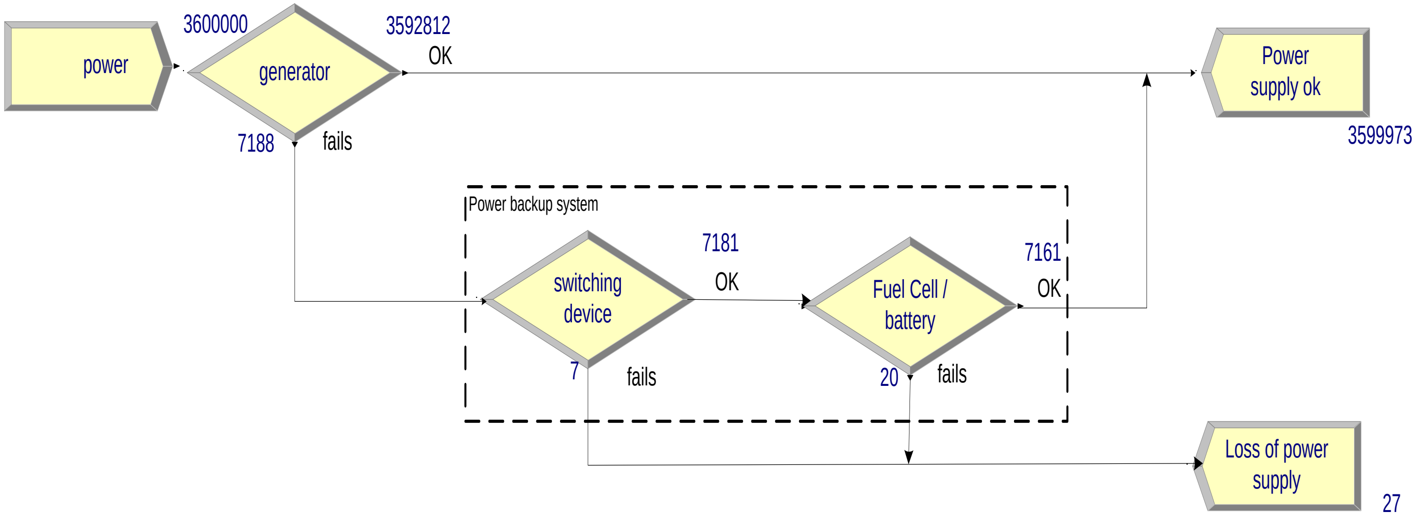
- Fault tree
- Event tree
- **Barrier diagram**



Modelling approach practised in risk analysis

Example power backup system

- Fault tree
- Event tree
- Barrier diagram
- **Dynamic using Discrete Event Simulation** (DES, Arena® vers. 14.50.0)



Point of departure in accident modelling

Consider a natural gas pipeline rupture and the prediction of the consecutive failure of supply to a customer:

P(Supply failure) = P(Supply failure | Pipeline rupture) x P(Pipeline rupture)

- <u>Rupture event easily predicted </u>by e.g. Fault tree
- the <u>consecutive supply failure is not easily predicted </u>by FT, as function includes:
  - Amount of gas (pressure) in the pipeline segment downstream,
  - Number of customers
  - Hourly gas consumption as a function of seasonal and production variations.

Approach of our choice: Discrete Event Simulation

1. Models mimick/imitate procecesses and events
2. No highly abstract theories
3. Domain experts understand models and influence their development
4. Animation and graphical scenarios contribute to understanding and confidence
5. Individual (hazardous) scenarios can be played back
6. Easy integration of the technical part and human performance

DES models for risk analysis

Easy account for dynamic stochastic dimensions in systems

1. Models are dynamic (vs. static conventional models)
2. Data are sampled statistically (Monte Carlo approach),
   - e.g. hole size, wind speed, release direction, number of persons working, seasonal – daily changes
   - Loss of partial performance and its degradation in time´
   - Dynamic demand (e.g. gas supply): seasonal - daily changes
3. Condition dependent down times
4. Gradual recovery after a failure, etc.
5. Multiple runs (many!) are performed to extract risk numbers for assessing Individual Risk, Potential Loss of Life, Group Risk)
   - **Simulation runs are more time consuming**

Reference projects

1. OPHRA –Offshore Platform Hydrocarbon Risk Analysis. *Financed by Dong Energy*

2. Simulation of human performance in time-pressured scenarios (Case: Performance of operators in a control room of a NPP under MLOCA scenario). *Performed under the Halden Reactor Project*

3. Reliability of a gas supply. *Financed by Swedegas, owner and operator the gas pipeline Dragør, DK – Gutherborg, SV*

4. Safe manning of merchant ships. *Financed by the Danish Maritime Fond*

5. Train driver performance modelling (developing engineering models for usability studies). *The Halden Project*

6. *Operational risk of assets for a Water Utility Company, Master project supported by Københavns Energi and Reliasset A/S*

7. Risk analysis of a generic hydrogen refuelling station. *Master project*

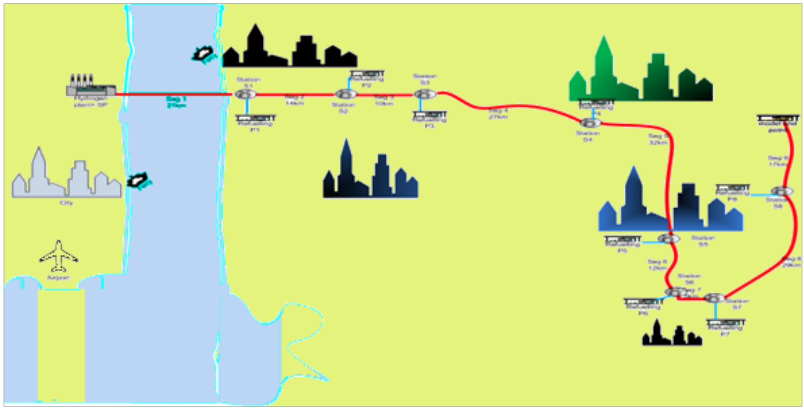
8. Optimizing the rating of offshore and onshore transformers for an offshore wind farm. Master project supported by DONG

