Experience Report:

Modelling and Simulation of Railway Emergency Response Plans

S4CIP Workshop, May 25, 2016

Lene Sandberg
Joint work with Søren Debois & Thomas Hildebrandt

IT UNIVERSITY OF COPENHAGEN

Metropolitan University College
Plan

• Cyber-threats to Critical Infrastructure
• The method
• The Great Belt Bridge incident case
• Collaborative mapping & simulation
• Conclusions
Cyber-threats & Infrastructure
Cyber-physical attacks on Critical Infrastructure

- Operators (DSB, BaneDanmark - Danish railway) robust against physical incidents, including terrorism.
- Operators IT system landscape very large and varied.
- However, traditional “No-IT” approach to train operators still form foundations of day-to-day operations.
The potential weakness

• Cyber-physical assault: Combined physical & cyber attack.

• Do emergency response plans hold up when both IT and physical infrastructure is physically attacked?
How to investigate?

• Extensive emergency response plans exist. Drills are performed regularly.

• Let’s simulate!

• But wait! Paper-based rehearsals don’t actually use ICT systems. How to simulate?

• We need to simulate both the actions of drill participants and breakdowns of IT systems.

• We have to be sure no-one “cheats” by accidentally assuming some system is functioning.
Declarative Process Models

- Formal model of emergency response process.
- Give enormous freedom within a set of rules.
- No-one cheats accidentally; the model won’t allow it.
How do we try this out?

How do we get the process model?
Case: Great Belt Bridge
Collaborative mapping

• Extensive documentation of emergency response procedures exists.

• We sat down with domain experts from DSB & BaneDanmark (Danish railway) and constructed a model based on that documentation.
Collaborative simulation

• Simulation gives the ability to explore un-anticipated paths and “what-if” scenarios.

• *Collaborative* simulation brings a new level of realism, especially for coordination problems of emergency response scenarios.
Simulation study, Metropol

- At Metropol, students of Emergency and Risk Management as participants.
- Tool provided insufficient overview.
- Tool did not hide available and executed actions of other participants.
Simulation study, DSB

• At DSB, with DSB emergency response team lead and experienced train driver.

• Recommendations:
  Pictures, text, documentation in-tool.
Conclusions

• Collaborative mapping and simulation of emergency response processes is a viable means of studying ICT/Cyber-physical vulnerabilities.

• DCR Formalism accessible to domain experts (with assistance)

• DCR Tooling *almost* there.
Thank you!

Lene Sandberg

Metropolitan University College