DTU Management
Department of Technology,
Management and Economics

Engineering Systems Design

Risk Management for Innovation

5th SRA Nordic Conference

Copenhagen

7 - 8 November 2019

Contents

Program

Conference day 1 | November 7, 2019

08:30 Registration
09:00 Conference opening by chair I. Kozine
09:10 Welcome by DTU's dean of research K. K. Andersen
09:30 Plenary

RISK AND INNOVATION DIALOGUE (Plenary, Room 101)

09:30	Keynote: No pain – no gain	**S. Berg**
10:10	Keynote: Addressing the Tensions Between Precaution and Innovation	**M.-V. Florin**
10:50	Coffee break	
11:10	Expert panel: Risk and Innovation	

12:00 **Lunch**

12:45 Session 1	**Room**	**Chair**
Track 1: Artificial Intelligence and Risk Analysis	Room 101	R. Taylor
Track 2: Risk Analysis of Cyber-Physical Systems	Room 102	N.C. Guzman
Track 3: Risk Perception and Communication	Room 208	A. Balzekiene

14:00 **Coffee break**

14:15 Session 2	**Room**	**Chair**
Track 4: Risk Analysis of Cyber-Physical Systems	Room 101	J. Zhang
Track 5: Risk Management for Organisations	Room 102	J. Oehmen
Track 6: Software Tools for Risk Analysis	Room 208	N.J. Duijm
Track 7: Risk Analysis for Critical Infrastructure	Room 212	S.H. Jore

15:30 **Coffee break**

15:45 Session 3	**Room**	**Chair**
Track 8: Risk Management for Organisations	Room 101	
Track 9: Uncertainty Assessment	Room 102	I. Kozine
Track 10: Learning from Accidents and Regulatory Practices	Room 208	F.H. Hedlund
Track 11: Issues of Digitalisation	Room 212	M. Ylönen

17:00 **Dinner**

18:00 SRA Nordic Chapter Board meeting

Conference day 2 | November 8, 2019

Risk Forum: "Digitalization – Smart or Scary?"

08:30	Registration	
09:00	Program start: Welcome & Introduction to Risk, Responsibility and Innovation for Smart Systems	
09:30	Impulse Talk #1 – Reliability of Smart Systems: Safety-Certifying Smart Systems for Railways - What works and what doesn't	**S. Munck**
10:00	Workshop Part #1 – "Experience Speed Dating" and reflection in group: The challenges of smart system reliability and fast innovation cycles	
12:00	Impulse talk #2 – Smart Systems, Smart Project, Smart Strategy? Opportunities and risks of a "smart business"	**C. Klint**
11:30	**Lunch and Networking**	
12:15	Workshop Part #2 – 1 on 1 discussions and reflection in group: Project and Strategy Risk Management Approaches for Smart Systems	
13:00	Impulse Talk #3 – Communicating and Discussing Digitalization Risks and Benefits - The Societal Perspective	**Prof. Dr. M. Horst**
13:45	**Coffee break**	
14:00	Workshop Part #3 – Table workshops and report out: Expectations and gaps in smart system risk regulation and perception	
14:45	Wrap-up	
15:00	Keynote: Failures and How to Avoid Them	**J. R. Taylor**
15:30	Closing Ceremony	
15:40	**Networking reception (and light dinner)**	
16:30	End of the day	

Risk Forum: "Digitalization – Smart or Scary?"

As part of the SRA Nordic Conference 2019, we are organizing the 7th Risk Forum.

The Risk Forum is a format that brings together risk practitioners from industry, government and academia. We explore debate and share experiences on current hot topics in risk management.

The Forums are organized around three main elements: Short impulse talks by leading experts in the field, interactive workshops, and networking opportunities.

The 7th Risk Forum is held as part of the 5th SRA Nordic Conference on November 8, 2019 in Copenhagen. The topic is "Digitalization – Smart or Scary?". Together, we will explore three major themes in this context:

- Development speed and smart system reliability: What are the implications of the vastly different innovation cycles and technological maturity that make up our complex cyber-physical systems, from autonomous cars to smart buildings? How can we safety-certify systems where critical components are under constant development, for example safety-critical autonomous systems?
- Project and strategy risks of smart systems: How can we better support project managers and senior executives in managing innovation projects that focus on digital innovation? How can we ensure that our risk and resilience management techniques span the technical, project and strategy space?
- Regulating perceived risks and benefits of smart systems: How do we account for risk (and benefits) perception in regulating "smart" systems, as well as the uneven distribution of their risks and benefits? How do we trade-off the additional benefits with the additional vulnerabilities we introduce?

Each topic will be introduced by an impulse talk of an internationally leading expert, followed by a workshop and experience exchange of the participants.

Keynotes and Impulse Talks

Day 1, 7 November

NO PAIN – NO GAIN
Svein Berg, *Managing Director of Nordic Innovation*

ADDRESSING THE TENSIONS BETWEEN PRECAUTION AND INNOVATION
Marie-Valentine Florin, *Executive director of the International Risk Governance Center at EPFL, Switzerland*

Day 2 - Risk Forum, 8 November

RELIABILITY OF SMART SYSTEMS: SAFETY-CERTIFYING SMART SYSTEMS FOR RAILWAYS - WHAT WORKS AND WHAT DOESN'T
Stig Munck, *Rambøll Danmark A/S*

SMART SYSTEMS, SMART PROJECT, SMART STRATEGY? OPPORTUNITIES AND RISKS OF A "SMART BUSINESS"
Claus Klint, *Director of Internet of Things, IBM Denmark*

COMMUNICATING AND DISCUSSING DIGITALIZATION RISKS AND BENEFITS - THE SOCIETAL PERSPECTIVE
Prof. Dr. Maja Horst, *Technical University of Denmark*

INNOVATION FAILURES AND HOW TO AVOID THEM
J. Robert Taylor, *Technical University of Denmark*

Sessions

SESSION 1

TRACK 1: ARTIFICIAL INTELLIGENCE AND RISK ANALYSIS

Offshore deep-water mooring line integrity monitoring using neural networks
N. H. Christiansen, *DNV GL Denmark – Oil & Gas*

Machine Learning and information theory for data-driven Uncertainty Quantification and Risk Analysis
U. Alibrandi, *Aarhus University, Aarhus, Denmark,*
K.M. Mosalam, *University of California at Berkeley, Berkeley, US*

Explaining the robustness of Deep Neural Network to support safety by design: A preliminary study
J. Zhang, J. Li, *Norwegian University of Science and Technology, Trondheim, Norway*
I. Kozine, *Technical University of Denmark*

TRACK 2: RISK ANALYSIS OF CYBER-PHYSICAL SYSTEMS

When major accidents are no longer accidental: The emergence of destructive cyber-attacks
N. H. Carreras Guzman, *Technical University of Denmark, Norwegian University of Science and Technology (NTNU)*
I. Kozine, *Technical University of Denmark*

Low risk: multi-innovative GIANT Wind Turbine concept
E. Muller, *MSME ETH Zurich, Switzerland (Roskilde, Denmark)*

Information visualisation for risk identification in cyber-physical systems
A. Idrissov, N. C. Guzman, A. Maier, *Technical University of Denmark*

A Systematic Approach to Cyber-Physical Hazard Analysis in Smart Buildings
B. Kalluri, R. J. Taylor and I. Kozine, *Technical University of Denmark*

TRACK 3: RISK PERCEPTION AND COMMUNICATION

Gender and Risk Perception: Quantifying the impact of gender on the assessment of natural, technological and civil risks
G. D. Brown, A. Largey, C. McMullan, *DCU Business School, Dublin City University, Glasnevin Campus, Ireland*

Algorithms as risk communication support tool within precision medicine
S. M. Kovacevic, F. Bouder, *University of Stavanger, Norway*

The role of experiential knowledge in climate change risk perception and decisions for adaptation and mitigation among citizens of Malmö, Sweden
K. Blennow, *Swedish University of Agricultural Sciences, Alnarp, Sweden,* J. Persson, *Lund University, Sweden*

Using NEP scale to explain public risk perception of energy technologies
A. Balžekienė, A Budžytė, *Kaunas University of Technology, Lithuania*

SESSION 2

TRACK 4: RISK ANALYSIS OF CYBER-PHYSICAL SYSTEMS

Developing and analyzing a digital instrumentation and control system for a safety fan
S. Sarshar, B. A. Gran, *Institute for Energy Technology (IFE), Halden, Norway*

In Depth Hazards and Security Analysis for an Industrial Test Enclave for Methods Testing and Validation
J. R. Taylor, C. Chronopoulos, S. Piccolo, *Technical University of Denmark*
S. Sarshar, J. E. Simensen, *Institute for Energy Technology (IFE), Halden, Norway*

Demystifying Cyber-Physical Risks in Smart Building
B. Kalluri, I. Kozine, *Technical University of Denmark*

Dynamic influence diagrams for risk-based decision making for rebars
S. Rastayesh, J. D. Sørensen, *Aalborg University, Department of Civil Engineering, Aalborg, Denmark*

TRACK 5: RISK MANAGEMENT FOR ORGANISATIONS

Risk based assessment to determine contract relationships between building clients and AEC companies and the impact on innovation
J. B. Berg, C. Thuesen, P. A. Jensen, *Technical University of Denmark*

Prevention of dust exposure in demolition work in Denmark– a participatory approach intervention
S. Grøn, *Technical University of Denmark*
H. J. Limborg, A. Kabel, *TeamArbejdsliv, Valby, Denmark,*
P. Kines, *The National Research Centre for the Working Environment, Copenhagen, Denmark*

Exploring the practical impact of municipal risk assessments through a longitudinal study of individual and organizational learning
A. Cedergren, H. Hassel, *Centre for Critical Infrastructure Protection (CenCIP), Lund University, Sweden*

Learning and Risk Management Practices in Engineering Design Teams of Innovative Projects
A. Shafqat, T. Welo, *Norwegian University of Science and Technology, Trondheim, Norway,*
J. Oehmen, *Technical University of Denmark*

TRACK 6: SOFTWARE TOOLS FOR RISK ANALYSIS

SafetyBarrierManager, a tool for safety-barrier diagrams and bowties
N. J. Duijm, *Nicestsolution, Jyllinge, Denmark*

HAZEX – A Tool for Semi-automated Hazards Analysis for Process Plants, Cyber-physical systems and Human Activities
J. R.Taylor, *Technical University of Denmark*

HUGIN Software for Risk Analysis
A. L. Madsen, N. Søndberg-Jeppesen, *HUGIN EXPERT A/S, Aalborg, Denmark; Aalborg University, Denmark*
F. Jensen, *HUGIN EXPERT A/S, Aalborg, Denmark*

Value creating Risk Management with RamRisk
J. Pedersen, *Rambøll, Copenhagen, Denmark*

TRACK 7: RISK ANALYSIS OF CRITICAL INFRASTRUCTURE

The role of regional airports for sustainable development and crisis management – A Swedish case study
C. Große, P.M. Olausson, B. Svensson, *Risk and Crisis Research Centre – Mid Sweden University, Sundsvall/Östersund, Sweden*

Towards cross-sector risk management in Swedish critical infrastructures
T. R. Sonesson, *Lund University, Sweden*

Fault Tree Analysis supporting water balance management in enrichment plants
R. Molarius, *VTT Technical Research Centre of Finland, Tampere, Finland*

SESSION 3

TRACK 8: RISK MANAGEMENT FOR ORGANISATIONS

Balancing speed and precision in risk management
F. B. Helweg-Larsen, *Risk & Security, Devoteam A/S, Copenhagen, Denmark*

Sustainability risk management (SRM) - a necessary perspective for companies of tomorrow: A tool to map the SDGs with the company's risk impact and identify its sustainable risk profile
A. Find, *Projektrisikostyring.com, Roskilde, Denmark,*
N. Foxby-Jacobsen, *Blue Tree ApS, Hellebæk, Denmark*

Applying the concept of Actuality to Project Risk Management
P. Willumsen, J. Oehmen, *Technical University of Denmark, Copenhagen, Denmark,* T. Welo, *NTNU, Trondheim, Norway,* M. Rossi, *Polytecnico di Milano*

3 reasons why every business plan on the planet ignores risks and how to fix it
A. Sidorenko, *RISK-ACADEMY, Malta*

TRACK 9: UNCERTAINTY ASSESSMENT

A Bayesian Belief Network approach to incorporate stakeholders' values into environmental risk assessment
A. Lehikoinen, M. Laurila-Pant, *University of Helsinki, Finland*
S. Mäntyniemi, R. Venesjärvi, *Natural Resources Institute Finland, Helsinki, Finland*

Knowledge-based construction of probabilities
N.J. Duijm, I. Kozine, *Technical University of Denmark*

Bayesian analysis of risk and uncertainty
U. Sahlin, *Lund University, Lund, Sweden*

Using Bayesian Networks for Root Cause Analysis of Observable Problems in Cyber-Physical Systems
S. Chockalingam, V. Katta, *Institute for Energy Technology, Halden, Norway*

TRACK 10: LEARNING FROM ACCIDENTS AND REGULATORY PRACTICES

Implementing a Lessons Learned Process in the Business Value Chain of a Project Driven Organisation
K. Balasubramaniam, *Technical University of Denmark*

De-learning – a challenge for risk management
F. H. Hedlund, *COWI, Copenhagen, Denmark; Technical University of Denmark*

Fragmentation in total institutions: Observations on regulatory practices and risk management
M. Björk, *Gothenburg University, Gothenburg, Sweden*
C. Thodelius, *Chalmers University of Technology, Gothenburg, Sweden,*
K. Nolbeck, *Sahlgrenska Academy at Gothenburg University, Gothenburg, Sweden*

TRACK 11: ISSUES OF DIGITALISATION

Safety culture and security culture - Discrepancies, tensions and synergies?
M. Ylönen, *Technical Research Centre of Finland, VTT,*
S. H. Jore, *University of Stavanger, Norway*

Conceptualizing smartness of CPSs
C. Chronopoulos, I. Kozine, *Technical University of Denmark*

Approaches for operationalizing digitalization strategies
B. A. Kadir, O. Broberg, *Technical University of Denmark*

Abstracts

Session 1

Track 1:
Artificial Intelligence and Risk Analysis

Offshore deep-water mooring line integrity monitoring using neural networks

N. H. Christiansen
DNV GL Denmark – Oil & Gas

As the offshore industry moves into deeper waters and increasingly tough environments, the need for robust integrity monitoring systems becomes ever more pronounced.