THE HYDROGEN SUPPLY SYSTEM

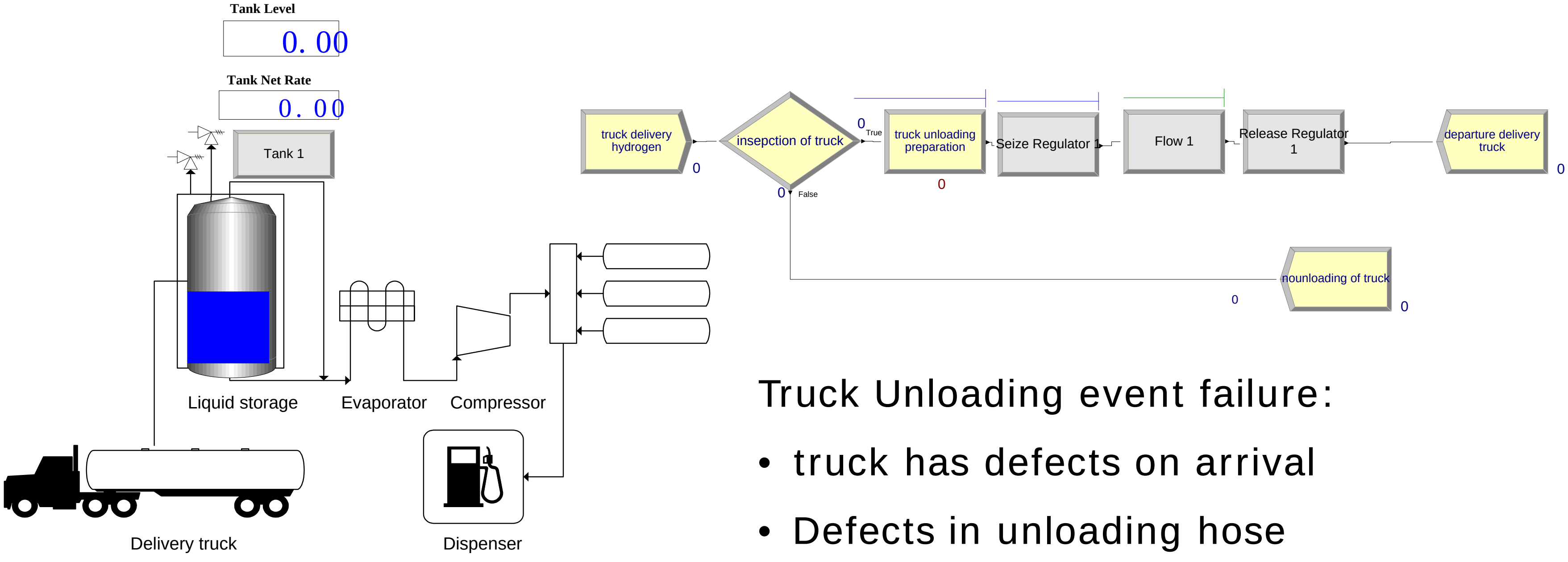
The network consists of a number of stations, the production is decentral and supply is by pipeline or truck delivery.

Goal: Uninterrupted Hydrogen delivery has to be achieved in all cases, while a minimum of hydrogen is stored on-site to reduce the risk potential

- A Hydrogen refuelling station:
  - Hydrogen supply by pipeline or road tanker
  - Storage facilities (main tank, compressor and buffer storage)
  - Dispensers to refuel car and busses
  - Cash desk

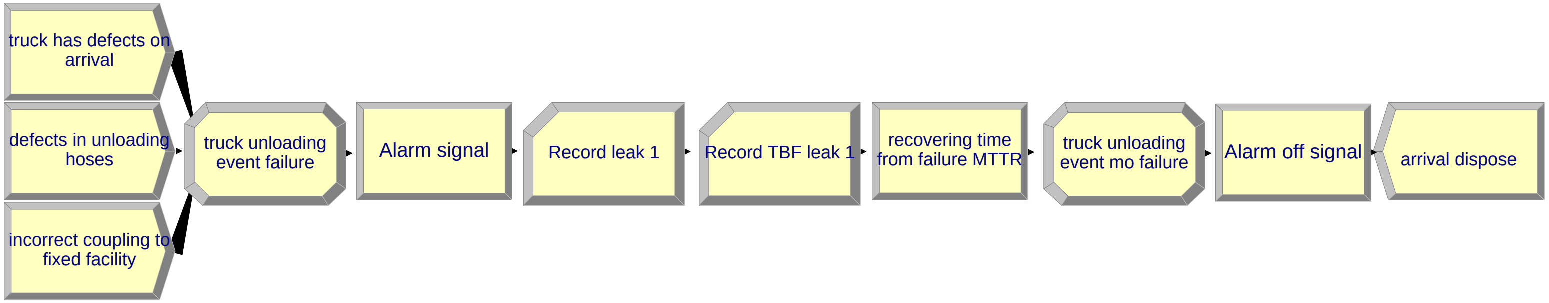


Example: Modelling of truck unloading



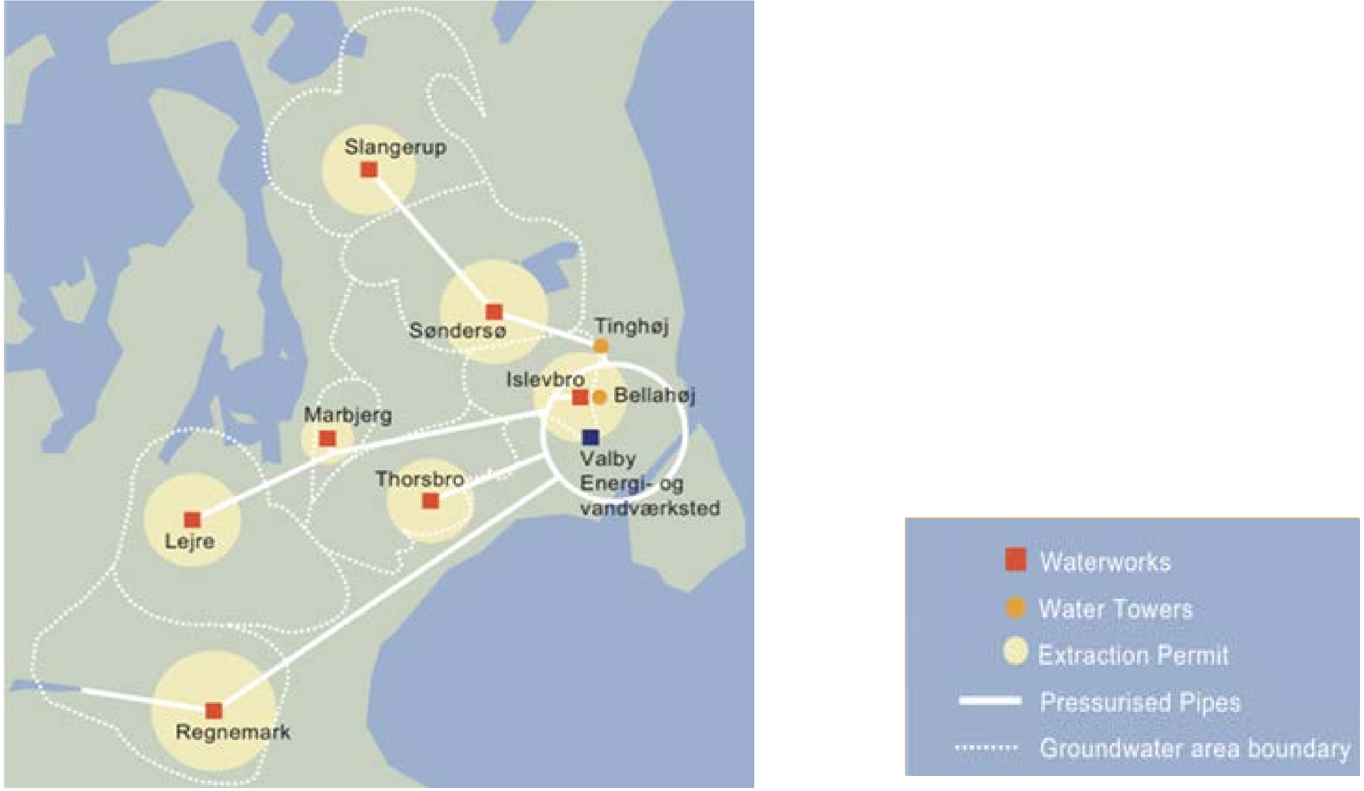
Truck Unloading event failure:

