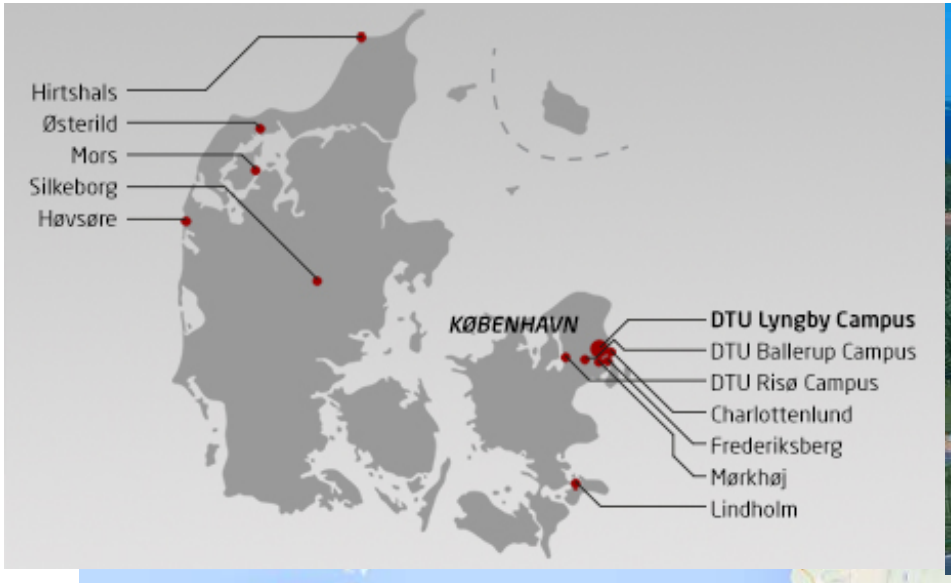
RISK RESEARCH FOR SAFETY CRITICAL SYSTEMS AT THE TECHNICAL UNIVERSITY OF DENMARK

Igor Kozine, ***Senior researcher***

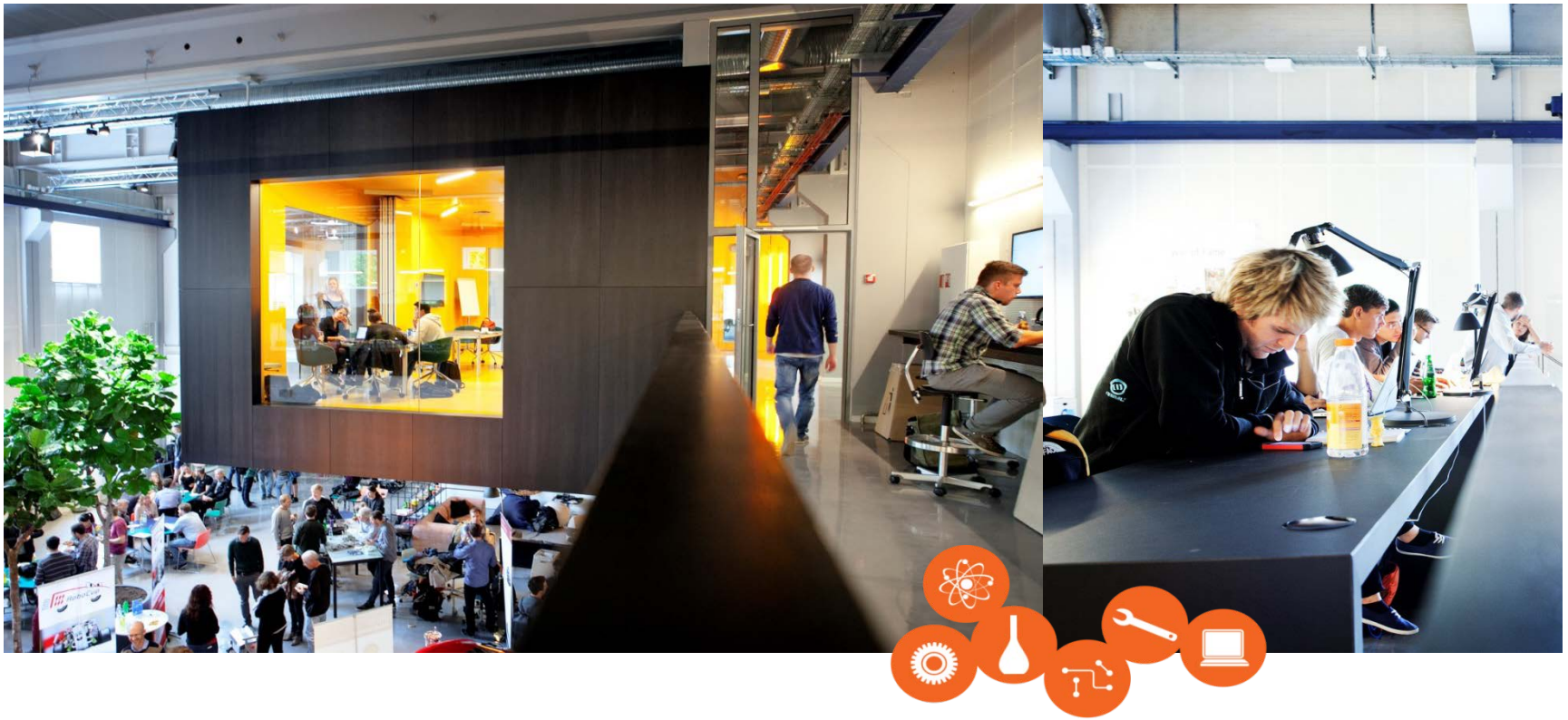
igko@dtu.dk


Hirtshals
Østerild
Mors
Silkeborg
Høvsøre
KØBENHAVN
DTU Lyngby Campus
DTU Ballerup Campus
DTU Risø Campus
Charlottenlund
Frederiksberg
Mørkhøj
Lindholm