Safe operation of floating installations requires absolute positioning control. A key element in this is a full functioning mooring line system. Mooring lines keeping these floating installations in place are hence both safety critical elements and exposed to very rough environmental conditions.

The tough conditions cause sensors, attached directly on the mooring lines, to fail often, resulting in a lot of false alarms which are very expensive and time consuming to handle. The ambition of the presented work has therefor been to develop a method based on a more reliable data source such as GPS positioning measurements collected on the floating installation away from very exposed locations.

Neural networks have been shown to be able to learn and predict the pattern between vessel motion and mooring line forces with very high accuracy [1, 2]. So, with this ability to learn the behavior of a floating installation perhaps the neural network can also be trained to detect mooring line failures by detecting changes in system's behavior and maybe even classify these abnormalities. The question is therefor: Is it possible to evaluate the state of the mooring system on a floating offshore installation only by analyzing GPS records using neural networks?

This presentation describes the idea behind the method, the applied algorithms, possibilities and challenges. It also demonstrates the importance of thorough risk analysis when applying neural networks in assessment of safety critical elements. One of the major challenges for the presented method is that the algorithm must be very sensitive to changes in system behavior but also insensitive to changes in weather conditions.

References

[1] Sagrilo L.V.S., Gao Z., Naess A. & Lima E.C.P. (2011), "A straightforward approach for using single time domain simulations to assess characteristic response", *Ocean Engineering*, Vol. 38, No. 5, pp. 1464-1471.

[2] Christiansen N.H., Voie P.E.T., Høgsberg J. & Sødahl N. (2013), "Efficient mooring line fatigue analysis using a hybrid method time domain simulation scheme", *Proceedings of the 32nd ASME International Conference on Ocean, Offshore and Arctic Engineering (OMAE '13)*, vol. 1.

Machine Learning and information theory for data-driven Uncertainty Quantification and Risk Analysis

U. Alibrandi
Aarhus University, Aarhus, Denmark
K.M. Mosalam
University of California at Berkeley, Berkeley, US

This paper presents a novel data-driven framework of Uncertainty Quantification, Structural Reliability and Risk Analysis based on the Information Theory and Machine Learning.

At first, main concepts of information theory are presented, e.g. Entropy, KL Divergence, Mutual Information (MI); their relationships with the classical uncertainty quantification, like maximum likelihood estimation and copulas are discussed. It is shown that the optimal probabilistic model may be determined through minimum relative entropy and the theory of statistical learning; it is also discussed that methods based on the maximum entropy, like the Kernel Density Maximum Entropy Method (KDMEM) [1, 2] recently proposed by the authors, may perform well for the evaluation of the marginal distributions, including the tails, from samples of small size.

It is shown that the coefficient of correlation is not a good measure of dependence between random variables, and that it always underestimates the true dependence. An alternative measure, called informational coefficient of correlation and based on the mutual information is suggested [3]. Its accuracy and robustness is shown through some representative examples. It may also represent a very attractive tool for probabilistic sensitivity analysis.

To determine the joint distribution of the basic random variables it is proposed the multivariate probabilistic model of Distributions with Independent Components (DIC) [4]. It has the same computational simplicity of Nataf, but it is more accurate, since it does not pursue any assumption about the tail dependency. DIC is applied to determine the joint distribution of wave height and period of wave data. The accuracy and effective of this novel data-driven framework of Uncertainty Quantification and Risk Analysis is also shown through applications of structural reliability analysis.

References

[1] Alibrandi, U. & Mosalam, K.M. (2017), "Kernel Density Maximum Entropy with generalized moments for evaluating probability distributions, including tails, from a small sample of data", *International Journal for Numerical Methods in Engineering*, **113**(13): 1904-28

[2] Alibrandi, U. & Mosalam, K.M. (2018), "Code-Conforming PEER Performance Based Earthquake Engineering using Stochastic Dynamic Analysis and Information Theory", *KSCE Journal of Civil Engineering*, **22**(3): 1002-15

[3] Alibrandi, U. and Mosalam, K.M. (2019a), "Information Theory for data-driven Risk Analysis: The informational coefficient of correlation", *29th European Safety and Reliability Conference*, September 22-26, 2019, Hannover

[4] Alibrandi, U. and Mosalam, K.M. (2019b), "Distribution with Independent Components for Uncertainty Quantification and Structural Reliability Analysis", *13th International Conference on Applications of Statistics and Probability in Civil Engineering, ICASP13*, May 26-30, 2019, Seoul, South Korea

Explaining the robustness of Deep Neural Network to support safety by design: A preliminary study

J. Zhang, J. Li
Department of Computer Science, Norwegian University of Science and Technology, Trondheim, Norway
I. Kozine
Engineering Systems Group, Technical University of Denmark, Copenhagen, Denmark

Context: Deep neural network (DNN) has shown the remarkable performance of planning and executing more and more complex tasks comparable to human experts. There is a trend to apply DNNs in a wide range of applications (e.g., autonomous vehicles, drones, health care devices, and robot systems). Unfortunately, a lot of empirical evidence has been shown that DNN is intrinsically vulnerable to adversarial perturbations (i.e., small changes added to the original input, cause misclassification). This makes it difficult to apply DNNs in safety-critical domains.

The robustness of DNN has drawn a lot of attention in AI safety community. Measurable robustness indicators is also recommended in the latest published cross-industry white paper (named safety first for automated driving [1]) to support safety by design. Robustness of a DNN is its ability to cope with perturbed inputs (i.e., intentionally generated adversarial inputs, and unintentionally received noisy input). Some studies [2, 3] have focused on the robustness of specific DNNs through understanding, detecting, and mitigating adversaries. A few other attempted to understand the characteristics of robust neural networks [4]. However, why the specific DNN is robust remains a standing open challenge.

Content: Instead of evaluating the robustness of a specific DNN, this on-going work focuses on gaining the critical insight behind robust DNNs. We evaluate three state-of-the-art analysis tools on verifying the robustness of DNNs. The outputs from the analysis tools are compared to answer the following research questions:

- RQ1: what is the commonality of robust DNN models?
- RQ2: What is the key difference between robust and non-robust DNN models?
- RQ3: If we change the model structure, hyper-parameter, and optimization methods of a robust DNN, is it still robust? If it is not robustness, what is the difference of output compared to the unchanged model?

Expected results and conclusion: This presentation will report our experimental findings on two aspects: 1) capability of the existing analysis tools (for revealing instinct features of robust DNNs), and 2) limitations of the tools. Besides, we plan to propose a new approach for explaining the robustness of DNN models as our future work. The outcome of this work can guide the software designer to choose a DNN model with appropriate robustness level.

References

[1] "Safety first for automated driving,"2019, Available: https://www.daimler.com/innovation/case/autonomous/safety-first-for-automated-driving-2.html
[2] N. Carlini and D. Wagner, "Towards Evaluating the Robustness of Neural Networks," in 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 39-57.
[3] T. Gehr, M. Mirman, D. Drachsler-Cohen, P. Tsankov, S. Chaudhuri, and M. Vechev, "AI2: Safety and Robustness Certification of Neural Networks with Abstract Interpretation," in 2018 IEEE Symposium on Security and Privacy (SP), 2018, pp. 3-18.
[4] M. Cisse, P. Bojanowski, E. Grave, Y. Dauphin, and N. Usunier, "Parseval networks: Improving robustness to adversarial examples," arXiv preprint arXiv:1704.08847, 2017.

Track 2:
Risk Analysis of Cyber-Physical Systems

When major accidents are no longer accidental: The emergence of destructive cyber-attacks

N. H. Carreras Guzman
Engineering Systems Group, Technical University of Denmark (DTU); Department of Mechanical and Industrial Engineering. Norwegian University of Science and Technology (NTNU)
I. Kozine
Engineering Systems Group, Technical University of Denmark (DTU)

Industrial systems and production processes incorporating and interconnecting new digital technologies possess well-known benefits in terms of efficiency, comfort and sustainability. Seemingly, these technological innovations should also prove useful to prevent *major accidents*. However, evidence from experimental research and real incident bulletins show how *emerging risks* could provoke – and already have provoked – serious physical damages. These new risks include unintentional errors such as software design flaws, conflicts between higher levels of process automation and the role of humans as supervisors, among others. Yet arguably, some of the most critical emerging risks stem from cyber-security vulnerabilities and their potential to cascade into serious physical damages. Examples include the cyber-attack to the Maroochy wastewater treatment facility in Australia in 2000, the Baku-Tbilisi-Ceyhan (BTC) pipeline cyber-attack in Turkey in 2008, the Stuxnet worm affecting an Iranian nuclear facility in 2010, the German Steel Mill cyber-attack in 2014, and the TRITON attack against the safety-critical systems of a petrochemical plant in Saudi Arabia in 2017. In the maritime context, Nordic recommended practices recognize now vulnerabilities of highest criticality, where hackers could potentially take remote control of ships navigating at sea and disrupt their navigation systems [1].

Hence, the question arises: Could *non-accidental* sources of risks from the *cyber* domain lead to the serious *physical* damages usually associated to major accidents? The answer seems affirmative. These are maliciously intended *cyber-physical attacks* leading to serious physical damages. In the Danish Defence Intelligence Service, they are also known as *destructive cyber-attacks* [2]. Although these incidents have safety implications, safety analysts tend to neglect them in their traditional analysis methods. Due to the malicious intent that characterizes these cyber-physical attacks, safety analysts tend to regard them as the domain of cyber-security. However, the domain of cyber-security has traditionally aimed at the confidentiality, integrity and availability of information technologies (IT), not at the safety of humans and physical systems. In fact, the domain of IT security and the domain of cyber-physical safety and security require different knowledge fields and different strategies to mitigate the particular risks. Therefore, the need for safety and security require an integration of concepts and tools to address these emerging risks.

This presentation will illustrate a new hazard scenario builder, named Cyber-Physical Harm Analysis for Safety and Security (CyPHASS). Building on the concept of Uncontrolled Flows of Information and Energy (UFoI-E) [3], the builder is a practical tool for risk identification that incorporates lessons from recent cyber-physical attacks. Furthermore, CyPHASS provides generic diagrams inspired by the bow-tie model to assist the process of identifying emerging hazards from the interactions between the cyber and the physical domains. Using CyPHASS, safety and security risk analysts will be able to identify both unintentional and malicious sources of risk, assess their interactions, and recommend suitable safety and security barriers to prevent and mitigate the potentially serious damages.

References

[1] DNV GL, “Cyber security resilience management for ships and mobile offshore units in operation,” *DNVGL-RP-0496*, no. September. 2016.
[2] Centre for Cyber Security, “Threat Assessment: The Cyber Threat Against Denmark 2019,” Copenhagen, 2019.
[3] N. H. Carreras Guzman, D. K. M. Kufoalor, I. Kozine, and M. A. Lundteigen, “Combined safety and security risk analysis using the UFoI-E method : A case study of an autonomous surface vessel,” in *29th European Safety and Reliability Conference. Accepted for publication*, 2019.

Low risk: multi-innovative GIANT Wind Turbine concept

E. Muller
MSME ETH Zurich, Switzerland
Roskilde, Denmark

GIANT Wind Turbine AHA^{HigHtecH} (Adaptable Hybrid Aerodynamo) holistic concept.
Low risk development of skyscraping 400 meters HIGH Wind Turbine: 300 meters rotor diameter, efficiency-boosting 150 meters BiG Hub diameter, 6 wings 50%RR (Rotor Radius), up to 30 Megawatt Capacity, slim innovative tower column with 8 guy rods (see crane rods).
The AHA^{HigHtecH} Wind Turbine features improved spin-out indirect impacts on Skyline, Climate, Environment, etc. Lower CO2 footprint, less exhaust of poisonous NOx, particles, etc from vehicles, ships “house warming”, etc.