- truck has defects on arrival
- Defects in unloading hose
- Incorrect coupling


truck has defects on arrival
defects in unloading hoses
incorrect coupling to fixed facility
truck unloading event failure
Alarm signal
Record leak 1
Record TBF leak 1
recovering time from failure MTTR
truck unloading event mo failure
Alarm off signal
arrival dispose

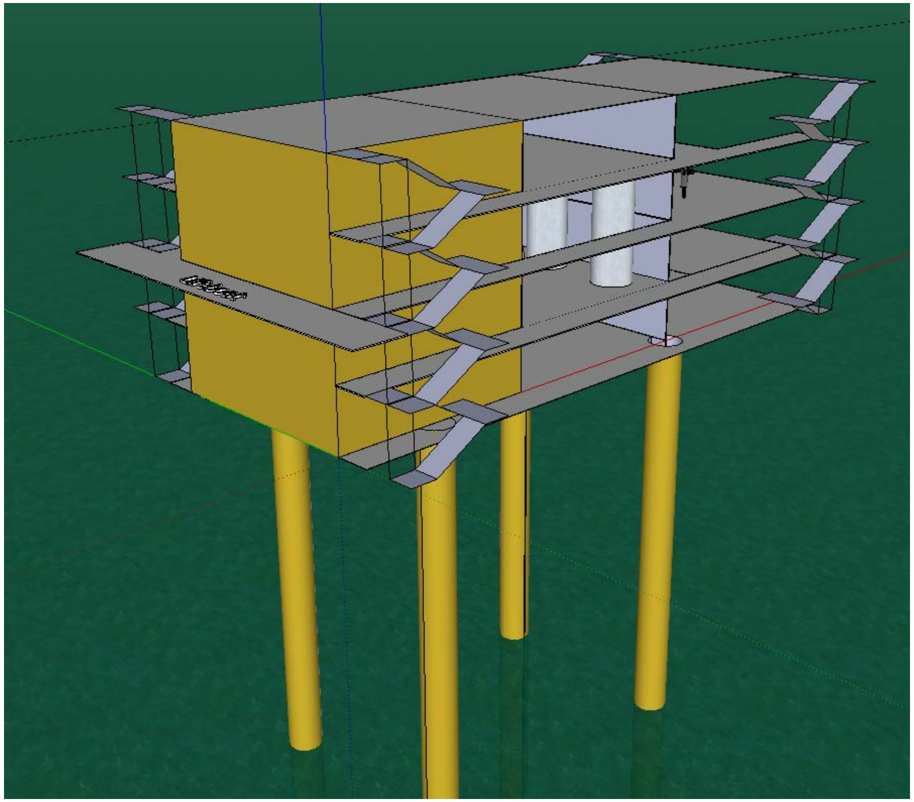
Arena® software version 14.50.00

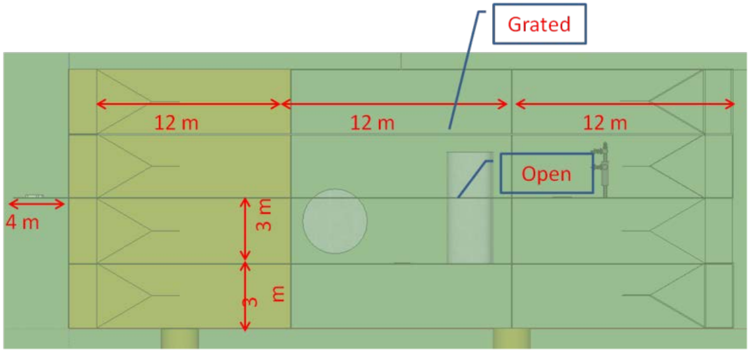
The water supply system in the area around Copenhagen