Risø National Laboratory


Baltic Sea
North Sea
Edinburgh
United Kingdom
Isle of Man
Dublin
Manchester
Liverpool
Danmark
Hamburg
Berlin
Polska
Poland

Technical University of Denmark

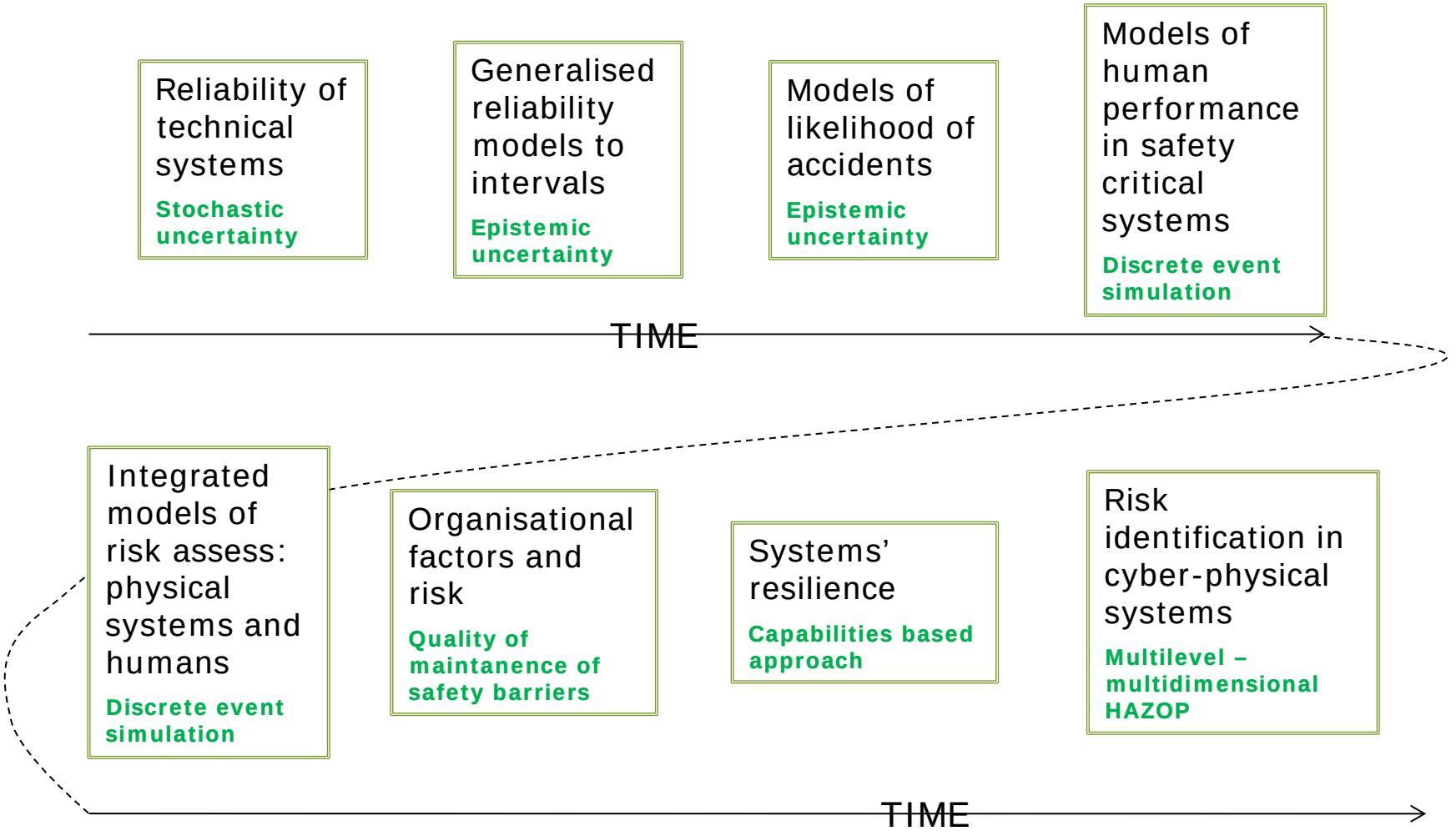


TECHNICAL UNIVERSITY OF DENMARK (DTU)

Founded in 1829, ca. 7,000 undergraduate students, 4,000 graduate students, 1,500 PhD fellows. There are 18 Departments (Aqua, Chemical Engineering, Chemistry, Civil Engineering, Compute, Electrical Engineering, Energy, Environment, Food, Fotonik, Management Engineering, Mechanical Engineering, Nanotech, Physics, Space, Systems Biology, Vet, Wind Energy) and Centres (e.g. Oil & Gas, Healthcare Technologies, Maritime, RailTech, Transport, UNEP, Business).