So many dozens of risks can be spared or reduced by the next generation, the AHA^{HigHtecH} GIANT Wind Turbines. AHA^{HigHtecH} is opening the next era in Wind Power: low risk and high emphasis on safety, polytechnical as well as human safety, shareholder and consumer safety.
Avoiding and minimizing risks by manufacturing steel wings with a dozen cutting-edge improvements. Several innovations of AHA^{HigHtecH} allow the quantum leap to lower risk implementation of steel wings which have so many USP: AHA^{HigHtecH} 50%RR-wings (6xhalf-length, 1/8 weight approx.) are cheap and much cheaper maintenance & repair, they are more efficient, less noisy, more stiff, more agile (10 times approximately), even less visible, more sustainable, recyclable and less risky than blade-composite-materials used today.

Further low-cost upsizing and weight reduction can be reached, if you can take the rotor out of the wind. Either innovatively tilting the rotor upwards into the umbrella position, which can be done easily and quickly!!! An innovative unloading of the tower from twisting torque from the rotor. Or, like with small wind turbines, the entire GIANT can be laid down (for much more frequent wing cleaning and polishing, M&R, exchange of wing set, to avoid lightning strikes, to let pass insects, earth, sand, high turbulent winds or a Hurricane). Avoiding and Minimizing Risks and Costs by assembling AHA^{HigHtecH} near ground (and decommissioning or re-erection in a developing country!)

AHA^{HigHtecH} 660 USP (Unique Selling Points) almost everything is improved
AHA^{HigHtecH} 60 USP 50% BETTER (HALF or 150%)

Winds of change, the AHA^{HigHtecH} has overcome the conventional concept limited in upsizing by inherent incurable Achilles`heels: too simple, poor agility, too heavy, less efficient, etc.
The even more efficient BIG HUB AHA^{HigHtecH} may open new exclusive low wind markets.
AHA^{HigHtecH} has excellent odds to dominate the global market of the GIANTs in 2050.

References

[1] Google: AHA wind turbine clic twice on the picture ”AHA turbine” for Rechargenews Article by Darius Snieckus
[2] Google: AHA vindmølle IDA Idekatalog pages 39 – 41
[3] Presentations of AHA^{HigHtecH} at DTU “European Master in Wind Energy” in 2014-2018 (108 slides)

Information visualisation for risk identification in cyber-physical systems

A. Idrissov, N. H. Carreras Guzman, A. Maier
Engineering Systems Group, Technical University of Denmark (DTU)

Cyber-physical systems (CPSs) are defined as combining of computational and physical systems [5]. Examples may include production systems and also critical infrastructure systems, such as power and water supply, telecommunication networks, transportation, government and emergency services [6]. Typically, CPSs are highly complex socio-technical structures on several levels of hierarchy, with various interactions between many actors, objects and processes. As such, modelling has been a common approach to abstraction and understanding of such complex CPSs [6]. By modelling system entities and their interconnections, hierarchically decomposing them into subsystems, one can analyse the behaviour of CPSs as a whole, track their vulnerabilities and prescribe improvements to mitigate potential risks.

While in practice traditionally, text, tables and diagrams are used as *visual representations* for system modeling, when the systems become too complex, these representations introduce information overload for the users. Though Unified Modelling Language (UML) [3] and SysML [4] diagrams are based on standardised and clearly defined logical conventions [7], the visual techniques used are often subpar and do not allow achieving efficient visual communication of underlying information to its users [8].

Information Visualisation is a branch of Human-Computer Interaction that studies "computer-supported, interactive, visual representations of data to amplify cognition" [1]. By encoding information into a changeable medium, it is said that information visualisations improve the cognitive processing power of users, allow fast information search, and assist recognition of patterns [1]. Using the concept of Uncontrolled Flows of Information and Energy (UFoI-E) [2], it is possible to build interactive diagrams to depict threats and hazards, corresponding detection, prevention and containment measures with respect to cyber-, physical and cyber physical layer states of CPSs. In the present study, we discuss the application of Information Visualisation techniques to design a model representation for UFoI-E-related risk identification in CPSs. Through designing an interactive visualisation that displays CPSs and their behaviour under various attack scenarios, our aim is to improve users' ability to systemise and make sense of potential hazards, their sources and appropriate defense strategies.

References

[1] Card, M. (1999). Readings in information visualization: using vision to think. Morgan Kaufmann
[2] Guzman, N. H. C., & Kozin, I. (2018). Uncontrolled flows of information and energy in cyber-physical systems. European Safety and Reliability Association Newsletter, Volume 9, pp. 2-3.
[3] Fowler, M., & Scott, K. (2004). UML distilled: a brief guide to the standard object modeling language. Addison-Wesley Professional.
[4] Friedenthal, S., Moore, A., & Steiner, R. (2014). A practical guide to SysML: the systems modeling language. Morgan Kaufmann.
[5] Lee, E. A. (2006, October). Cyber-physical systems-are computing foundations adequate. In Position paper for NSF workshop on cyber-physical systems: research motivation, techniques and roadmap, Volume 2, pp. 1-9.
[6] Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability engineering & System safety, Volume 121, pp. 43-60.
[7] Patou, F, Dimaki, M, Maier, A, Svendsen, WE, Madsen, J. Model-Based systems engineering for life-sciences instrumentation development. Systems engineering. 2019; Volume 22, pp. 98– 113.
[8] Sindiy, O., Litomisky, K., Davidoff, S., & Dekens, F. (2013). Introduction to information visualization (infovis) techniques for model-based systems engineering. Procedia Computer Science, 16, pp. 49-58.

A Systematic Approach to Cyber-Physical Hazard Analysis in Smart Buildings

B. Kalluri, R. J. Taylor and I. Kozine
Technical University of Denmark, Kgs. Lyngby, Denmark

The progressive integration of Information Technology (IT) such as networks, interactive displays, computer applications, cloud technologies and Operational Technologies (OT) such as sensors, actuators and controllers in buildings on one hand promises improved energy efficiency, occupant comfort, and operational efficiency in managing buildings. On the other hand, it paves the way for vulnerabilities that could compromise safety and security of occupants, assets and further disrupt business continuity. As the technologies for Smart Buildings (SBs) are rapidly evolving and more buildings are turning into smart environments, the cyber-physical threats and hazards are eminent.

In theory, failure modes that would develop due the integration of OT and IT can't be described by simple failure of individual components in buildings, but only through unprecedented interaction of group of components and their interfaces. This phenomenon is analogous to emergent hazards in the context of Smart Buildings. Thus, the specific goal of this study is to identify such emergent hazards that would compromise the fire safety of Active Fire Protection (AFP) systems in a smart office environment. The proposed approach explores the application of bigraphs and/or digraphs to model a hypothetical SB with integrated AFP system, HVAC system for thermal comfort and door-access controls for security. Further, the effectiveness of the proposed approach is validated through hazard identification sessions with experts.

To the best of our knowledge, it is one of the first study that attempts to study the cyber-physical hazards in integrated SBs with an objective to develop safety barriers and improve current risk analysis approach and fire safety inspection process.

Track 3:
Risk Perception and Communication

Gender and Risk Perception: Quantifying the impact of gender on the assessment of natural, technological and civil risks

G. D. Brown, A. Largey, C. McMullan
DCU Business School, Dublin City University, Glasnevin Campus, Ireland

To enhance disaster-reduction policies and risk communication messages, there is a need for an improved understanding of how people perceive risk [1]. How gender impacts individuals' risk perception is one significant dimension [2-4]. To contribute, our study examines the differences between females' and males' risk perception using a comprehensive range of 17 risks taken from the 26 risks listed on the 2012 Irish National Risk Assessment [5].
Data was gathered using self-administered questionnaires, from 1977 respondents', of whom 59.1% identified as female. Using ordered probit analysis with marginal effect calculations and OLS regression we estimate the impact of gender on three components of 17 involuntary risks (likelihood, impact and overall risk rating) while controlling for a set of independent variables (socio-demographic factors, risk exposure, household preparedness, fatalism/wishful thinking/denial).
The results show that while the magnitude and significance of the gender coefficients vary by risk, a general pattern becomes apparent: females judged involuntary risks as being more likely, having a greater impact, and/or having a higher overall risk rating than their male counterparts. The impact rating for Fire was the one significant exception to this pattern - where males rated the impact of Fire higher than females. 40 of 51 regressions show as significant for the gender coefficient when controlling for the set of independent variables, with gender showing as significant for more likelihood risk ratings (15 of the 17 risks) and overall risk ratings (14 of the 17 risks) than impact risk ratings (11 of the 17 risks).
These findings suggest that the specific risk is relevant when considering the significance of the effect of gender. This finding leads to three contributions: 1) Our results indicate that the impact of gender on risk assessment depended on the risk. This suggests that merging risk constructs into broader measures could provide misleading results regarding the effects of gender. 2) Our results also highlight that it is important not only to consider overall risk rating but also the individual components, (likelihood and impact, for each specific risk). Our results show that for some risks there were significant differences between the effect of gender on impact, likelihood and overall risk rating. 3) Finally, our results show that while gender may influence specific risk ratings, the effect is not observed across all 17 involuntary risks.

References

[1] Aerts, J.C.J.H., Botzen, W.J., Clarke, K.C., Cutter, S.L., Hall, J.W., Merz, B., Michel-Kerjan, E., Mysiak, J., Surminski, S. and Kunreuther, H. (2018), "Integrating human behaviour dynamics into flood disaster risk assessment", Nature Climate Change, Vol. 8, No. 3, pp. 1-8.
[2] Finucane, M.L., Slovic, P., Mertz, C.K., Flynn, J. and Satterfield, T.A. (2000), "Gender, Race, and Perceived Risk: The 'White Male' Effect", Health, Risk & Society, Vol. 2, No. 2, pp. 159-172.
[3] Flynn, J., Slovic, P. and Mertz, C.K. (1994), "Gender, Race, and Perception of Environmental Health Risks", Risk Analysis, Vol. 14, No. 6, pp. 1101-1108.
[4] Lujala, P., Lein, H. and Rød, J.K. (2015), "Climate Change, Natural Hazards, and Risk Perception: The Role of Proximity and Personal Experience", Local Environment, Vol. 20, No. 4, pp. 489-509.
[5] McMullan, C, Brown, G.D., Tully, E. and Craven, T. (2018), "Methodology, Process & Outcomes: Delivering the National Risk Assessment 2017". Emergency Management Institute Ireland. http://doras.dcu.ie/22263/1/EMII_Research_Symposium_Feb_2018.pdf Accessed 8th March 2019.

Algorithms as risk communication support tool within precision medicine

S. Mrksic Kovacevic, F. Bouder
University of Stavanger, Stavanger, Norway

The development of machine learning and artificial intelligence (AI) is leading to unprecedented possibilities in many sectors. Within medicine, the field precision medicine offers an example of high impact. Better informed decisions bear the prospect of improving health outcomes. Algorithms can be seen as one of the crucial AI tools used in the field. They have a potential of increasing efficiency both from the diagnosis and treatment perspective. With the primary aim of understanding their development, use and regulation in practice, we conducted 30 in-depth, semi-structured interviews. Our target group were experts coming from the healthcare, development and regulatory sides located in Norway, Sweden, Denmark, United Kingdom, USA, Germany and The Netherlands. Results confirm the potential of algorithms as a possible risk communication support tool. However, this does not come without certain challenges such as definitions, validity, reliability and the way they are regulated. Despite revolutionary prospects for precision medicine, there is definitely a need for improvements before making algorithms a key tool for risk-sensitive decisions and communication.

The role of experiential knowledge in climate change risk perception and decisions for adaptation and mitigation among citizens of Malmö, Sweden

K. Blennow
Swedish University of Agricultural Sciences, Alnarp, Sweden
J. Persson
Lund University, Lund, Sweden

While climate change (CC) mitigation refers to efforts to stabilize greenhouse gas concentrations in the atmosphere, adaptation is about adjusting to the (positive or negative) effects of CC [1]. Claims have been made that (1) CC mitigation action is motivated by psychologically distant concerns and beliefs about CC while (2) adaptation is motivated by proximate concerns for local CC impacts, and (3) that the effectiveness of CC communications should be framed in a global context for mitigation and a local context for adaptation [2]. Let us refer to this set of claims as the psychologically distant hypothesis - even if strictly speaking it consists of three independent claims.