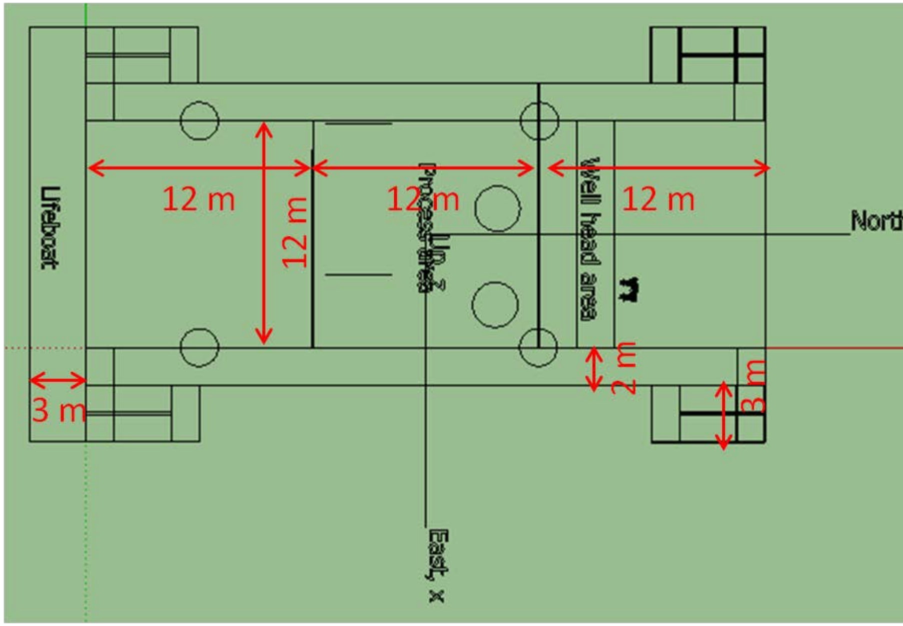


OPHRA - Feasibility study supported by DONG energy

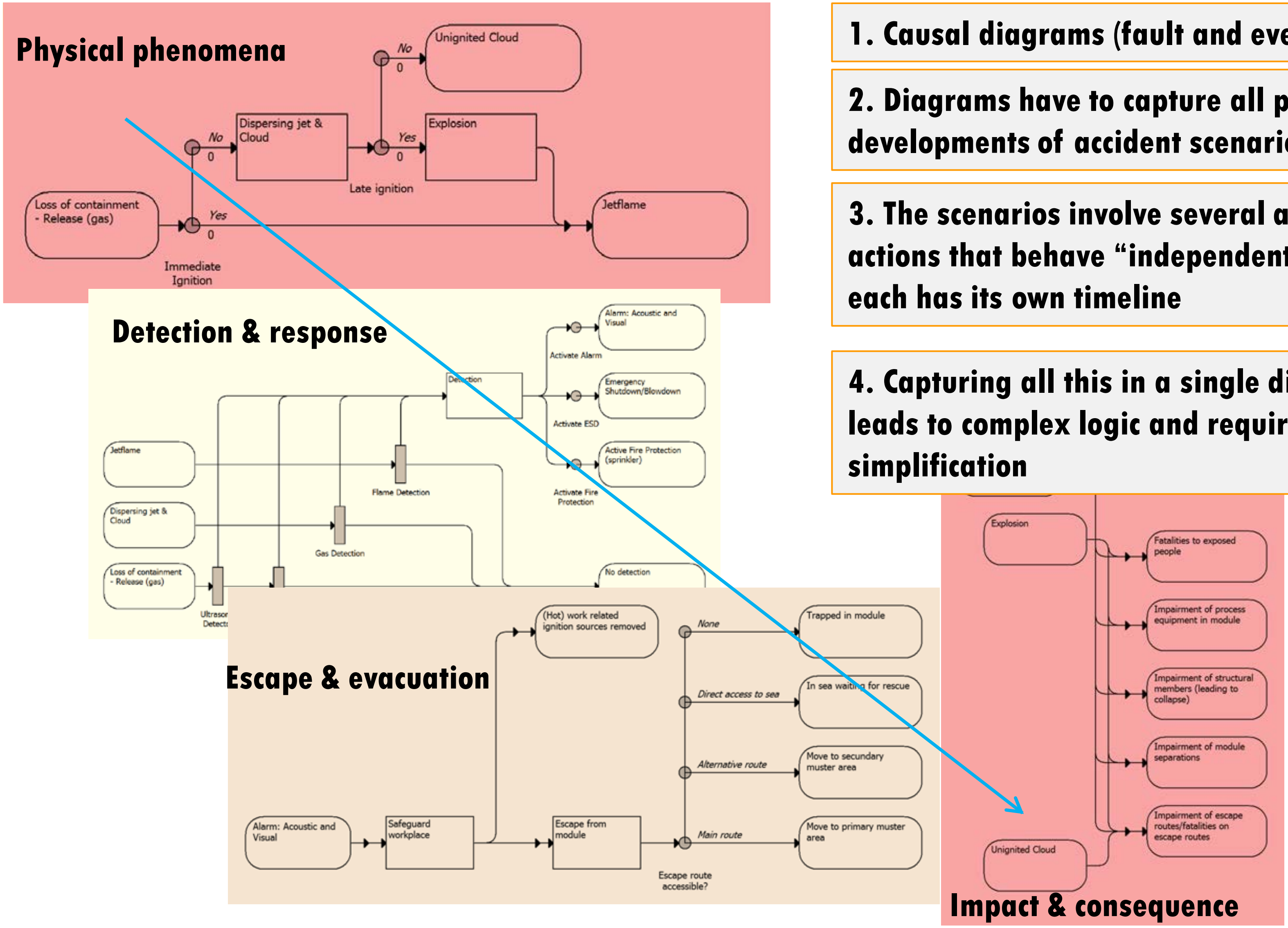
- Only releases in center of process area
- Only gas releases







Conventional approach


Physical phenomena
Unignited Cloud
No
0
Dispersing jet & Cloud
No
0
Yes
0
Explosion
Late ignition
Loss of containment - Release (gas)
Yes
0
Jetflame
Immediate Ignition
Detection & response
Alarm: Acoustic and Visual
Activate Alarm
Detection
Emergency Shutdown/Blowdown
Activate ESD
Jetflame
Active Fire Protection (sprinkler)
Flame Detection
Activate Fire Protection
Dispersing jet & Cloud
Gas Detection
Loss of containment - Release (gas)
No detection
Ultrasonic Detection
Escape & evacuation
(Hot) work related ignition sources removed
None
Trapped in module
Direct access to sea
In sea waiting for rescue
Alternative route
Move to secundary muster area
Alarm: Acoustic and Visual
Safeguard workplace
Escape from module
Main route
Move to primary muster area
Escape route accessible?
Explosion
Fatalities to exposed people
Impairment of process equipment in module
Impairment of structural members (leading to collapse)
Impairment of module separations
Impairment of escape routes/fatalities on escape routes
Unignited Cloud
Impact & consequence

1. Causal diagrams (fault and event trees)

2. Diagrams have to capture all possible developments of accident scenarios

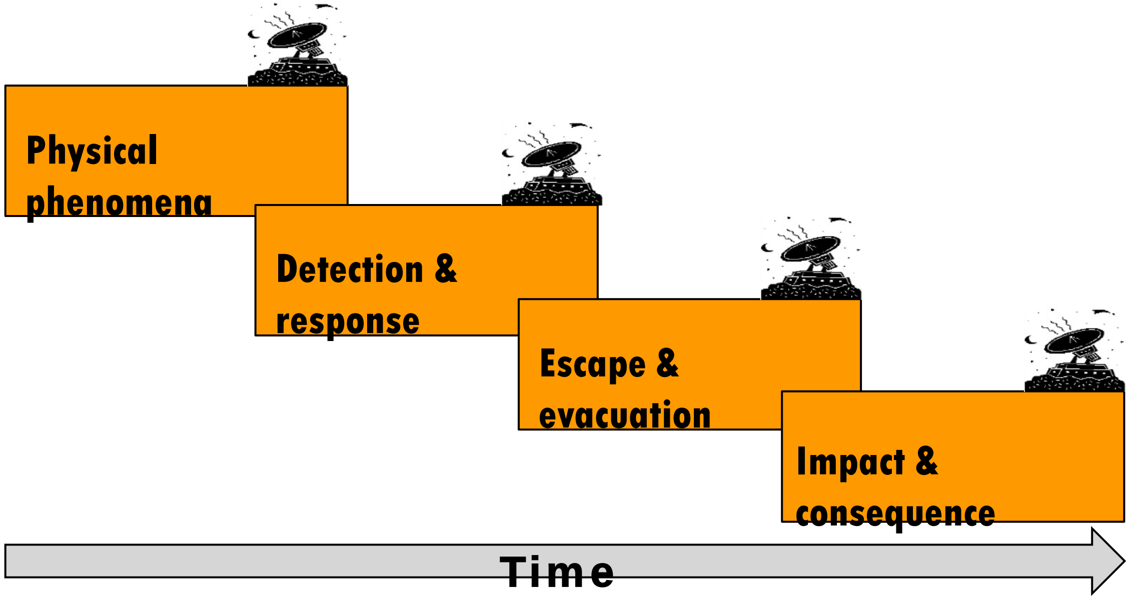
3. The scenarios involve several agents and actions that behave “independently” and each has its own timeline

