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

Markert, Frank; Kozin, Igor

Publication date: 2015

Document Version Peer reviewed version

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

Frank Markert  Igor Kozine
fram@dtu.dk  igko@dtu.dk

Produktionstorvet byg. 424
2800 Kongens Lyngby
Danmark
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

![Fault Tree Diagram]

- Loss of power supply
  - Probability: $P=1.199\times10^{-5}$
- Power generator fails 0.2%
- Power backup system fails
  - Switching device fails 0.1%
  - Fuel cell/battery fails 0.5%
Modelling approach practised in risk analysis

Example power backup system

- Fault tree
- Event tree
Modelling approach practised in risk analysis

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

Example power backup system
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:

\[ P(\text{Supply failure}) = P(\text{Supply failure} \mid \text{Pipeline rupture}) \times P(\text{Pipeline rupture}) \]

- Rupture event easily predicted by e.g. Fault tree
- the consecutive supply failure is not easily predicted 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 mimic or imitate processes 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
DESI 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
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

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 feedback 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

1)
- Create release events
- Initialize parameters
- Hole Parameters
- VBA
- Delay accident
- Detector check

2)
- Immediate ignition
  - Ignition parameters
  - VBA
  - Alarm flame
  - Calc ASET
  - Write jet flame parameter
  - Number jet fires
  - VBA
  - Alarm gas
  - VBA
  - VBA
  - Calc ASET
  - Write delayed ignition
  - Write dispersion table
  - Number gas explosions

3)
- Create crew
- Initialization
- Working
- Working place
- ASET RSET
  - Counting rescued workers
  - Rescued workers
  - Counting fatalities
  - Workers died

Arena® software version 14.50.00

SPs Riskseminar, Lund 25. November 2014
Example results:

<table>
<thead>
<tr>
<th>Input</th>
<th>average</th>
<th>st.dev.</th>
<th>min</th>
<th>max</th>
</tr>
</thead>
<tbody>
<tr>
<td>wind speed (m/s)</td>
<td>11</td>
<td>5</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>wind direction (degrees)</td>
<td>91</td>
<td>52</td>
<td>0</td>
<td>180</td>
</tr>
<tr>
<td>hole size statistic (mm)</td>
<td>12</td>
<td>28</td>
<td>1</td>
<td>200</td>
</tr>
<tr>
<td>No. workers at random positions</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

Output:

<table>
<thead>
<tr>
<th>Output</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>wind speed in module (m/s)</td>
<td>0.6</td>
<td>0.3</td>
<td>0.1</td>
<td>1.4</td>
</tr>
<tr>
<td>mass flow (kg/s)</td>
<td>6.2</td>
<td>27.8</td>
<td>0.007</td>
<td>271.5</td>
</tr>
<tr>
<td>SEPmax jet flame (kW/s)</td>
<td>40</td>
<td>11</td>
<td>28</td>
<td>93</td>
</tr>
<tr>
<td>RSET (s)</td>
<td>240</td>
<td>176</td>
<td>301</td>
<td></td>
</tr>
<tr>
<td>ASET (s)</td>
<td>427</td>
<td>0</td>
<td>&gt;600</td>
<td></td>
</tr>
<tr>
<td>No. fatalities per accident</td>
<td>1.3</td>
<td>1.8</td>
<td>0</td>
<td>5</td>
</tr>
</tbody>
</table>
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)
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.)**
- $\mu$: storage capacity (items, “chunks”)
- $\delta$: decay time of an item
- $\kappa$: main code type (physical, acoustic, visual, semantic)
- $\tau$: cycle time
Model structure using DES with queues

External input

Distracting events

Task lost

Time expired?

Extrn queue

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

Driver

Perception channel
(Open/Close)

Perceive stimulus t_p

Stimulus to WM t_s

Working Memory (WM)

Tasks in queue

Retrieve task with highest priority & attributes

Taking decision Depending on task

Train

Cockpit

Panel

Train position

Train behaviour

Time forward Δt or t_acum

Time forward t_acum

Action t_a

Look at:
1. Outside
2. Panel
3. Other

Δt_r + t_m

Time t

Time t

25. November 2014

DTU Management Engineering, Technical University of Denmark
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