Here we test the following empirical consequences of the psychological distance hypothesis, see e.g. [2]: CC mitigation and adaptation behaviour are not statistically significantly correlated, [a consequence of 1 and 2] (1); the strength of belief in having experienced the local effects of CC is statistically significantly correlated to CC adaptation behaviour, [a consequence of 2] (2); the strength of belief in having experienced the local effects of CC is not statistically significantly correlated to mitigation behaviour, [a consequence of 1] (3); the expectation of net negative local effects of CC is statistically significantly correlated with adaptation behaviour (4), and the expectation of net negative local effects of CC is not statistically significantly correlated with mitigation behaviour (5). Decisions for taking CC adaptation and mitigation action by 338 citizens of Malmö, Sweden*, were analysed using the Bayesian proportions test using a 95% credible interval [3]. We found that mitigation and adaptation decisions were statistically significantly correlated (a), that experiential knowledge was statistically significantly correlated with both adaptation behaviour (b) and mitigation behaviour (c), and that the expectation of net negative effects of CC on local values was statistically significantly correlated with both adaptation and mitigation behavior (d and e).

Hence, three of the five empirical consequences of the psychological distance hypothesis could not be corroborated by our data. That not only CC adaptation behavior but also mitigation behavior was statistically significantly correlated with the experience of local effects of CC, as well as with net negative expectations (and hence also the strength of belief in the local effects of CC) indicates that the distinction between CC adaptation and mitigation signifies something other than the psychological distance hypothesis entails. However, since the hypothesis is complex, components of it might be true. This allows for an alternative explanation, which is in agreement with the results of [4] who found that the strength of belief in the local effects of CC combined with (and not as separate entities) the strength of belief in having experienced the effects of CC are correlated with CC adaptation behavior. The alternative explanation casts additional doubt on the part of the psychological distance hypothesis, which claims that the effectiveness of CC communications should be framed in a global context for mitigation and a local context for adaptation.

References

[1] Baede, A., van der Linden, P., and Verbruggen, A. (2007) "Annex II: Glossary." In Climate Change 2007: Synthesis Report, edited by R. Pauchari and A. Reisinger, 76-99. Geneva: IPCC;
[2] Haden, V.R., Niles, M.T., Lubell, M., Perlman, J., Jackson L.E. (2012) "Global and Local Concerns: What Attitudes and Beliefs Motivate Farmers to Mitigate and Adapt to Climate Change?" PLOS ONE 7(12): e52882;
[3] Bååth, R (2014) "Bayesian First Aid: A Package that Implements Bayesian Alternatives to the Classical *.test Functions in R". In the proceedings of UseR! 2014 - the International R User Conference.;
[4] Blennow, K., Persson, J., Tomé, M., Hanewinkel, M. (2012) "Climate change: believing and seeing implies adapting". PLOS ONE, 7(11):e50181.

*The authors are grateful to the students of the 2018 Master level course "*Climate change: Landscape in transition*" at the Swedish University of Agricultural Sciences, Alnarp, for making the data collected by them available for use in the research. Participation in the survey was voluntary and the handling of the data is in agreement with GDPR.

Using NEP scale to explain public risk perception of energy technologies

A. Balžekienė, A Budžytė
Civil Society and Sustainability research group
Kaunas University of Technology, Kaunas, Lithuania

Environmental worldviews are often reported as having significant effect public perception on environmental and technological risk perception. One of the most methodologically rigorous and widely used measure of environmental orientations is New Ecological Paradigm scale (NEP), developed by Dunlap and Van Liere in 1978, and later constantly tested and revised [2]. The NEP scale was mainly used in explaining environmental risk perception, but also there are few studies using the scale to investigate the perception of energy technologies, for example, nuclear risk perception [4]; wind energy [1]; renewables [3] and else.

HEP – NEP divide (human exceptionalism vs. new ecological paradigm) in public worldviews falls in line with the rationale behind public support for non-renewable – renewable energy sources. Therefore, NEP scale could have significant explanatory power in explaining risk perception of energy technologies.

This presentation will analyze how environmental orientations in Lithuania are shaping public attitudes in energy technologies risk perception, focusing on renewables – non renewables divide. Analysis is based on the data from representative public opinion survey, conducted in autumn 2018 in Lithuania. In Lithuania, the NEP scale was not used previously in the surveys, analyzing risk perception of energy technologies, therefore this presentation could provide some new insights into the diversity of Lithuanian public attitudes.

Results indicate that pro-environmental orientations are positively and significantly correlated risk perception of some non-renewables (like coal, oil), and negatively – with risk perception of renewables (such as sun and wind power). But not all the statements of NEP scale are significant, therefore more nuanced analysis and discussion is needed.

Presentation is based on the project “Public Perceptions of Climate Change: Lithuanian case in a European Comparative Perspective” funded by a grant (No. MIP-17-126/SV3-0511) from the Research Council of Lithuania, 2017-2020

References

[1] Bidwel, D. (2013), “The role of values in public beliefs and attitudes towards commercial wind energy”, *Energy Policy*, Vol. 58, p.p. 189-199
[2] Dunlap, R.E. et al. (2000), “New Trends in Measuring Environmental Attitudes: Measuring Endorsement of the New Ecological Paradigm: A Revised NEP Scale”, *Journal of Social Issues*, Vol. 56, No. 3, 2000, pp. 425–442
[3] Ntanos, S. et al. (2019) “An Application of the New Environmental Paradigm (NEP) Scale in a Greek Context”, *Energies*, Vol. *12*(2)
[4] Witfield, S.C. et al. (2009), “*The Future of Nuclear Power: Value Orientations and Risk Perception*”, *Risk Analysis*, Vol. 29, No. 3, p.p. 425-437

Session 2

Track 4:
Risk Analysis of Cyber-Physical Systems

Developing and analyzing a digital instrumentation and control system for a safety fan

S. Sarshar, B. A. Gran
Institute for Energy Technology (IFE), Halden, Norway

The activities on Safety of Digital Instrumentation and Control Systems within the OECD Halden Reactor Project (HRP) have the overall objective to contribute to the safe development and application of Digital Instrumentation & Control (DI&C) in NPPs [1]. More complex DI&C systems often imply that these systems have many dependencies and interconnections, which challenges both safety and security. Research questions are how safety and security aspects should be designed into critical DI&C systems [2], how to address challenges experienced by the licensee and regulator in the safety demonstration of DI&C systems [3], and to explore the human and organizational aspects of undertaking a risk assessment. A challenge with research on these questions are the access to good cases. Many cases are unfortunate to simple, lack safety relevance or lacking enough information and documentation to be applicable as case.

Therefore, the HRP research on safety assurance in DI&C systems now is building competence through developing a DI&C system for a nuclear power plant. The case selected is the safety fan of the air filter system of the Halden Reactor. Since the reactor is not in operation and will be decommissioned, it now allows the project access to the analogue system currently installed and which we will digitalize. The steps include establishing a concept description, the development and safety assessment plans, system requirements specification, risk analysis and safety assessment report.

The safety fan project will provide the possibility (1) to build competence and gathering experience from the development process of DI&C system, (2) develop the case with all required documentation required for a safety demonstration, (3) explore pros and cons of applying different requirement specification methods (e.g. supported by graphical specifications), (4) explore pros and cons and assess the human and organizational aspects of risk analysis methods, and (5) apply the case as a cyber-physical system for attack in the Cybersecurity Center at IFE. The air filter system containment functionality as case is also applicable in non-nuclear domains. Similar systems and functions are required for containment of gas within a room, e.g. released gas to stop a fire or leaked gas from a tank.

References

[1] MTO Proposal for the Three-Year Period 2018-2020, HP-1490, vol. 2, (For use within the Halden Project Member Organizations only)
[2] Hauge, A.A., Katta, V., Karpati, P., Gran, B.A., 2018, Safety Demonstration – A Strategy for Assessors, in Proceedings of the 14th International Conference on Probabilistic Safety Assessment and Management (PSAM 14), September 16-20, 2018, Los Angeles, CA, USA.
[3] Hauge, A.A. and Karpati, P., 2019, Current state of safety demonstration practice internationally, HWR-1259, Enlarged Halden Reactor Programme, May 19-24, 2019, Sandefjord, Norway.

In Depth Hazards and Security Analysis for an Industrial Test Enclave for Methods Testing and Validation

J. R. Taylor, C. Chronopoulos, S. Piccolo
Technical University of Denmark (DTU), Kgs. Lyngby, Denmark
S. Sarshar, J. E. Simensen
Institute for Energy Technology (IFE), Halden, Norway

One of the challenges facing safety and security assessments is that when incident and accident investigations are made and the incident scenario described in detail, the scenario seldom matches those identified in risk analyses. There are several reasons for this. The main ones are that the hazards identified by risk analysis are usually prevented; and that the methods used for hazard identification do not sufficiently cover the range of problems which can arise in complex systems.

The OECD Halden Reactor Project has developed and constructed an industrial automation enclave [1] intended for detailed investigation of safety and security analysis methods. The installations is described as an enclave because it is isolated from possible outside influences, and more importantly, cannot affect/infect external systems when investigating security attacks.

The part of the project described here covers in depth risk analyses using methods intended for in depth safety analysis at the level where system weaknesses can exist. The methods so far tested are in deep FMEA, deep HAZID, HAZOP with lessons learned support, sneak path analysis, action error analysis of start-up and maintenance procedures, and system simulation with fault insertion for emergent hazards. Several techniques for security assessment have also been applied, including security sneak path analysis.

The studies show the extent to which completeness depends on the use of combinations of methods, and the degree of coverage which can be achieved.

References

[1] Simensen, J.E., Sarshar, S., Hauge, A.A., Olsen, S., Sechi, F. and Jørgensen P-A., 2019, Test Enclave – Technical Specification Documentation, HWR-1244, Enlarged Halden Reactor Programme, May 19-24, 2019, Sandefjord, Norway.

Demystifying Cyber-Physical Risks in Smart Building

B. Kalluri, I. Kozine
Technical University of Denmark, Kgs. Lyngby, Denmark

Today buildings in urban environment are being transformed into complex cyber-physical systems (SPCs) in the process of mitigating their impact on climate and achieving sustainability, while meeting primary goals such as providing a comfortable, productive, safe and secure environment for occupants and enterprises. These buildings typically encompass systems such as lighting, HVAC (Heating, Ventilation and Air-Conditioning), fire-safety, security etc., that seamlessly interact with business processes and their environment. Smart Buildings (SBs) are an emerging class of built-environment that tightly integrate systems, processes, and environment through Information and Communication Technologies. Integration makes SBs vulnerable to faults and failures (both deliberate and unintentional) that may lead to hazards which would eventually disrupt processes. In the horizon of Smart Buildings and Cities, addressing this open challenge is paramount.

The purpose of this presentation is to present a novel approach to develop a model which will aid risk analysts to identify potential safety hazards latent in integrated SBs. Additionally, it will enable trace their cascaded effects between building systems due to their interoperation, and eventually implement barriers to impede its overall risk. The discussion presented here is a case that argues how do we ensure robust fire protection without compromising smart capabilities of SBs?

The novelty of this approach is thus two-fold. Firstly, it develops a critical understanding of SBs by demystifying ‘what makes buildings smarter? what are their typical capabilities and dimensions?’ and further arguing whether buildings can be treated as CPSs’. Secondly, it presents a diagrammatic representation of SBs that would help risk analysts to apply knowledge from other disciplines namely reliability, risk and robustness. This study is a starting point that shall enable critical analysis of buildings in future, which are otherwise underexamined for unprecedented cyber and physical threats.

Dynamic influence diagrams for risk-based decision making for rebars

S. Rastayesh, J. D. Sørensen
Aalborg University, Department of Civil Engineering, Aalborg, Denmark

This paper presents recent contributions to the Marie Skłodowska-Curie Innovative Training Network titled INFRASTAR (Innovation and Networking for Fatigue and Reliability Analysis of Structures - Training for Assessment of Risk) to the field of reliability and risk-based approaches for decision-making in wind turbine and bridges (http://infrastar.eu/). In this paper, a risk-based framework based on a Bayesian approach is applied where a probabilistic damage evolution model is applied to assess the reliability and to plan mitigation actions, including inspection, repair, and change operation of bridge. Using dynamic influence diagrams by Bayesian networks (BNs), which relate variables to each other over adjacent time steps, decision making is carried out. Nowadays, one of the challenges in the industries is to minimize the cost of operation and maintenance (O&M) as well as inspection. [1] Two topics became popular to find the best solution in this regard: Risk-based inspection and risk-based O&M; they could be assumed as a subset of risk-based decision making. Extension of the lifetime of bridges is a significant issue for engineers as their collapse or failures could cause economic and environmental consequences. Hence, in decision-making, it is of key importance to take cost-efficient actions to avoid any failure in these structures. Decisions taken at the design stage can be updated when information becomes available on climate or traffic actions, possibly changing over time. Hence, it is an important subject for risk decision-makers to update their actions according to the real state of the structure. In other word, bridges are continuously exposing to loads which has a direct influence on their lifetime [2], results in an increased risk of failure. These environmental impacts can be due to fatigue of reinforcement steel components in a composite bridge [3,4]. In this paper, a composite bridge with steel box girder and concrete deck is assumed as a case study to investigate this issue. A risk-based framework based on a Bayesian approach is applied where a probabilistic damage evolution model is utilized to assess the reliability and to plan mitigation actions, including inspection, repair, and change operation of bridge. Using dynamic influence diagrams by Bayesian networks (BNs), which relate variables to each other over adjacent time steps, decision making is carried out. Therefore, different strategies are applied to prolong their life cycle performance using risk-based inspection and risk-based O&M. A comprehensive framework utilizing BNs is suggested for risk-based inspection and O&M planning. The decision tool is proposed to deal with structures exposed to deterioration damage over time; damage over time can be calculated using this information. The aim is to find the optimum decisions based on the cost of maintenance and inspection. Besides, this procedure can help to find the optimal time interval for maintenance and inspection. The procedure will prevent failures in the structures in order to reduce consequences caused by late inspections or maintenance as well as early ones to optimize the cost of repair and inspection. The application is presented for an illustrative example for the assumed bridge.