4. Capturing all this in a single diagram leads to complex logic and requires simplification

Application of dynamic & dependent models

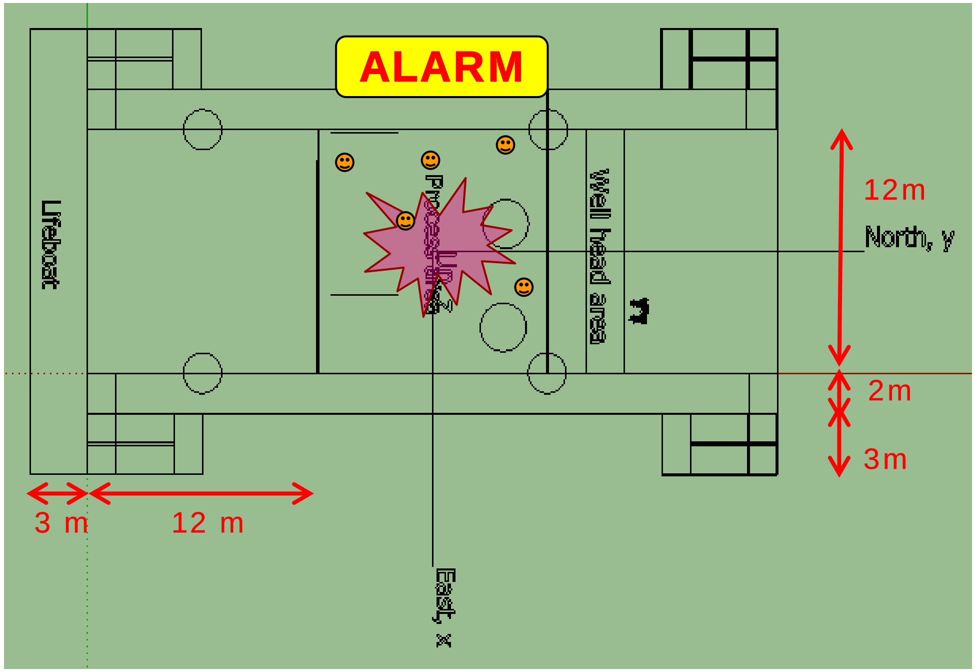
Alternative:

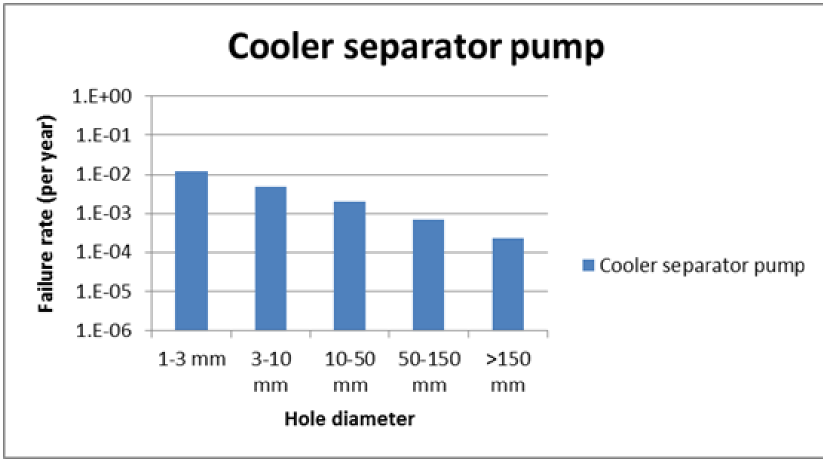
model each process separately but allow feed-back and interaction between processes

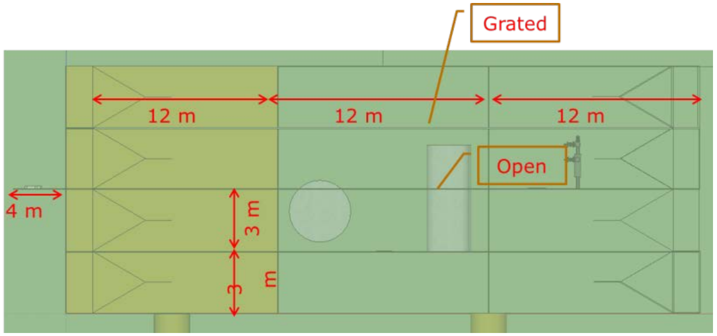


- The event sequences trigger each other and are simulated concurrently.
- Events taking place in one sequence change the conditions in the other sequences (dynamic interaction)