Reliability and Risk Research

Academic milestones



Reliability and Risk Research

Domains

Nuclear power generation

Wind power generation (onshore-offshore)

Oil and gas transportation

Shale gas production

Offshore oil and gas production

Maritime

Railway

Bridges and tunnels

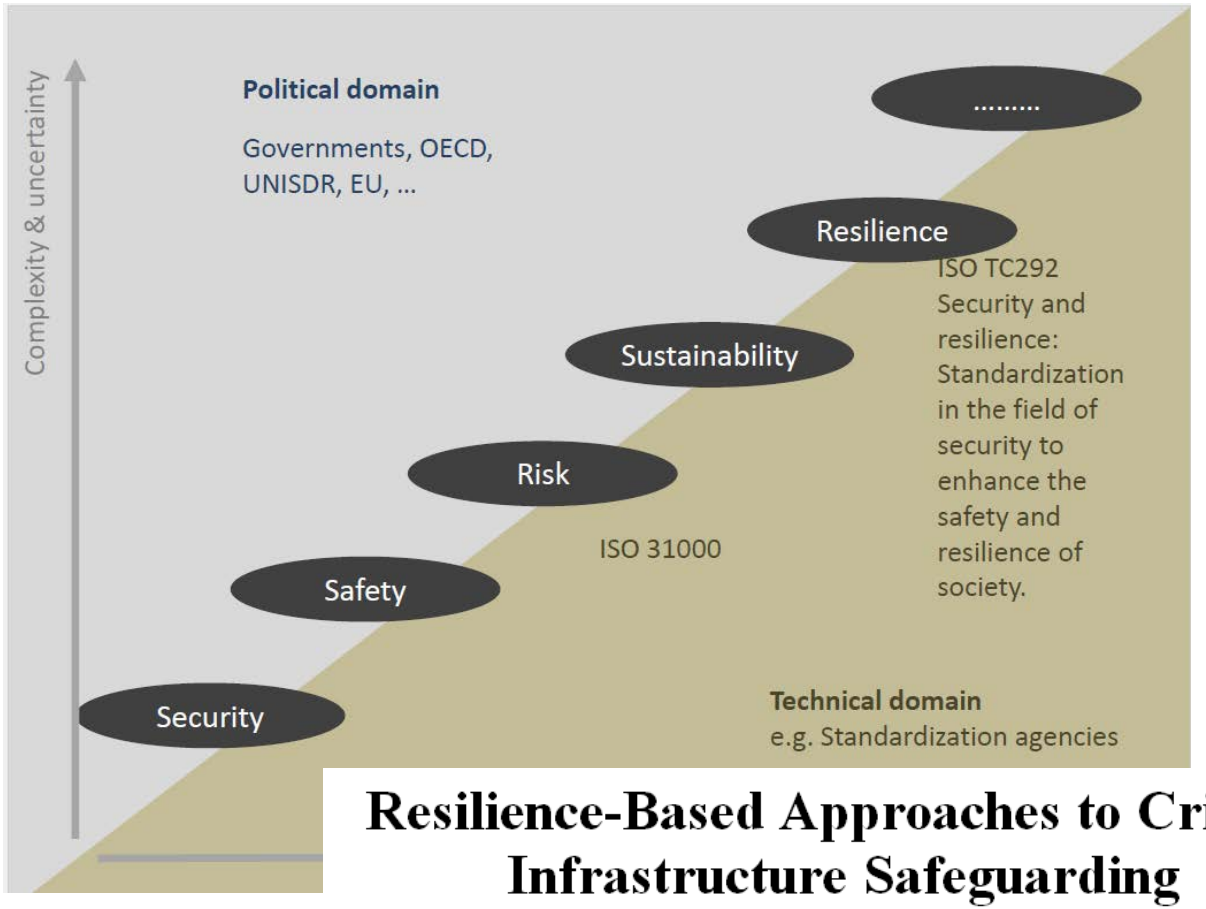
Chemical

Hydrogen-driven vehicles, transportation and distribution

Water supply

Etc.

From Risk to Resilience



Resilience-Based Approaches to Critical Infrastructure Safeguarding

Marie-Valentine Florin,

NATO Workshop

26-29 June 2016, Ponta Delgada, Azores, PORTUGAL

Capabilities-based approach for assessing the resilience of critical infrastructure

Resilience capabilities are defined as enablers of activities and functions that serve the resilience goals.

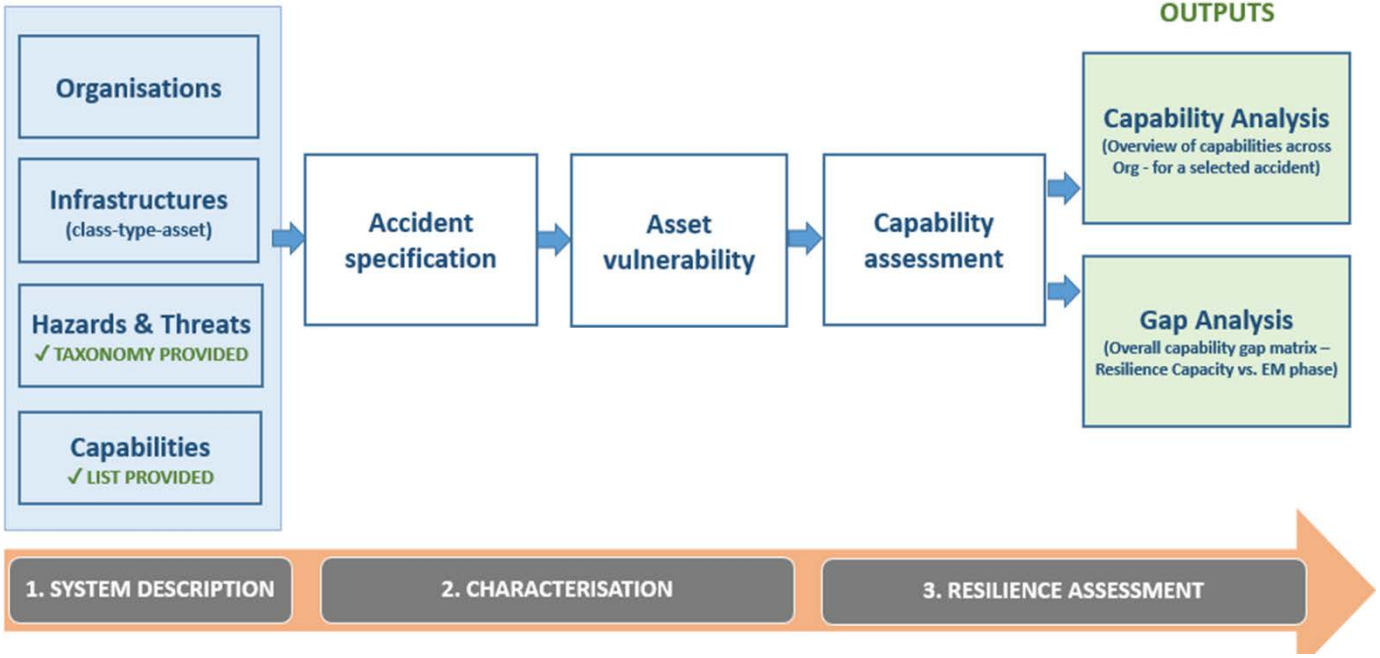
A *resilience capability* is further broken down into three related compounds: *assets*, *resources*, and *practices/routines*.