References

[1] Rastayesh, S., Nielsen, J. S., & Sørensen, J. D. (2018). Bayesian Network Methods for Risk-Based Decision Making for Wind Turbines. In *14th EAWE - PhD Seminar on Wind Energy* Brussel: European Academy of Wind Energy.

[2] Mankar, A., Rastayesh, S., & Sørensen, J. D. (2019). Fatigue Reliability analysis of Crêt De l'Anneau Viaduct: a case study. *Structure & Infrastructure Engineering*. https://doi.org/10.1080/15732479.2019.1633361

[3] Rastayesh, S., Mankar, & Sørensen, J. D. (2018). Comparative investigation of uncertainty analysis with different methodologies on fatigue data of rebars In *IRSEC 2018 International Reliability and Safety Engineering Conference* International Reliability and Safety Engineering Conference

[4] Mankar, A., Rastayesh, S., & Sørensen, J. D. (2018). Sensitivity and Identifiability Study for Uncertainty Analysis of Material Model for Concrete Fatigue. In *IRSEC 2018 International Reliability and Safety Engineering Conference* International Reliability and Safety Engineering Conference.

Track 5:
Risk Management for Organisations

Risk based assessment to determine contract relationships between building clients and AEC companies and the impact on innovation

J. B. Berg, C. Thuesen, P. A. Jensen
Technical University of Denmark, Department of Technology, Management and Economics, Kgs. Lyngby, Denmark

Traditionally in Europe the relationship between building clients and AEC (Architect, Engineering and

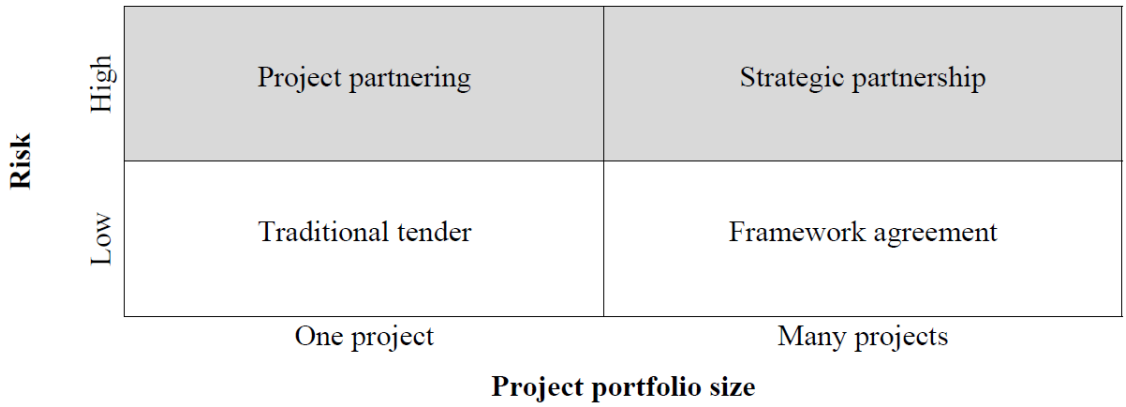
Contracting) companies have been characterized by being market based and adversarial. Having this type of relationship is one of the main factors that leads to conflicts and a low degree of innovation, which are characteristics of the construction industry,[1].

As a reaction to this perceived problematic situation, a number of new contract types have emerged in the last couple of decades, which broadly can be categorized as relational contracts. This contract type enables the building client to get early involvement of the AEC firms, make a holistic risk assessment, and create positive cross company incentive schemes. These mechanisms are very important especially when dealing with a project with a certain degree of uncertainty [2].

The cost and complexity of implementing these relational contract types have to be justified in terms of risk reduction and potential innovation gains. This is why relational contracts like project partnering or Integrated Project Delivery are less elaborate, and are suited for single projects. Strategic Partnerships have its strengths, when the portfolio of projects is large and projects are similar in scope or type.

It can be a very complicated task to evaluate, which contract type is the most suited for a given project or portfolio of projects and a great number of variables have to be considered. Chief among these variables is risk. In figure 1, an example of risk plotted against portfolio size has been made in a simple matrix decision chart. Since innovation in construction often involves changing the risk profile of a project, such decision matrices can help visualize, which contract type would be most appropriate.

Figure 1 Simple matrix decision chart to evaluate contract relationship between building client and AEC companies based on risk and portfolio size. (Relational contract types in gray)



References

[1] B. Colledge, “Relational Contracting – Creating Value Beyond the Project,” Lean Constr. J., vol. 2, no. April, pp. 30–45, 2005.
[2] O. E. Williamson, “Transaction-Cost Economics: The Governance of Contractual Relations,” J. Law Econ., vol. 22, no. 2, 1979.

Prevention of dust exposure in demolition work in Denmark– a participatory approach intervention

S. Grøn
Technical University of Denmark, Department of Technology, Management and Economics, Innovation, Kgs Lyngby, Denmark
H. J. Limborg, A. Kabel
TeamArbejdsliv, Valby, Denmark
P. Kines
The National Research Centre for the Working Environment, Copenhagen, Denmark

Risk of exposure to silica dust is a well-documented health risk for construction workers, particularly in demolition. Despite effective exposure prevention measures, silicosis and Chronic Obstructive Pulmonary Disease (COPD) continues to be a widespread disease among these workers. This is partly due to the tasks and materials they deal with combined with factors such as a low degree of regulation and guidelines, as well as turbulence with subcontracting labour. An intervention program was developed and pilot tested to prevent demolition workers from exposure to silica dust using a participatory approach, based on the principles for knowledge transfer and exchange. The program was developed in collaboration with the demolition industry partners, stakeholders from participating companies and demolition crews at a total of nine sites. Experiences were documented from on-going meetings and semi-structured interviews. A ‘dust reduction’ tool was developed whereby site specific plans were drawn up and implemented based on an audit, a safety conditions- and behaviour observation method, and a template for briefings (toolbox talks) for the demolition teams. The participating companies found the tool useful, however, the motivation to further use the tool varied greatly, depending on organizational level. The most difficult group to motivate was the demolition crews due to issues related to the fragmentation of the labour force within the industry. The management level group found that in order to continue to use it the tool, they would need to be able to integrate it in their safety management systems and find support from guidelines and regulations developed specifically for demolition work.
We conclude that providing a method to nurture a dust prevention culture in demolition companies could be a valuable part of a coordinated multisectoral strategy. This strategy could include developing relevant and coherent regulations enforced by the work authorities or the industry bodies.

Exploring the practical impact of municipal risk assessments through a longitudinal study of individual and organizational learning

A. Cedergren, H. Hassel
Centre for Critical Infrastructure Protection (CenCIP), Lund University, Sweden

Risk assessments are routinely conducted in a wide array of different organisations with the aim of reducing potential future losses. While significant research has been devoted to the theoretical underpinning of the concept of risk, less attention in the research community has been paid to exploring the practical impact of risk assessments. This contribution draws on a three-year longitudinal study investigating to what extent learning among those involved in the process of conducting municipal risk assessments have taken place. The municipality of Malmö, Sweden, is used as an empirical case, where a risk assessment method that integrates principles from risk management as well as continuity management has been developed and implemented. The risk assessment process is decentralised and each municipal department is responsible to conduct the assessment with a common method and guideline as a point of departure. Data collection was conducted by using questionnaires distributed to the practitioners once every year during the three-year period. In addition, workshops and interviews with preparedness planners have been conducted. The study explores how preparedness planners in the municipality view the way individual as well as organisational learning has occurred in terms of, for example, their understanding of risks and vulnerabilities and commitment among staff and leadership. The results show that there has been a general positive trend in terms of learning among those directly involved in the risk assessment process. For example, they demonstrate a perception of increased risk awareness. However, commitment among leadership did not seem to be equally promising. Moreover, as the results of the risk assessment so far have not been aggregated across departments, preparedness planners did not perceive that lessons were shared between municipal departments. Finally, the study concludes that general challenges to achieve learning include high staff turnover and lack of continuity of the risk assessment process.

Learning and Risk Management Practices in Engineering Design Teams of Innovative Projects

A. Shafqat, T. Welo
Norwegian University of Science and Technology, Trondheim, Norway
J. Oehmen,
Technical University of Denmark, Copenhagen, Denmark

Companies strive to seek technological advancement and growth. In order to outperform their competitors, companies both try to introduce new products or improve existing ones. At the same time, the companies struggle to optimize the lead-time, quality and cost of the product development projects [2, 1]. Product development process (PDP) faces uncertainty and risks including technical risks, schedule risks, financial risks and marketing risks [4], due to the nature of product development. In the design phase of the PDP, engineering design teams face uncertainty, problems to solve and technology limitations. As a result, the design teams continuously acquire knowledge and learn through various learning strategies. Consequently, they ultimately improve the efficiency of the PDP outcomes. In problem solving, the team do experiments, make prototypes and conduct past product reviews. They learn by doing, learn from failures and incidents and learn from teammates and coaches. Sometimes they outsource tasks which they need to coordinate [3].

In product development projects, however, the problem solving process in which engineering design teams try to find the best possible solutions commonly results in cost or time overrun. This study presents a research framework that helps understand the link between learning strategies, cost-of-learning and risk management in engineering design phase of PDP. To reduce the cost-of-learning through risk management, the research framework proposes an approach suitable to design engineers.

We explore the possible explanation to inefficiency in the PDP by focusing on the design teams, their learning strategies to solve the design problems as well as their risk management practices to identify the main design issues. We conduct interviews with project managers and design engineers in innovative and growing engineering firms in Denmark. We find that design teams were focusing on only one learning (probing) strategy to mitigate risks and find solutions for their design problems. Moreover, risk management practices were not identified as a priority of the design teams.

References

[1] Chauhan, A. S., Yadav, O. P., Soni, G. and Jain, R. (2017) “A holistic approach to manage risks in NPD process”, *in Reliability and Maintainability Symposium (RAMS)*, 2017 Annual, IEEE, 1-5. https://doi.org/10.1109/ram.2017.7889796

[2] Oehmen, J., Olechowski, A., Robert Kenley, C. and Ben-Daya, M. (2014), “Analysis of the effect of risk management practices on the performance of new product development programs”, *Technovation*, 34(8), 441-453. https://doi.org/10.1016/j.technovation.2013.12.005

[3] Shafqat, A., Oehmen, J., Welo, T., & Willumsen, P. (2019), “The Cost of Learning from Failures and Mistakes in Product Design: Reviewing the Literature” *Proceedings of the Design Society: International Conference on Engineering Design*, 1(1), 1653-1662. doi:10.1017/dsi.2019.171

[4] Wu, J. and Wu, Z. (2014), "Integrated risk management and product innovation in China: The moderating role of board of directors", *Technovation*, 34(8), 466-476. https://doi.org/10.1016/j.technovation.2013.11.006

Track 6:
Software Tools for Risk Analysis

SafetyBarrierManager, a tool for safety-barrier diagrams and bowties

N. J. Duijm
Nicestsolution, Jyllinge, Denmark

Since the implementation of the first European Directive on Major Accident Hazard Control in Denmark, late 1980ies, the concept of safety barriers and safety-barrier diagrams has been popular in this country. The idea to consider hazard controls as “barriers” is probably universal, and the idea of displaying the combined effect of those controls graphically was probably born in several places independently from each other. Nowadays “Bowties” are the most common way of graphical representation of hazard controls.

Initially safety-barrier diagrams were drawn by hand or using general spread sheet tools. After completion of the “ARAMIS” project by 2006, Risø National Laboratory felt the lack of a more dedicated tool and started to develop “SafetyBarrierManager”. This tool builds on the concepts of the Danish tradition of drafting safety-barrier diagrams, as well as the “Bowtie” ideas from “ARAMIS”, i.e. a strong link with fault tree and event tree techniques. It uses the techniques for quantifying fault trees as were developed at Risø National Laboratory in the previous decades.

The presentation will discuss the ideas behind SafetyBarrierManager, such as graph theory, scenario-based thinking, and the distinction between front-line barriers and underlying safety-management tasks. Some features will be demonstrated, such as enforcing the use of “complete” barriers, and how graphical elements create direct access to comprehensive background information that can be made available to all stakeholders.