The off-shore platform

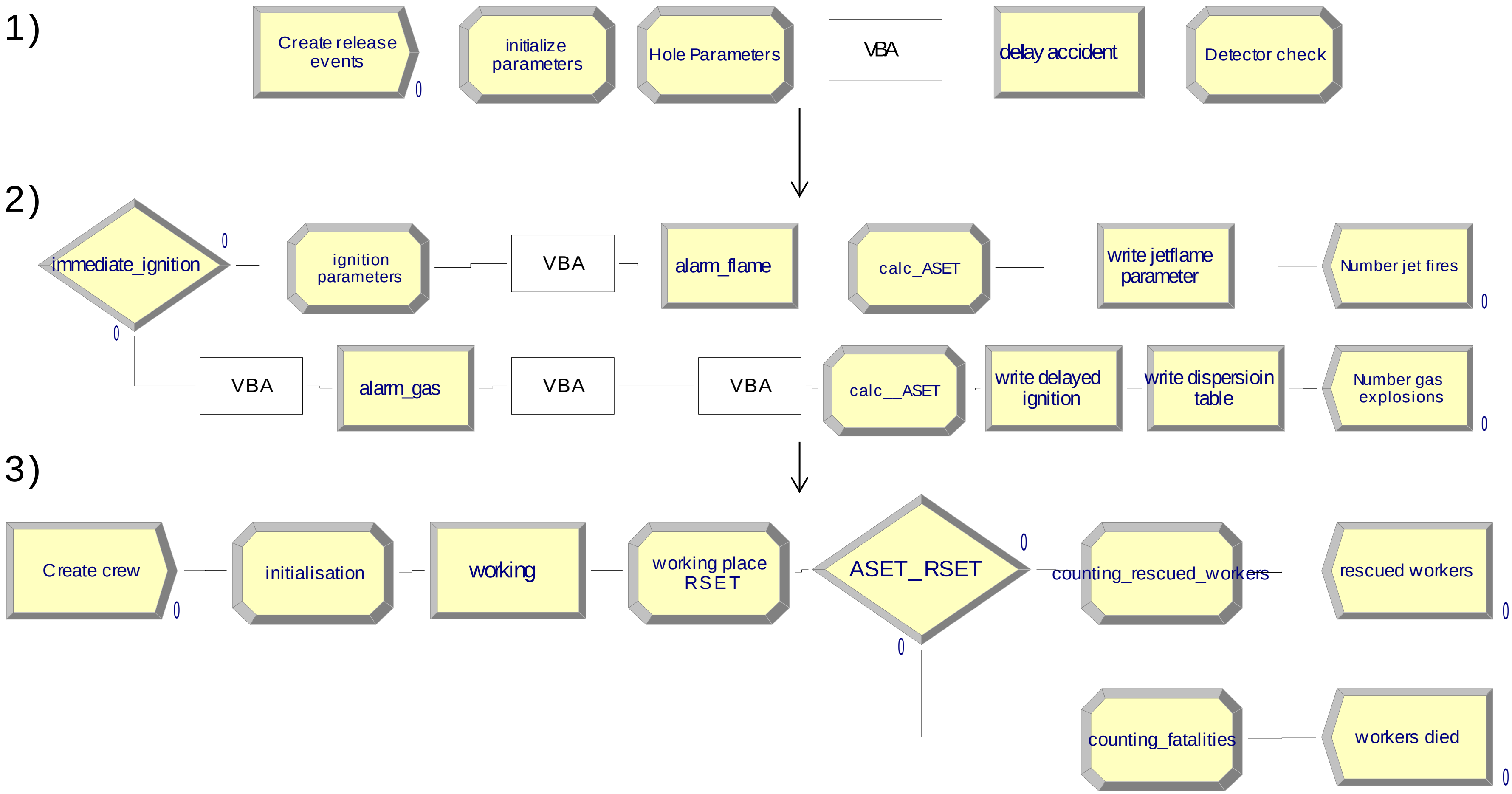






DES model logic

1) input parameters, 2) Consequences, 3) Evacuation



Arena® software version 14.50.00

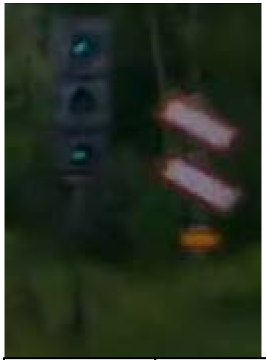
Example results:

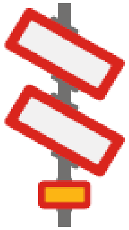
10000 simulation runs				
Input:	**average**	**st.dev.**	**min**	**max**
wind speed (m/s)	11	5	5	20
wind direction (degrees)	91	52	0	180
hole size statistic (mm)	12	28	1	200
No. workers at random positions	4		3	5
Output:				
wind speed in module (m/s)	0.6	0.3	0.1	1.4
mass flow (kg/s)	6.2	27.8	0.007	271.5
SEPmax jet flame (kW/s)	40	11	28	93
RSET (s)	240		176	301
ASET (s)	427		0	>600
No. fatilities per accident	1.3	1.8	0	5

A task network model of human activities for improving usability and safety

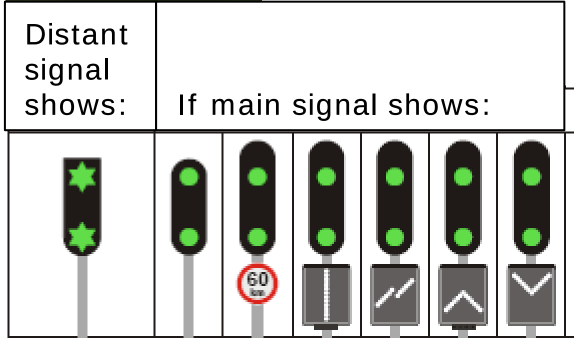
Domain: train driver

- Motivation: relatively high number of SPADS (Signals Passed At Danger) on Danish railways
- Relatively simple task (move train from station to station within the limits communicated to the train driver through track-side signals and signs)



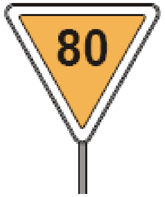


800m to station

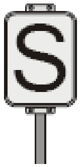


Distant signal shows:

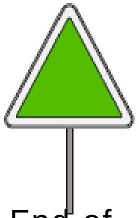
If main signal shows:



Expect speed limit



Stop before the mark



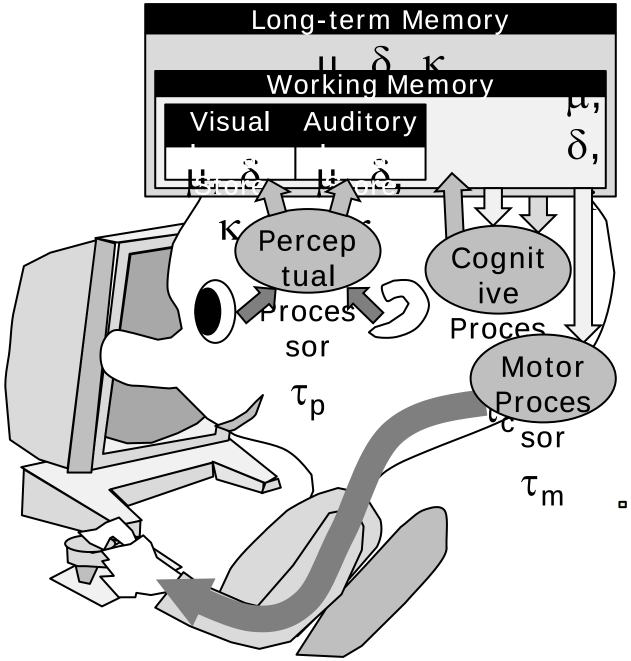
End of speed limit

Model concepts – 3 submodels

- **Movement of the train**: speed & position in response to position of controls (speed and brake). Includes generation of data on control panel (speedometer)