Resilience capabilities' space				
System types	**Phases of the Emergency Management Cycle**			
	Prevention/ Mitigation	Preparedness	Response	Recovery
Technical				
Organizational				
Social				
Economic				
Resilience goals & activities to serve goals	*Prevent* disruption	Maintain & sustain resilience capabilities	*Absorb* shock & *adapt*	*Adapt* & *restore*

Capabilities-based approach for assessing the resilience of critical infrastructure

The approach is being developed in the framework of the EU financed project 'Resilience Capacities Assessment for Critical Infrastructures Disruptions' (READ).

The strategy of the capabilities-based planning is to prepare for a large variety of threats and risks instead of simply preparing for specific scenarios.



WELCOME TO INTERNATIONAL CONFERENCE!

Creating Resilience Capability against Critical Infrastructure Disruptions: Foundations, Practices and Challenges

IDA Conference Center, Copenhagen, Denmark

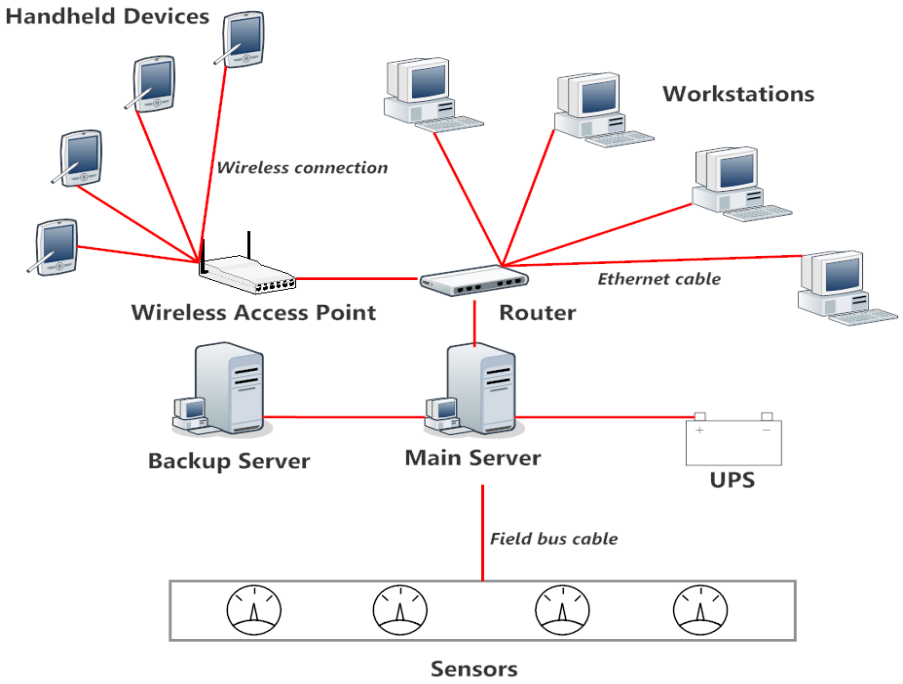
13 April, 2015

Risks identification in cyber-physical systems

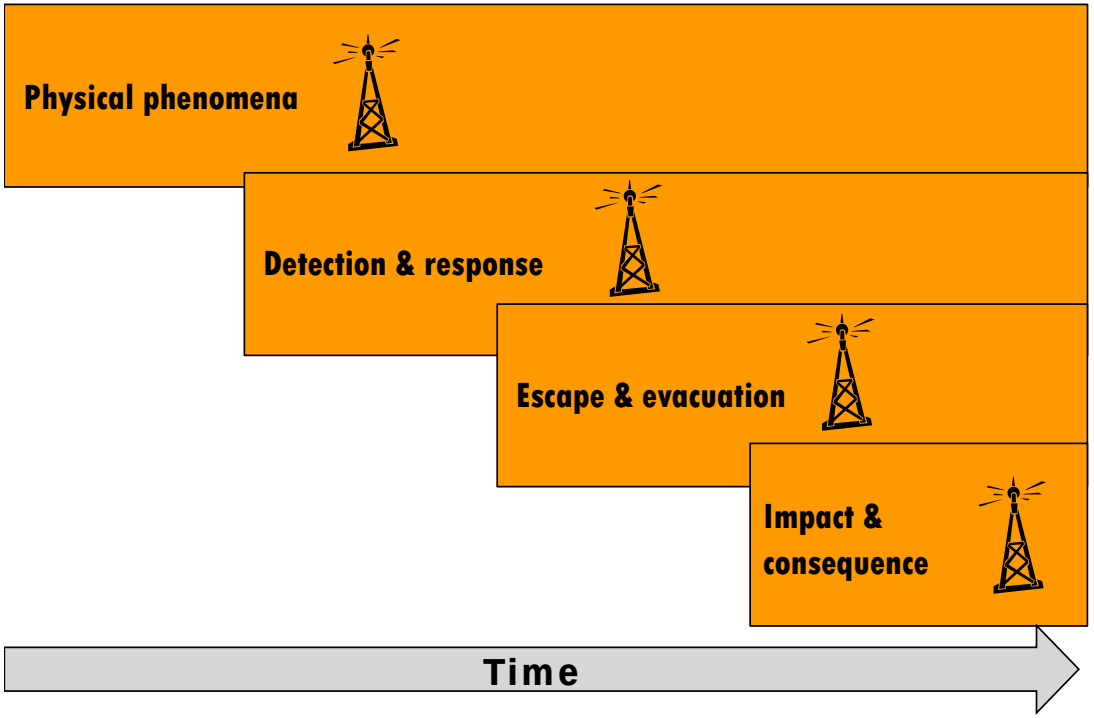
An approach is being developed based on Hazard and Operability Studies (HAZOP). Focal points of the approach are:

- identifying appropriate system representations (respecting the designers' choice of formalism)
- identifying relevant system parameters and deviation guidewords for hazard identification

A *distributed maintenance management system* inside a nuclear power plant has been so far to demonstrate the approach.



Offshore Platform Hydrocarbon Risk Assessment – OPHRA: Feasibility study of an alternative method for Quantitative Risk Assessment using Discrete Event Simulation



Each process is modelled separately and sends feed-back to the others providing interaction between processes