References

[1] Duijm, N.J. (2017) “SafetyBarrierManager, a software tool to perform risk analysis using ARAMIS's principles,” in Bernatik, C., Huang, C., Salvi, O. (Ed.), Risk Analysis and Management – Trends, Challenges and Emerging Issues: Proc. of the 6th Int. Conf. on Risk Analysis and Crisis Response (RACR 2017). CRC Press, 2017. p. 253-259.

[2] Duijm, N.J. (2009). “Safety-barrier diagrams as a safety management tool”, Reliability Engineering and System Safety, Vol. 94, No. 2, pp. 332–341.

HAZEX – A Tool for Semi-automated Hazards Analysis for Process Plants, Cyber-physical systems and Human Activities

J. R.Taylor
Technical University of Denmark, DTU Management Engineering

HAZEX was originally developed as a support tool for Haazard and Operability Analysis for 40 oil and gas plants in Venezuela. The semi-automatic version was soon found to be necessary for quality control of the HAZOP studies made to satisfy the Major Hazards Directive (Seveso Directive) [2]. The method used was to represent all HAZOP records as event sequence diagrams, and to encode them as event sequence statements in an event language ELAN. This can be used to as a textual method for storing and manipulating fault trees, cause consequence diagrams and Bayesian networks.

The semi-automation for a long time involved just using existing HAZOP analyses as check lists for hazards for different equipment types. The analyst team was presented with possible hazardous event causes and asked to say whether these could be relevant for the actual case, and similarly for consequences and safeguards. The check lists are arranged hierarchically, so that large classes of hazards could be excluded by anwering just one question in the negative. The analysis team could at any time add further hazards and consequences. In this way the check list of hazards was gradually extended. This approach has been used in 103 major risk analysis projects and has therefore collected a very large range of experience [3].

Extended studies were made of the completeness of hazard identification using HAZEX as a tool to check professionally made HAZOP studies . One of the extensions made was to allow rapid look up of “Lessons Learned” from accident reports, and retrieval of relevant photographs from earlier incidents. Facilities for Action Error Analysis were also added [4].

Later, facilities for automated analysis of event propagation were added [1, 5], based on diagram input such as piping and instrumentation diagrams, circuit diagrams, functional block diagrams and various finite state diagram representations using libraries of generic component models. This has proved useful in analyzing cyber-physical systems and organizational systems. As a research tool the program has proved very useful in allowing various hazard identification methodologies to be tested without the confounding factor of the experience of the individual analyst.

References

[1] Taylor, J. R., (1982), An algorithm for fault tree construction, IEEE Trans Reliability, R-31: 137
[2] Taylor JR, Vangsted, E, (1992), A comparative evaluation of safety features based on risk analysis for 25 plants, 7th Int Symp on Loss Prevention and Safety Promotion in the Process Industries, AIDIC
[3] Taylor JR (2012) Lessons learned from forty years of HAZOP, Loss Prevention Bulletin 227 October 2012
[4] Taylor JR (2016), Human Error in Process Plant Design and Operation, CRC Press
[5] Taylor JR (2017) Automated HAZOP Revisited, Process Safety and Environmental Protection 1 1 1 pp 635–651
[6] Taylor JR (2019) HAZEX Users Manual

HUGIN Software for Risk Analysis

A. L. Madsen, N. Søndberg-Jeppesen
HUGIN EXPERT A/S, Aalborg, Denmark
Department of Computer Science, Aalborg University, Denmark
F. Jensen
HUGIN EXPERT A/S, Aalborg, Denmark

HUGIN is a software package for Bayesian networks and influence diagrams (also known as probabilistic graphical models) [1,2]. Bayesian networks and influence diagrams are intuitive graphical models for reasoning and decision making under uncertainty [3] that have a number of key features that make them excellent tools for risk analysis. These features include the ability to combine data and knowledge into a single model representation, the same model supports root cause analysis and prediction, due to their graphical nature the models are easy to communicate, the models compute with missing values, calculations are often very efficient, and the models can be constructed incrementally and reuse of sub-models is supported through an object-oriented paradigm.

Due to their nature of managing uncertainty, Bayesian networks and influence diagrams have been applied for risk analysis in a wide range of different domains ranging from medical risk prediction [4] over prediction of default risk for large corporates [5] and maneuver recognition as part of risk analysis in autonomous driving [6] to risk analysis on ship collisions [7].

This presentation will by example introduce the concept of Bayesian networks and influence diagrams using HUGIN software. HUGIN software is a complete package of tools for developing, deploying and maintaining Bayesian network and influence diagram models. It has an intuitive Graphical User Interface (GUI) available for a number of different software platforms as well as a set of Application Programming Interfaces (APIs) to the HUGIN Decision Engine (DE) for major programming languages (there are, for instance, APIs for C, C++, C#, Java and python) as well as libraries for handheld devices. The HUGIN DE is designed for integration of Bayesian network and influence diagram functionality into existing IT platforms using APIs. The software has been available since 1989 and is being used by both small and large companies as well as universities and research institutions world-wide.

The presentation will use the HUGIN GUI to demonstrate a number of Bayesian network and influence diagram models developed for real-world problems related to risk analysis.

References

[1] Madsen, A. L., Jensen, F., Kjærulff, U. B., Lang, M. (2005). The HUGIN Tool for Probabilistic Graphical Models, International Journal of Artificial Intelligence Tools 14 (3), pages 507-543.
[2] Madsen, A. L., Lang, M., Kjærulff, U., and Jensen, F., (2003), The Hugin Tool for Learning Bayesian Networks, Proceedings of The Seventh ECSQARU conference, pages 549-605.
[3] Kjærulff, U. B. and Madsen, A. L. (2013), Bayesian Networks and Influence Diagrams – A Guide to Construction and Analysis, Springer. Second Edition.
[4] Ward, L., Paul, M. Andreassen, S. (2017). Automatic learning of mortality in a CPN model of the systemic inflammatory response syndrome, Mathematical Biosciences, Vol. 284, 2017, pages 12-20,
[5] Ejsing, E., Vastrup, P. and Madsen, A. L. (2008), Probability of default for large corporates, in O. Pourret, P. Naim, B. Marcot (eds), Bayesian Networks: A Practical Guide to Applications, pages 329-344.
[6] Weidl, G., Madsen, A.L., Wang, S., Kasper, D., Karlsen, M. (2018), Early and accurate recognition of highway traffic maneuvers considering real world application: a novel framework using Bayesian networks, IEEE Intelligent Transportation Systems Magazine 10 (3), pages 146-158.
[7] Hansen, P. F., Pedersen, P. T. (1998), Risk Analysis of Conventional and Solo Watch Keeping Kgs. Lyngby, Denmark, Technical University of Denmark, 61 pages.

Value creating Risk Management with RamRisk

J. Pedersen
Head of Department, Ramboll, Copenhagen, Denmark

The purpose of risk management is to handle uncertainties by reducing threats and promoting opportunities. RamRisk is a web-based solution specifically designed to do this in a timely manner. This is crucial for any organisation and essential for the successful outcome of all projects. RamRisk complies fully with ISO 31000 – 'Risk management – Principles and guidelines.'

The user-friendly interface enables all team members to describe, categorise, evaluate and handle the risks of your projects or organisation. RamRisk makes it easier to collaborate on risk and helps to put risk on the agenda. RamRisk is accessible 24/7 from any browser on your PC or mobile device.

In the presentation we give an introduction to RamRisk and how it is used by many clients in value creating risk management processes.

References

[1] www.ramrisk.com

Track 7:
Risk Analysis of Critical Infrastructure

The role of regional airports for sustainable development and crisis management – A Swedish case study

C. Große, P.M. Olausson, B. Svensson
Risk and Crisis Research Centre – Mid Sweden University, Sundsvall/Östersund, Sweden

Transportation by air provides crucial functionalities to industry, retail, public services and the daily life of people, which includes not only travel to work and back but also business trips and tourism. Aviation supports supply chains of goods and public services and particularly those which are of time-critical importance and rely on transports by air. Sweden's geographic conditions attribute an important role to transportation by air in order to bridge the often large distances within the country and to reach out to Europe or intercontinental destinations. Regional airports provide thereby a vital basis infrastructure for aviation. However, regional airports have to content with economic requirements and geopolitical discussions with regard to green gas emissions. Such tensions can result in shutdowns of municipality-owned and operated airports, which in turn affects the surrounding region.

The aim of this study is to explore the diversified roll that a regional airport plays in society, both for the surrounding area and for crisis management. In general, this study has focused on regional airports in Sweden and, in particular, on the Sundsvall-Timrå-Airport. The data collection and analyses comprised material from a literature review as well as a policy analysis. Furthermore, it includes several interviews with local stakeholders, an observation of a regional collaboration exercise among land-based and air-based rescue forces, and a workshop with participants representing public and private actors. Besides stakeholders from two airports in the middle of Sweden, the study includes perspectives that represent several interests including local and regional crisis management, health care, university education, infrastructure development, sustainable development, prison and probation service, large industry, medium-sized manufacturers, tourism and a voluntary organization of flying forces.

This study demonstrates that the essential role of regional airports for society's resilience is constantly overlooked. It contributes to give a nuanced picture of the Swedish case that illustrates the various stakeholder interests with respect to the functionality of a regional airport. The results of the literature review indicates that common approaches for estimating the effects of airports on the regional economy have neglected the impact of regional airports on risk reduction, resilience and crisis management. The analysis of Swedish policies has recognized this ignorance. However, the participants have emphasised the importance of reliable airports for ambulance transports, rescue services and crisis management for example in the context of wildfires such as those that occurred in Sweden in summer 2018. This study encourages a broader discussion with regard to aviation that also reflects on issues related to risk management and the protection of critical infrastructure.

Towards cross-sector risk management in Swedish critical infrastructures

T. R. Sonesson
Division of Risk Management and Societal Safety, Lund University, Sweden

Modern societies have come to depend on certain vital services, such as electricity, transportation and information, and a loss of their continuous supply would affect the modern citizen far more than his or her 19th century counterpart [1]. Past disruptive events have, furthermore, highlighted the existence of dependencies between the systems that sustain these services, commonly referred to as critical infrastructures [2]. As a consequence, a disruption in one infrastructure system might propagate to others through, so called, cascading effects enhancing its overall consequences [4].

Due to these cascades, and processes such as fragmentation and privatization, the infrastructures involved in such a disruption are, furthermore, governed by a large number of heterogenous – public and private – actors with sometimes conflicting goals [3]. Consequently, while society has grown more vulnerable to infrastructure disruptions, the infrastructure systems and governance situation has also grown to be more complex. To describe convincingly the overall societal effects of a critical infrastructure disruption, their dependent behavior must be considered, and, preferably, incorporated in a joint cross-sector risk management process.

As a step towards enabling this end goal. A system-of-systems model of two Swedish national critical infrastructures, namely the national power transmission system (PTS), and an electricity-dependent national backbone information and communication system (ICS), has been constructed. A generic modelling approach was chosen. It extends on current topological approaches by incorporating capacity flow constraints to capture the salient properties of technical infrastructures. This approach allowed us to populate the model using real-life data, and reduce the computational cost of the simulations.

The model was used to perform a number of disruption simulations. From the simulations we found that, the dependent ICS deteriorate far more rapidly than in the non-dependent case. Consequently, the dependency from the ICS to the PTS increases its vulnerability substantially. Furthermore, when disturbing solely the PTS components, we saw an asymmetry between the magnitude of the consequences in the two systems where the consequences to the ICS was generally higher than for the PTS.

These results highlight that the vulnerability issues seen in previous studies are also prevalent in a Swedish infrastructure context. Future research will study these issues further, by adding more infrastructures to the model, and by applying a more decision-centered approach to better connect the simulation results to the real governance situation that they aim to inform. Applying this governance lens to the very technical modelling and simulation approach is a rather novel approach that can contribute to the field.

References

[1] Boin, A., Lagadec, P., Michel-Kerjan, E., & Overdijk, W. (2003). "Critical infrastructures under threat: Learning from the Anthrax scare". *Journal of Contingencies and Crisis Management*, 11(3), 99–104.

[2] Buldyrev, S. V, Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). "Catastrophic cascade of failures in interdependent networks". *Nature*, 464(7291), 1025–1028.

[3] Cedergren, A., Lidell, K., & Lidell, K. (2019). "Critical infrastructures and the tragedy of the commons dilemma: Implications from institutional restructuring on reliability and safety". *Journal of Contingencies and Crisis Management*, 1–11.

[4] Johansson, J., & Hassel, H. (2010). "An approach for modelling interdependent infrastructures in the context of vulnerability analysis". *Reliability Engineering and System Safety*, 95(12), 1335–1344.