- **Environment:** side track objects, external visual objects and audio inputs, depending on the position of the train and other events

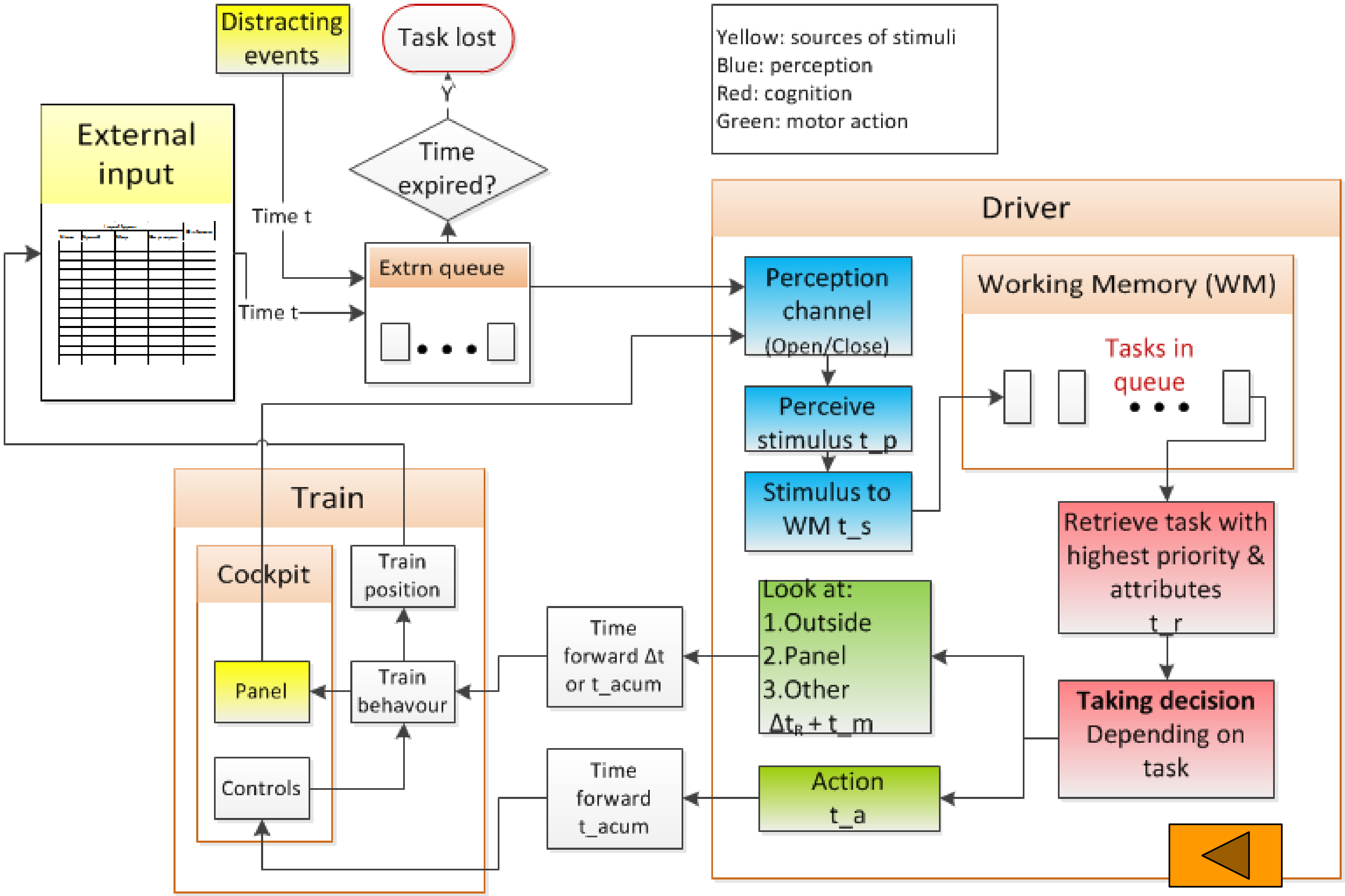
- A **cognitive model of a train driver**



Model Human Processor (Card et al.)

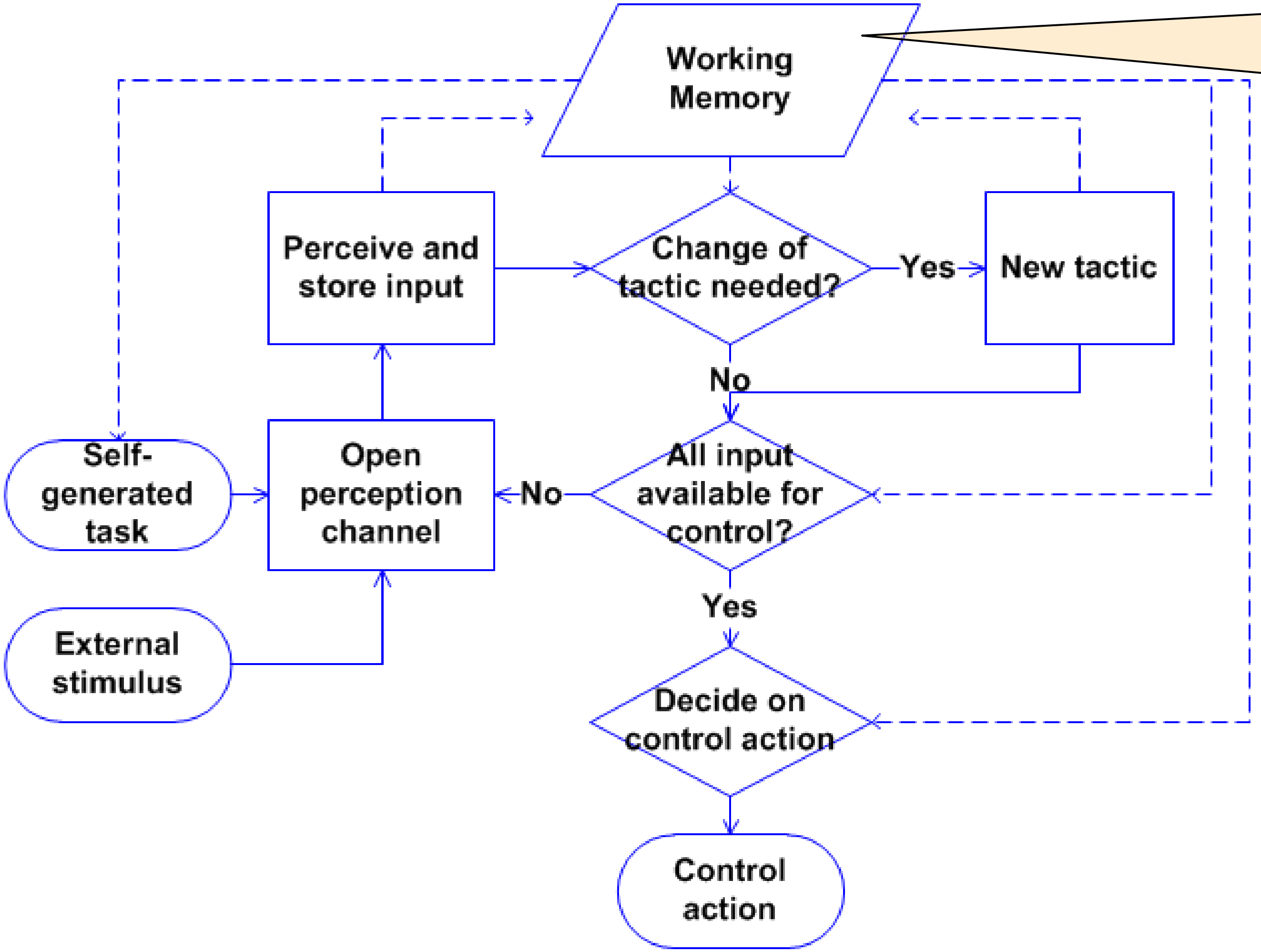
- μ: storage capacity (items, ”chunks”)
- δ: decay time of an item
- κ: main code type (physical, acoustic, visual, semantic)
- τ: cycle time