Simulation based tool for risk assessment and mitigation in complex systems with strategic components

- Risk modelling tools for ***cyber-physical*** systems are limited to systems with non-strategic component while accounting for ***strategic component*** behaviour is essential.
- These systems often exhibit externalities that may have significant effect on the systemic risks. Selfish or/and malicious components are potential risk contributors and the severity of their consequences should be attempted to being modelled.
- We can hardly expect that the assessment of consequences can be amenable to analytic evaluation.
- We suggest research towards incorporating strategic component behaviour into simulation based tools for risk analysis and mitigation.

Generalizing reliability models to interval probabilities

Football example

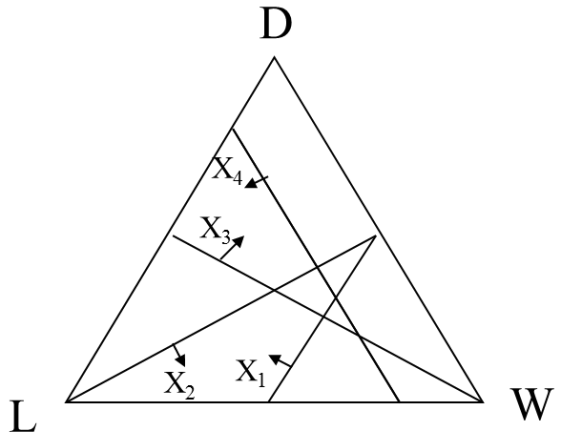
The three possible outcomes are win (W), draw (D) and loss (L) for the home team.
Your beliefs about the match are expressed through the following simple probability judgements

X_1: chance to win is less than 50%
X_2: win is at least as probable as draw
X_3: draw is at least as probable as loss
X_4: the odds against loss are no more than 4 to 1

$P(W) \in [0.33, 0.5]$

$P(D) \in [0.25, 0.4]$

$P(L) \in [0.2, 0.33]$

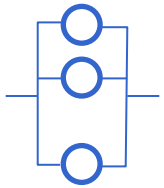


Generalizing reliability models to interval probabilities

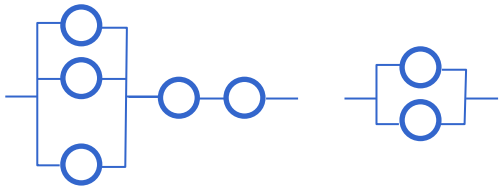
Parallel-series systems

Components connected in series

in parallel



in series-parallel



If reliability information on components is provided in the form of upper and/or lower bounds on probabilistic reliability characteristics, upper and lower bounds of system's reliability can be calculated.