Fault Tree Analysis supporting water balance management in enrichment plants

R. Molarius
VTT Technical Research Centre of Finland, Tampere, Finland

In mining sites related enrichment plants, the management of waters poses a significant threat for the company in terms of environmental risks, or major accidents [1]. In enrichment plants, a mass of water is needed for aqueous extraction of metals and other mining processes. These waters include extraction chemicals as well as different kinds of metals and heavy metals from the rock even if there is a trend to use non-toxic extraction processed for bioleaching [3, 4]. The most forward-looking companies have put into operation the water balance models to ensure the wise and environment-friendly water management. These models help companies in balancing water use; in water negative areas where it rains less than evaporates, this means optimizing water recycling, and in water positive areas, such as Scandinavian where it rains more than evaporates, it helps in cleaning and removing waters from ponds and processes by the most acceptable way.

The water balance models are good tools to manage waters, but they can also be used in anticipating the environmental or major risks at the production plant. However, this needs more specific models than generally used in the enrichment plants.

This presentation provides a view of risks that are not easily noticed nor managed by water balance models in water positive areas, today. These risks were identified by using the What-if and Fault Tree Analysis [2] in a Scandinavian enrichment plant. The research pointed out that to manage all water risks it is important that the companies shall not trust with eyes closed that water balance models solve all their water related challenges.

The study was a part of the SERENE project that has received funding from European Institute of Innovation and Technology (EIT), a body of the European Union, under the Horizon 2020, the EU Framework Programme for Research and Innovation.

References

[1] Azam, S. and Li, Q. (2010). Tailings dam failures: a review of the last one hundred years. *Geotechnical News*, 28,4, 50-54.
[2] Haimes, Y. Y. (2005). *Risk modeling, assessment, and management* (Vol. 40). John Wiley & Sons.
[3] Hilson, G. and Monhemius, A. J. (2006). Alternatives to cyanide in the gold mining industry: what prospects for the future? *Journal of Cleaner production*, 14, 12-13, 1158-1167.
[4] Puhakka, J. A., Kaksonen, A. H. and Riekkola-Vanhanen, M. (2007). Heap leaching of black schist. *Biomining*, 139-151. Springer, Berlin, Heidelberg.

Session 3

Track 8:
Risk Management for Organisations

Balancing speed and precision in risk management

F. B. Helweg-Larsen
Expert Director, Risk & Security, Devoteam A/S, Copenhagen, Denmark

Identifying, assessing and deciding on risk in information systems is a challenge for most organizations. Risk Management frameworks like NIST [3] provide guidance for the basic process and are widely used in government and private organizations.

While the process is generally sensible and provides a good workflow, the decision process involving people and their often-limited knowledge of the likelihood of a risk, cleated a huge challenge. The questions asked in most risk assessments are very difficult to answer a often assumes a level on insight that is not available. This is where people start guessing.

The psychology of decision making and behavioral economics, as described by Kahneman [1] and Ariely [2], document the irrationality that takes place when people have to make complicated decisions with little time available. To ensure that the data in risk management are valid and usable, it is essential that the psychology of decision making is taken into account and incorporated in the workflow. Some individuals should make quick and simple decision with focus on speed and other should make rational decisions focused on precision.

Kahneman [1] describes the very poor abilities to determine risks and potential outcomes, even by skilled professionals, and one should be careful when calculating and aggregating risks based on very uncertain assessments.

Simplicity, decision and actions should be essential ingredients in risk management. All humans have an urge to control uncertainty, but we should recognize the fact that we sometimes have no idea about the materialization of a risk. “I don’t know” is term that is rarely used in risk management, but one that can be very accurate.

This talk will also cover the subject of digitalization and automation of risk management processes in order to create a smoother workflow that can involve stakeholders in different ways without using massive resources on communication and exchanging spreadsheets over e-mail.

The transparency and efficiency that workflow systems can provide is in itself an important tool for risk management, as it can help you balance speed and precision in your process. These workflow systems are often referred to as *Enterprise Service Management* and are available in most larger organizational, often used for incident management in it department. However, the use of systems like these are evolving rapidly.

This talk will combine the theory of Kahnemans [1] system 1 and system 2 thinking, the irrationality in the way we make decision described by Ariely [2] and the practical use of these theories in risk management, supported by technology.

References

[1] Kahneman, D. (2018), *Thinking, Fast & Slow*, Farrar, Straus & Giroux Inc, New York, United States
[2] Ariely, D. (2009), *Predictably Irrational*, HarperCollins Publishers, London, United Kingdom
[3] Joint Task Force (2018), *Risk Management Framework for Information Systems and Organizations*, National Institute for Standards and Technology, Maryland, USA

Sustainability risk management (SRM) - a necessary perspective for companies of tomorrow: A tool to map the SDGs with the company's risk impact and identify its sustainable risk profile

A. Find
CEO and senior director, Projektrisikostyring.com, Roskilde, Denmark
N. Foxby-Jacobsen
CEO and senior adviser, Blue Tree ApS, Hellebæk, Denmark

Companies today have to relate to a number of emerging challenges that can have significant impact on their business e.g. digital transformation, disruption of business models, resource constraints, climate and environmental pressures. They all result in at increasing number of risks as threats and opportunities that companies must deal with to ensure their profitability or even survival. In 2015 the challenges that focus on environment, social or economic aspects where addressed in UNs Sustainable Development Goals (SDGs). This make the goals both relevant and useful for all companies to address.
Today most companies find that sustainability risk can lead to significant impact on business, and that this perspective are not adequately addressed in traditional enterprise risk management (ERM). The lack of tools makes it difficult for companies to conduct a comprehensive risk assessment. This is further reinforced by the complexity of the SDGs with the wide number of sub-targets and indicators, and that these are not fully translated into a Danish context. In addition, many companies also find it difficult to assess which areas of action are needed to mitigate in relation to the SDGs. So, a risk assessment of a company's impact on the SDGs will supplement the existing risk assessment with an important component. This drives innovation and enhance actions that support circular economy solutions.
To address these challenges and opportunities for companies we have developed a tool called; Sustainability Risk management tool (SRM tool). It helps companies conducting a systematic sustainably risk assessment and suggest relevant mitigation actions. The target group is small and medium-sized (SME) companies. The values for the company are a systematic data-based analyses of their sustainable risk profile. The method is based on the company's product cycle and value chain mapped against the SDGs, and a prioritizing of the identified impact areas and risks (level 1). The mapping is used to identify relevant improvement action (level 2). These suggestions are based on best practice recommendations. The risk method used is based on the international risk management standard "Management of Risk" (M_o_R) and the ISO 31000 standard. The SRM tool leads the company through questions about their shareholders, consumption and behavior
patterns, control impact etc. to determine their impact profile. The model also takes into account external contextual factors, such as political stability, social and infrastructural development. The finding can document the company's action plan on sustainability, and monitor the risk pictures development over time. The risk impacts and actions should be disclosed in the company's sustainability report, and included in the companies ERM. The tool is in a POC (proof of concept) version with focus on level 1 of the risk assessment. Recommendations on actions will comes in a later version. The long-term perspective for the tool is that it can share sustainable risk data map to the SDGs across companies and industries to validate what risks companies typically encounter and which areas of actions are most effective. We are in the phase of testing the SRM tool level 1 and are looking for companies that are interested in participating in the test.
We would like to participate in a poster presentation and if possible, also in a of presentation of the tool.

References

[1] Axelos, "Management of Risk", Global risk Management Best Practice Standard, 28-08-2019, https://www.axelos.com/best-practice-solutions/mor
[2] ISO Organization, "ISO Risk Management Standard 31000", 28-08-2019, https://www.iso.org/iso-31000-riskmanagement.html
[3] Raworth, K. (2017), "Doughnut Economics", Random House Business, New York.
[4] WBCSD (2017), "Sustainability and enterprise risk management", pdf, WBCSD, 28-08-2019. https://www.wbcsd.org/Programs/Redefining-Value/Business-Decision-Making/Measurement-Valuation/Resources/Sustainability-and-enterprise-risk-management-The-first-step-towards-integration#

Applying the concept of Actuality to Project Risk Management

P. Willumsen, J. Oehmen,
Technical University of Denmark, Copenhagen, Denmark
T. Welo,
NTNU, Trondheim, Norway
M. Rossi,
Polytecnico di Milano

On the one hand, studies on project risk management (RM) yield contradictory and incomplete results regarding risk management's impact on project success [3, 4, 7]. There is a discrepancy between theory and practice of project risk management [1] and Kutsch and Hall [6] argue that despite a great deal of work towards prescriptive risk management guidelines, little work exists to reveal what risk management is actually done (or not done) by project managers, and why.
On the other hand, the management of risk is not limited to the risk management processes (De Carvalho and Rabechini Junior, 2015) and when researchers study only the formalized risk management process they often leave out important aspects which also serve to manage risk in practice [7] . This research addresses both observations by applying a theoretical lens of actuality from project management studies [2, 5] to the study of project risk management. Actuality research considers both implicit and explicit factors and the interrelationship and inseparability between agency and structure in the context, rather than considering them as discrete and detached from each other [2]. This study contributes a literature review and empirical study in line with actuality research and incorporates a multi-method qualitative in-situ approach to data collection including case studies, action research and observations. Additionally a sense-making framework is conceptualized regarding the actuality of managing risk in projects. The primary categories in the framework are formal explicit RM, formal implicit RM, informal explicit RM and informal implicit RM.
The literature review reveals that very few studies follow approaches in line with actuality. The majority of articles reviewed addresses explicit formalized RM and does not follow empirical approaches in line with actuality research. Risk management researchers often leave out many compounding factors, thus making their results incomplete and questionable for a practitioner who might be in a context where the best practices do not apply. The empirical study reveals how formal, informal, explicit and implicit project risk management work in concert and provides a holistic picture of how risks are managed in engineering projects. The case studies and cross sectional interview study present contextual accounts of risk management activities in practice – it varied in each case what processes served to manage risk, formally as well as informally. Practitioners considered the management of risks to be addressed by much more than the formal risk management process, yet this is often not a focus of risk research.

References

[1] Ahlemann, F., El Arbi, F., Kaiser, M.G., Heck, A., 2013. A process framework for theoretically grounded prescriptive research in the project management field. International Journal of Project Management 31, 43–56. https://doi.org/10.1016/j.ijproman.2012.03.008
[2] Cicmil, S., Williams, T., Thomas, J., Hodgson, D., 2006. Rethinking Project Management: Researching the actuality of projects. International Journal of Project Management. https://doi.org/10.1016/j.ijproman.2006.08.006
[3] De Bakker, K., 2011. Dialogue on risk - Effect of project risk management on project success.
[4] De Carvalho, M.M., Rabechini Junior, R., 2015. Impact of risk management on project performance: The importance of soft skills. International Journal of Production Research 53, 321–340. https://doi.org/10.1080/00207543.2014.919423
[5] Hällgren, M., Söderholm, A., 2011. Projects-as-practice, in: The Oxford Handbook of Project Management. p. 512. https://doi.org/10.1093/oxfordhb/9780199563142.003.0022
[6] Kutsch, E., Hall, M., 2009. The Rational Choice of Not Applying Project Risk Management in Information Technology Projects. Project Management Journal 40, 72–81. https://doi.org/10.1002/pmj.20112
[7] Willumsen, P., Oehmen, J., Stingl, V., Geraldi, J., 2019. Value creation through project risk management. International Journal of Project Management. https://doi.org/10.1016/j.ijproman.2019.01.007

3 reasons why every business plan on the planet ignores risks and how to fix it

A. Sidorenko
RISK-ACADEMY, Malta

Three reasons why every business plan on the planet ignores risks and how to fix it: Jensen's inequality, cognitive biases and risk psychology and poor integration of risk management. Alex will present mathematical proof collected globally over the last 100+ years explaining why every business plan, every strategy, every budget in the world is actually much riskier than presented to the shareholders. The methodological and psychological mistakes are so great, no wonder many companies fail to deliver on stakeholder expectations.

In the second part of the presentation, Alex will show how using simple risk management tools like decision trees, influence diagrams, scenarios and simulations can significantly improve the quality of decision making, planning and performance management. This will be an eye opening and very interactive session.