Model structure using DES with queues



Yellow: sources of stimuli
Blue: perception
Red: cognition
Green: motor action

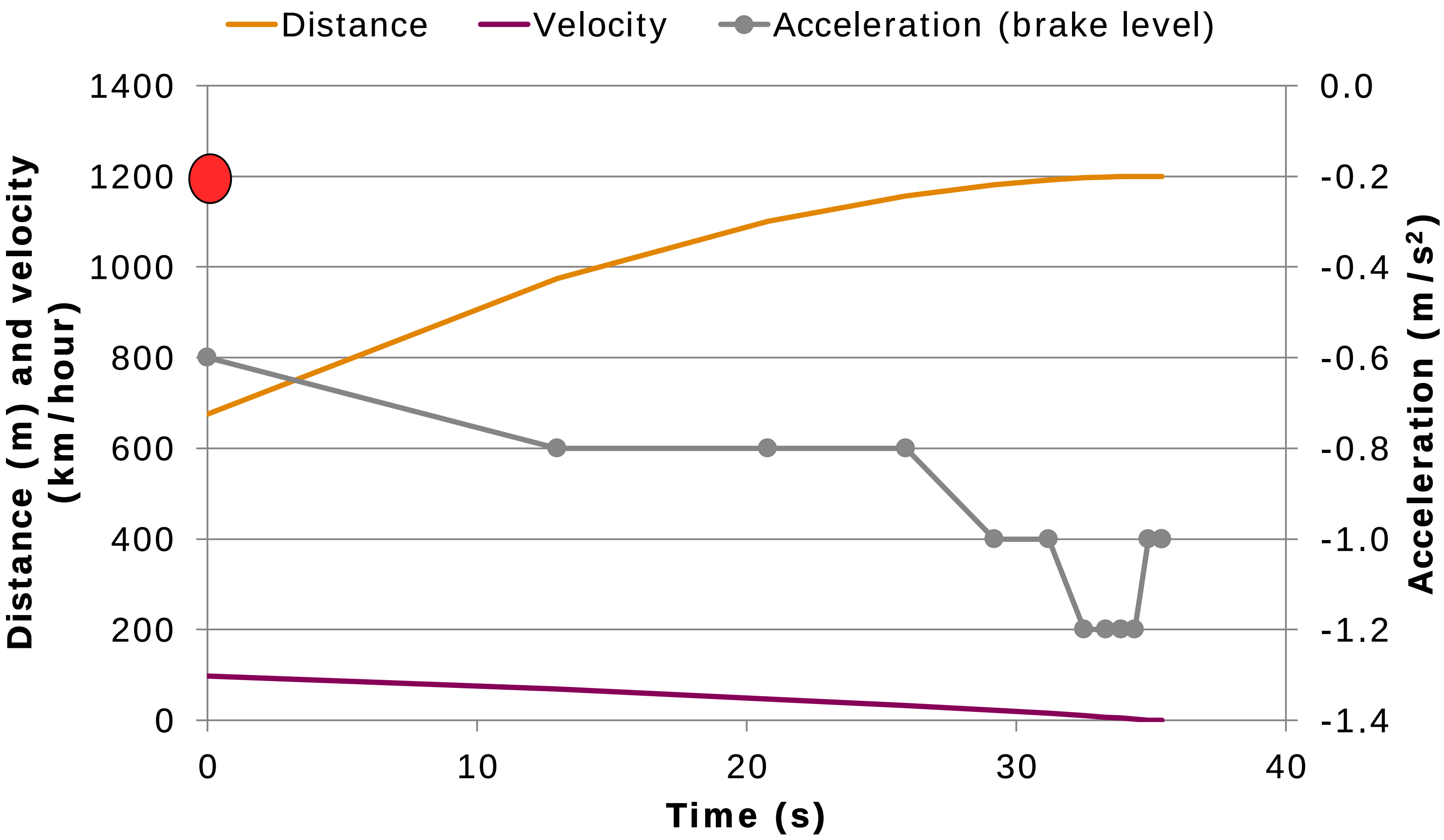
Train driver control model



Info on:
strategy, current tactic, location, speed, state of train, …

Example of tactic: braking to stop before signal

At each dot, the driver evaluates the braking rate by observing speed and distance to signal



Concluding remarks

- Discrete Event Simulation modelling has proven viability for the risk analysis of different safety critical systems.
- It works and can produces a great deal of informative output and, in particular, probabilistic risk measures.
  - Fault trees, Event trees and safety barrier diagrams are rather easily modeled and simulated by DES environments.
- The model may also predict rare events that may occur during the lifetime of an installation, but on the cost of the simulation run time -> drawback compared with analytical calculations
- The quality of safety barriers may depend on
  - procedures and maintenance standards
  - the educational level of the personal.

➢ Within the DES environment, it is possible to include human operations.

➢ Technical focused risk assessments can directly take human factors and performance into account.

Concluding remarks

- The application of DES modeling in connection with risk analysis for which dynamic characteristics of the modeled processes cannot be neglected.
- Hereunder the advantages compared to conventional models used in risk management are shown.
  - This enables to make better predictions for dynamical situations (variations in input parameters).
  - Such models provide more detailed answers to questions
  - Models retain geographical dependencies and time patterns.
- The approach is highly applicable in other areas e.g. fire safety management

Thank you for your interest

fram@dtu.dk