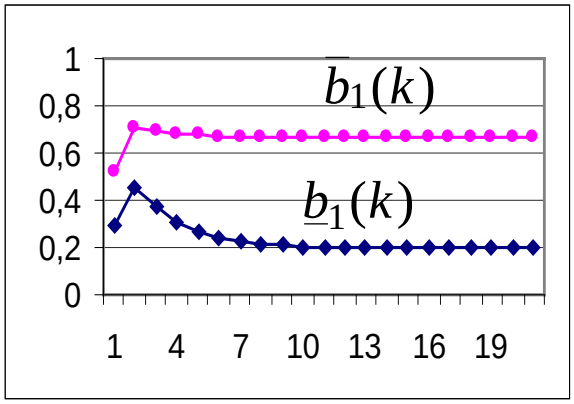
Generalizing reliability models to interval probabilities

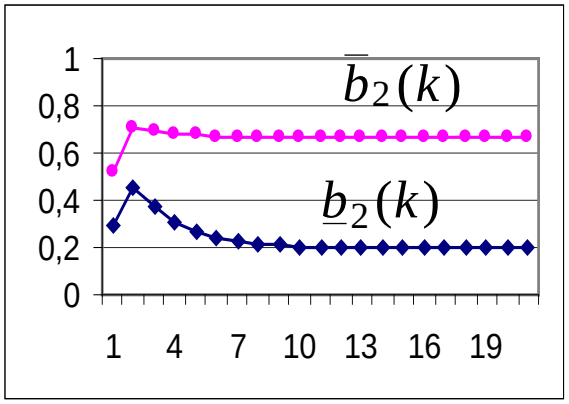
Markov chains

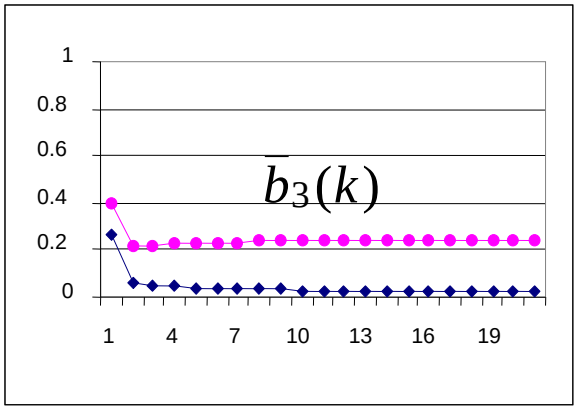
When state and transition probabilities are given as intervals, a solution to propagation of state probabilities was provided

$$\{\underline{b}_j(0)\} = \{0.21; 0.29; 0.27\} \qquad \{\overline{b}_j(0)\} = \{0.31; 0.52; 0.4\}$$

$$\|\underline{a}_{ij}\| = \begin{Vmatrix} 0.7 & 0.05 & 0.01 \\ 0.15 & 0.6 & 0.08 \\ 0.02 & 0.7 & 0.1 \end{Vmatrix} \qquad \|\overline{a}_{ij}\| = \begin{Vmatrix} 0.9 & 0.29 & 0.25 \\ 0.3 & 0.77 & 0.2 \\ 0.1 & 0.88 & 0.2 \end{Vmatrix}$$







Generalizing reliability models to interval probabilities

Stress-strength reliability models under incomplete information

Y is a random variable describing the ***strength*** of a system

X is a random variable describing the ***stress*** applied to the system

The reliability of the system is determined as ***R=Pr(X<Y)***

Lack of knowledge about independence of ***X*** and ***Y***	Independent ***X*** and ***Y***
Partially known probability distributions Only ***n*** points of prob distribution of ***X*** are known and m points of ***Y***	
Known moments of probability distributions Precise or imprecise moments of prob distributions of ***X*** and ***Y*** are known	
Probability distributions on nested intervals Nested intervals of ***X*** and ***Y*** with known probs of finding the true values inside them	

$$\Pr\{\underline{\alpha}_i \le X \le \overline{\alpha}_i\} = p_i,\ \Pr\{\underline{\beta}_j \le Y \le \overline{\beta}_j\} = q_j,\ i = 1, ..., n,\ j = 1, ..., m,$$

$$[\underline{\alpha}_1, \overline{\alpha}_1] \subseteq [\underline{\alpha}_2, \overline{\alpha}_2] \subseteq ... \subseteq [\underline{\alpha}_n, \overline{\alpha}_n],\ [\underline{\beta}_1, \overline{\beta}_1] \subseteq [\underline{\beta}_2, \overline{\beta}_2] \subseteq ... \subseteq [\underline{\beta}_m, \overline{\beta}_m],$$

$$p_1 \le p_2 \le ... \le p_n,\ q_1 \le q_2 \le ... \le q_m.$$

Generalizing reliability models to interval probabilities:

Stress-strength reliability models under incomplete information

Y is a random variable describing the ***strength*** of a system

X is a random variable describing the ***stress*** applied to the system

The reliability of the system is determined as ***R=Pr(X<Y)***

Example of results

Source information	**Structural reliability** (lower and upper bounds)
Case of independent X and Y	
$\underline{p}_i \le \Pr\{X \le \alpha_i\} \le \overline{p}_i$ $\underline{q}_j \le \Pr\{Y \le \beta_j\} \le \overline{q}_j$	$\underline{R} = \sum_{i=1}^{n} (\underline{p}_i - \underline{p}_{i-1})(1 - \overline{q}_{j(i)})$ $\overline{R} = 1 - \sum_{k=1}^{m} (\underline{q}_k - \underline{q}_{k-1})(1 - \overline{p}_{I(k)})$
$F_X(x)$ $\underline{q}_j \le \Pr\{Y \le \beta_j\} \le \overline{q}_j$	$\underline{R} = \sum_{i=1}^{m} (1 - \overline{q}_i)(F_X(\beta_i) - F_X(\beta_{i-1}))$ $\overline{R} = 1 - \sum_{k=1}^{m} (\underline{q}_k - \underline{q}_{k-1})(1 - F_X(\beta_k))$
$F_Y(y)$ $\underline{p}_j \le \Pr\{X \le \alpha_j\} \le \overline{p}_j$	$\underline{R} = \sum_{i=1}^{n} (\underline{p}_i - \underline{p}_{i-1})(1 - F_Y(\alpha_i))$ $\overline{R} = 1 - \sum_{i=1}^{n} (1 - \overline{p}_i)(F_Y(\alpha_i) - F_Y(\alpha_{i-1}))$
Ignorance of independence	
$\underline{p}_i \le \Pr\{X \le \alpha_i\} \le \overline{p}_i$ $\underline{q}_j \le \Pr\{Y \le \beta_j\} \le \overline{q}_j$	$\underline{R}^* = \max_{i=1,\ldots,n} \max\left(0, \underline{p}_i - \overline{q}_{j(i)}\right)$ $\overline{R}^* = 1 - \max_{k=1,\ldots,m} \max\left(0, \underline{q}_k - \overline{p}_{I(k)}\right)$

Generalizing reliability models to interval probabilities

Other results

- Interval-Valued Structural Reliability Models Based on Statistical Inference (Imprecise Dirichlet Model)
- Combining Unreliable Judgements and Deriving Probability Parameters of Interest
- Improving Imprecise Reliability Models by Employing Constraints on Probability Density Functions, Failure Rate and other. (Use of the calculus of variations and automated control theory.)
- Constructing Imprecise Probability Models

Project risk management

The potentials of post-probabilistic uncertainty and risk quantification for **(running PhD project)**

Alternative approaches for representing and quantifying uncertainty and risk in the management of large engineering projects are investigated:

1. Imprecise probability
2. Dempster-Shafer theory of evidence
3. Possibility theory, which is formally a special case of the imprecise probabilities, so we won't discuss it separately
4. Semi-quantitative representations including the NUSAP tool.

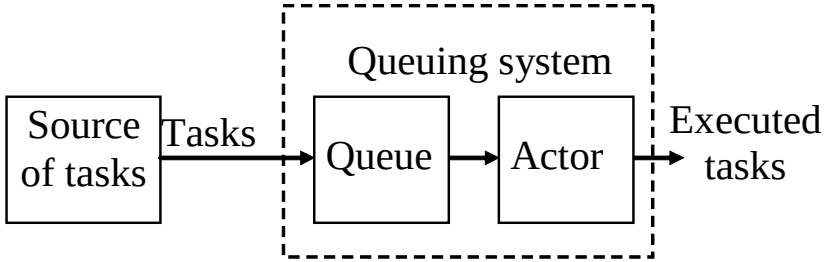
Two cases:

Construction of off-shore wind turbine farms, and

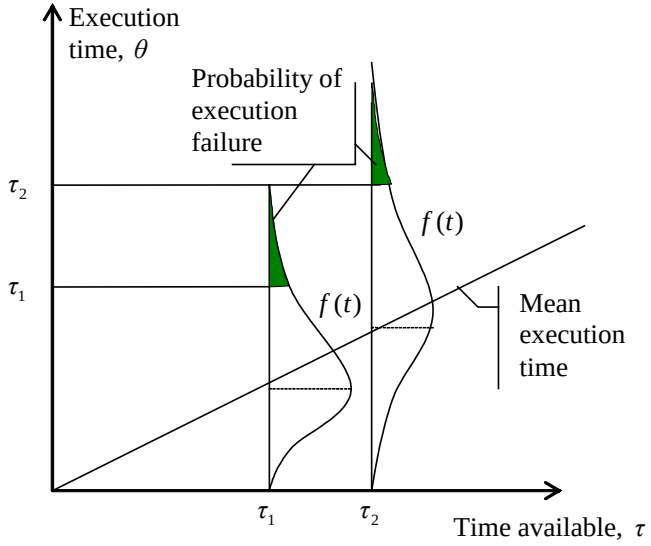
Construction of the fixed link between Denmark and Germany (20 km submersible tunnel)

Simulation of Human Performance in Time-Pressured Scenarios

The model of human performance can be presented as a queuing system



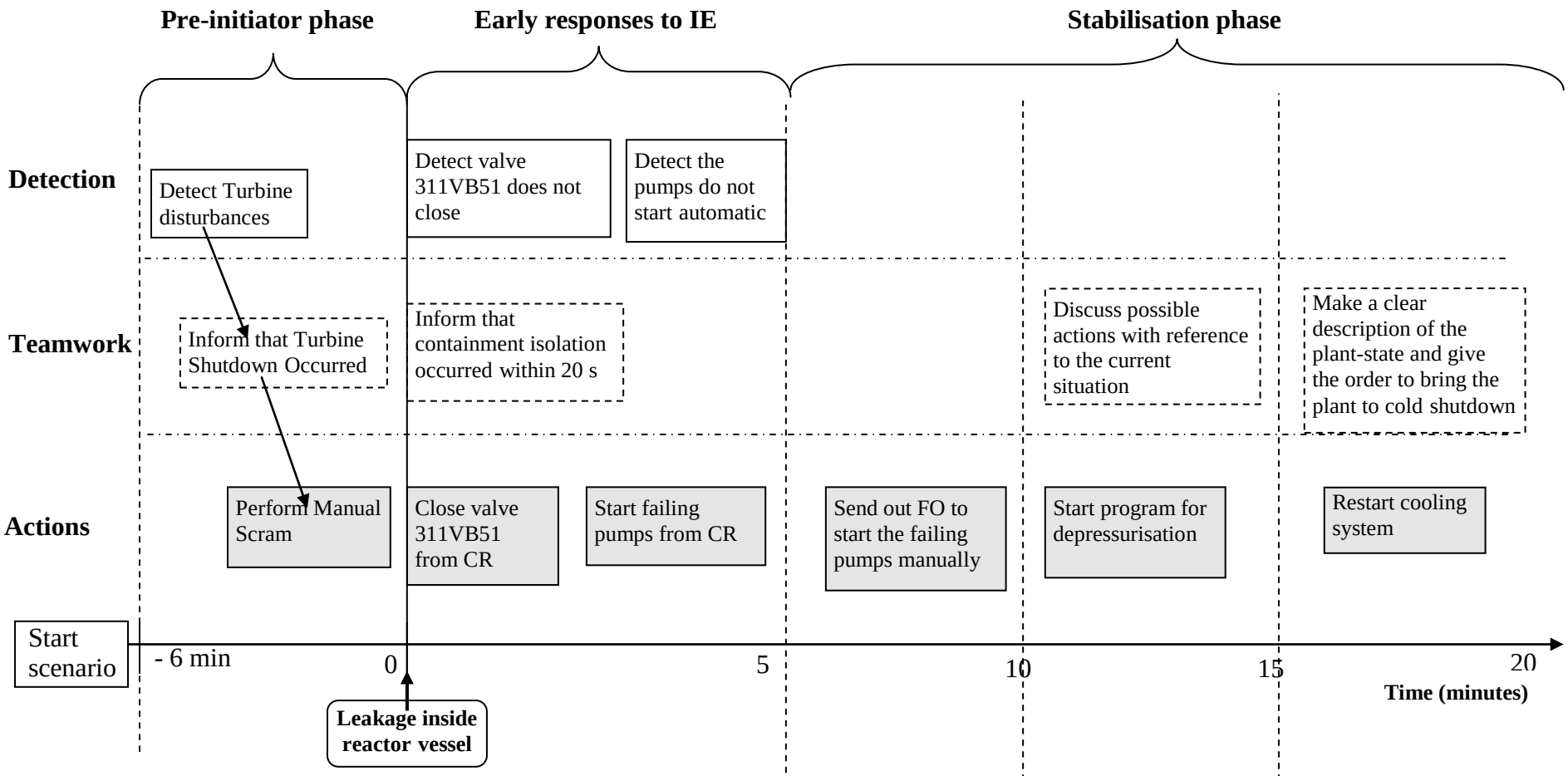
The probability of failure is defined as the probability of execution time exceeding time available



Discrete event simulation for the analysis of human performance and risks of socio-technical systems:

Simulation of Human Performance in Time-Pressured Scenarios

First, a task analysis is done



Discrete event simulation for the analysis of human performance and risks of socio-technical systems:

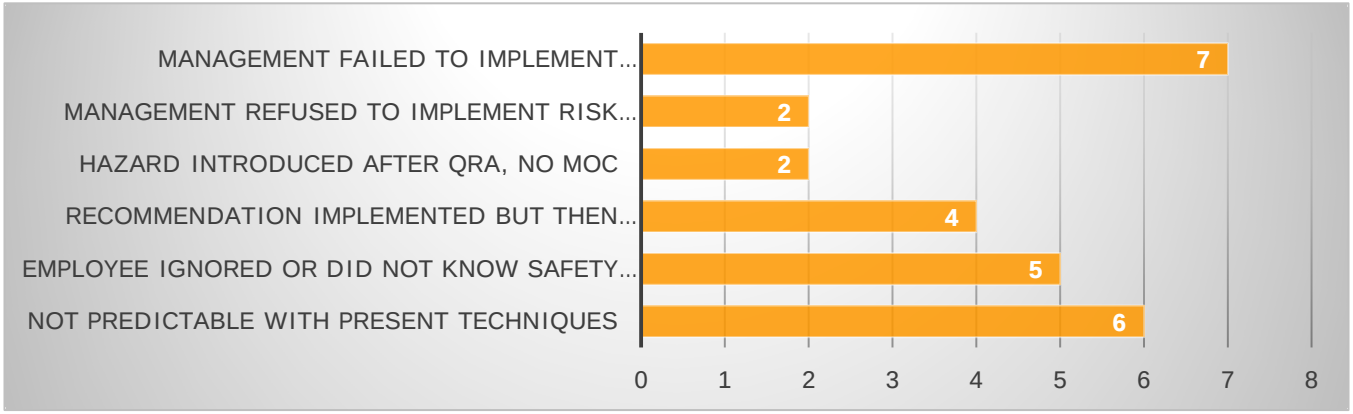
Other reference projects

1. Reliability of a gas supply to customers. *Financed by Swedegas, owner and operator the gas pipeline Dragør, DK – Gutherborg, SV*
2. Safe manning of merchant ships. *Financed by the Danish Maritime Foundation*
3. Train driver performance modelling (developing engineering models for usability studies). *Being performed in the framework of the Halden Project*
4. Operational risk of assets for a Water Utility Company. *Supported by Københavns Energi and Reliasset A/S*
5. Risk analysis of a generic hydrogen refuelling station. *Internal financing*
6. Optimizing the rating of offshore and onshore transformers for an offshore wind farm. *Internal financing*
7. Powering stochastic reliability models (Markov models) by discrete event simulation. *Internal financing*

Unforeseen events with high impacts: validation of practices and models for predictability

Research project proposal

A recent study of risk analysis results for 103 oil, gas and chemical plants carried out over a 36-year period demonstrates that 20% of the accidents that affected these plants were found to have been due to unforeseen accident scenarios.



Hypotheses. (1) worst-case scenarios seem to take place more frequently than foreseen in the risk analyses applied, (2) lack of predictability is major source of risk that is left unattended and that is often comparable with or greater than the predicted risk, and (3) all this happens because of deficiencies in risk identification practices and models of prediction of rare events.

DTU Management Engineering