Learning Objectives:

1. Understand methodological limitations in planning and decision-making and learn how to overcome them through better risk management
2. Understand psychological limitations in planning and decision-making and learn how to overcome them through better risk management
3. Learn how to present insights from risk analysis to decision makers helping them change their decision-making habits

References

[1] Decision Quality: Value Creation from Better Business Decisions by Carl Spetzler, Hannah Winter, and Jennifer Meyer
[2] The Failure of Risk Management: Why It's Broken and How to Fix It by Douglas W. Hubbard
[3] The Flaw of Averages: Why We Underestimate Risk in the Face of Uncertainty by Sam L. Savage and Jeff Danziger
[4] Foundations of Decision Analysis by Ronald A. Howard and Ali E. Abbas
[5] How to Measure Anything: Finding the Value of Intangibles in Business by Douglas W. Hubbard
[6] An Introduction to Bayesian Inference and Decision by Robert W. Winkler
[7] Risk Savvy: How to Make Good Decisions by Gerd Gigerenzer
[8] Thinking, Fast and Slow by Daniel Kahneman

Track 9:
Uncertainty Assessment

A Bayesian Belief Network approach to incorporate stakeholders' values into environmental risk assessment

A. Lehikoinen, M. Laurila-Pant
University of Helsinki, Ecosystems and Environment Research Programme. Helsinki, Finland
S. Mäntyniemi, R. Venesjärvi
Natural Resources Institute Finland, Helsinki, Finland

Ecosystems are under accelerating pressure caused by multiple human activities that may have additive impacts due to various social-environmental feedback loops. To minimize the overall harm caused, wise allocation of those activities is needed. Environmental risks arising from the anthropogenic pressures result from the probability and magnitude of the unwanted effects to the environment, combined with how harmful these effects are seen. However, the definition of harm or utility is always perspective-dependent. Therefore the risk management decisions should be evaluated across sectoral boundaries, acknowledging the diversity of ecological and social values in the same analytic framework. People's commitment to environmental management decisions may affect the level on which the new regulations and rules are followed, thus further affecting the effectiveness of the management. Commitment of the stakeholders can be increased by involving them into the planning and decision-making processes. However, combining multiple views and reaching group consensus is often challenging as the preferences and values vary between and even within divergent stakeholder groups.

We present a sequential probabilistic approach to analyse the stakeholders' values and include them in formal risk assessment and decision support [1]. We used Bayesian inference to estimate population parameters for stakeholder groups, based on random samples of value judgements by individuals. The approach allows quantification of the variability in views among and within stakeholder groups. Resulting parameter distributions were then used to populate a discrete graphical BBN, to summarize and visualize the information and to link it to a larger decision analytic influence diagram (ID). As part of an ID, this BBN element serves as a distribution-form definition of the level of harm or utility associated to probabilistic changes in the states of the target variables (ecosystem attributes) following to implementation of alternative management strategies. This way the ID finds the solution that, given the prevailing knowledge and uncertainties, represents the formally optimal compromise in the presence of potentially conflicting objectives. The ID can also be used to analyse, whether the differences in the views of the participating stakeholders actually change the ranking order of the alternative management strategies or not.

The presented approach provides the managers important information about the views of the stakeholders: how the stakeholders perceive the harms and utilities and how this should be acknowledged in the management process. We also suggest that besides the direct involvement in the formal risk assessment and decision analysis, the presented approach has potential to improve the stakeholders' understanding on the system that generates the risks. In addition it can inform the groups about each other's thinking and support discussions. Thus we believe our approach can remarkably facilitate the stakeholders' involvement in different stages of the risk assessment and management process and this way increase their willingness to commit to the final decisions.

References

[1] Laurila-Pant, M., Mäntyniemi, S., Venesjärvi, R., & Lehikoinen, A. (2019, In press). Incorporating stakeholders' values into environmental decision support: A Bayesian Belief Network approach. Science of the Total Environment Vol. 697. https://doi.org/10.1016/j.scitotenv.2019.134026

Knowledge-based construction of probabilities

N. J. Duijm, I. Kozine
Technical University of Denmark DTU, Department of Technology, Management and Economics, Kgs. Lyngby, Denmark

Risk analyses provide input to decisions on activities exposing (other) people or our environment to risk. It shall be possible to have a critical discussion about such risk analyses. The use of subjective probabilities makes such analyses immune to a critical discussion, unless these "subjective" probabilities are justified by references to explicitly formulated knowledge.

In this paper, we will present our arguments against subjective probabilities, that is, probabilities expressed as degrees of belief of individuals based on the tacit, implicit knowledge of these individuals. We argue that such probabilities, often justified as "expert opinion", are immune to criticism and cannot be falsified ("Only objective knowledge is criticizable: subjective knowledge becomes criticizable only when it becomes objective", [4]). This also applies to expert judgement using a team of experts – consensus (or weighted judgement) is not in itself an evidence of truth.

We propose that probabilities be constructed based on an explicitly formulated collection of knowledge, and using explicitly formulated methods (also founded on the before mentioned collection of knowledge) to transfer that knowledge into a hypothesis about probability. We do not claim that only one such method exists, but rather that different experts or teams may produce different, competing results – but because the basis for the construction is explicit and transparent, it will be possible to have a scientific discourse and to make an informed decision about the preferred hypothesis.

Earlier work has stressed the relation between background knowledge and subjective probability (e.g. [2, 1]), requiring the background knowledge to be "strong". However, we are not aware of clear elaborations of the relation between knowledge and the construction of probability. In line with the suggestion from Kaplan [3], we focus on the elicitation of knowledge from experts, not on the expert's opinion on probability. This in contrast to the approach described by Aven [1], where the expert directly is supposed to provide degrees of belief (i.e. subjective probability) on some property. In our approach, the *domain* expert is to express justified beliefs (knowledge) in a form of "statements", "explanatory theories", "observation statements", etc. [4] within his/her field of expertise. The expert's tacit, implicit knowledge needs to be transferred into explicit knowledge or information in order to be of scientific relevance (for a further discussion see [5]). A *probability* expert is then to transfer that information into a probability hypothesis.

The transformation from knowledge into a probability hypothesis is not necessarily complex, we claim that this approach comprehends and combines many traditional approaches to probability, e.g. the frequentist approach, comparative probabilities, physical failure models, etc. We will provide a few examples.

References

[1] Aven, T. (2017). "Improving the foundation and practice of reliability engineering", *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, Vol. 231, No. 3, pp. 295–305.
[2] Aven, T., Reniers, G. (2013). "How to define and interpret a probability in a risk and safety setting", *Safety Science*, Vol. 51, No. 1, pp 223–231.
[3] Kaplan, S. (1997). "The words of risk analysis", *Risk Analysis*, Vol. 17, No. 4, pp. 407–417.
[4] Popper, K.R. (1972, revised 1979), *Objective Knowledge An Evolutionary Approach*, Oxford University Press, Oxford.
[5] Zins, C. (2007). "Conceptual Approaches for Defining Data, Information, and Knowledge". *J Am Soc Inf Sci Technol*, Vol. 58, No. 4, pp. 479–493.

Bayesian analysis of risk and uncertainty

U. Sahlin
Lund University, Lund, Sweden

Bayesian analysis is a coherent principle of learning and making predictions from expert judgement and data. Core concepts of Bayesian analysis are a subjective probability to quantify epistemic uncertainty, a joint probability distribution derived from a causal model of all variables and parameters, probability theory to combine probabilities, and Bayes rule to update parameters. In addition, Bayesian analysis has a natural link to Bayesian Decision Theory. I will give some examples of the use of Bayesian analysis in assessment of risk and uncertainty and comment on some common misconceptions of what Bayesian analysis is and is not.

References

[1] Cox, L. A. (2012). *Improving risk analysis*. New York, NY: Springer.
[2] Cox, D. R. (2006). *Principles of statistical inference*. Cambridge ; New York: Cambridge University Press.

Using Bayesian Networks for Root Cause Analysis of Observable Problems in Cyber-Physical Systems

S. Chockalingam, V. Katta
Institute for Energy Technology, Halden, Norway

Modern societies rely on proper functioning of Critical Infrastructures (CIs) in different sectors such as energy, transportation, and water management which is vital for economic growth and societal wellbeing. Over the years, CIs have become dependent on Cyber-Physical Systems (CPSs) to ensure efficient operations, which are responsible for monitoring and steering processes as, among others, electric power generation, automotive production, and flood control. Such systems are susceptible to both attacks [1] and technical failures [2].

Because of modern societies' dependence on CPSs, adequate response to observable problems is essential. In order to select appropriate response strategies, it is crucial for decision-makers to be able to distinguish between attacks and technical failures. Once they can distinguish between attacks and technical failures, it is also important for decision-makers to be able to determine the most likely root cause (for instance, the attack vector used to cause an observable problem) to select appropriate response strategies. In most cases, the initiation of a response strategy, presumably aimed at technical failures, would be ineffective in the event of a targeted attack and may lead to further complications. For instance, replacing a sensor that is sending incorrect measurement data with a new sensor would be a suitable response strategy to technical failure of the sensor. However, this may not be an appropriate response strategy to an attack on the sensor, as it would not block the corresponding attack vector. If the decision-makers could determine that the observable problem was due to an attack, the appropriate response strategies to block each attack vector could be different. For instance, the appropriate response strategy for a data manipulation attack on the sensor could be different from physical tampering of the sensor. The initiation of inappropriate response strategies would delay the recovery of the system from adversaries and might lead to harmful consequences. Noticeably, there is a lack of decision support to determine the most likely root cause of observable problems.

Bayesian Networks (BNs) have the capacity to tackle this challenge especially based on their real-world applications in medical diagnosis [3] and fault diagnosis [4]. In our previous work, we developed a framework for constructing BN models to enable decision-makers to distinguish between attacks and technical failures [5]. However, this framework is incomplete without the capability to determine the most likely root cause of observable problems. In this work, we use BNs to tackle the challenge of determining the most likely root cause of observable problems as they enable diagnostic reasoning. Firstly, we propose a framework for constructing BN models to determine the most likely root cause of observable problems. We customised and utilised three different types of variables from existing diagnostic BN models which constitutes our framework. Furthermore, we demonstrated the use of the proposed framework using an example in smart grids. Finally, we highlight the challenges and future research directions.

References

[1] Sun, C. Hahn, A. Liu, C. (2018), "Cyber Security of a Power Grid: State-of-the-art", International Journal of Electric Power & Energy Systems, Vol. 99, pp. 45 – 56.

[2] Zhivich, M. Cunningham, R.K. (2009), "The Real Cost of Software Errors", IEEE Security & Privacy, Vol. 7, No. 2, pp. 87 – 90.

[3] Nikovski, D. (2000), "Constructing Bayesian Networks for Medical Diagnosis from Incomplete and Partially Correct Statistics", IEEE Transactions on Knowledge and Data Engineering, Vol. 9, No. 4, pp. 509 – 516.

[4] Nakatsu, R.T. (2009), "Reasoning with Diagrams: Decision-Making and Problem-Solving with Diagrams", John Wiley & Sons.

[5] Chockalingam, S. Pieters, W. Teixeira, A. Khakzad, N. Van Gelder, P. (2019), "Combining Bayesian Networks and Fishbone Diagrams to Distinguish between Intentional Attacks and Accidental Technical Failures," in Cybenko, G. Pym, D. Fila, B. (Ed.), Graphical Models for Security, Springer, pp. 31 – 50.

Track 10:
Learning from Accidents and Regulatory Practices

Implementing a Lessons Learned Process in the Business Value Chain of a Project Driven Organisation

K. Balasubramaniam
Technical University of Denmark, Kgs. Lyngby, Denmark

A key capability for any organisation's risk management is the ability to communicate risk events and learn from them, a capability that organisations try to strengthen through formalised lessons learned (LL) processes [1, 2]. However, organisations find the LL processes hard to carry through, consequently incentivising scholars to study causation and barriers for LL systems not to be realised [7]. Nevertheless, few studies have focused on creating an LL system customised to the users. This presentation presents how an LL repository and reporting system should be designed for the users, by applying User Experience (UX) design methodology which enables the system to be designed by the users [3, 4]. The findings are based on six user interviews with senior managers from the project driven organisation ABB. The research was divided in a two-stage iterative design-process, where the first phase explored the business requirements and current recommendations to create an initial design of the LL repository and reporting system, to further re-design according to the users' experiences, emotions and beliefs [8]. The findings indicate users' preference towards sharing experience from risk events through active communication, in virtual workshops and meetings, wherein reading an LL report required precise information to determine if it aids mitigation for future risks. The users required an LL process allowing fast and efficient information access for risk identification, encouraging active feedback through likes and comments, with effective search and share possibilities to promote better dissemination of experience. The recommended LL process encourages users to retrieve LL reports through a back-end search engine, extensive (yet easy) LL repository, where the report is readily actionable with contact possibilities, and further created continuously during project risk assessment. Furthermore, obsolete information should be deleted by a document controller, to establish an optimised repository [5]. Ensuring a sustainable risk knowledge sharing from the users' perspective would require access to the right information at right time, and with ease. However, despite the interest of risk knowledge sharing, the user interviews reveals that users forget they are equally responsible for the creation of LL reports [6]. Thus, organisations still need to focus on creating a better organisational culture in order to incentivise knowledge sharing. The recommended design is interconnected with several ERPs in order to enable cross-border information flow, and promote better knowledge management through AI and back-end search engines. Lastly, this research contributes to the literature on bottom-up approached LL processes and project risk management.

References

[1] Duffield, S. & Whitty, J. (2014). Developing a systemic lessons learned knowledge model for organizational learning through projects. International Journal of Project Management, 33(2), 311–324. doi:10.1016/j.ijproman.2014.07.004

[2] Duffield, S. & Whitty, J. (2016). Application of the systemic lessons learned knowledge model for organizational learning through projects. International Journal of Project Management, 34(7), 1280–1293.doi:10.1016/j.ijproman.2016.07.001

[3] Kashfi, P., Feldt, R., & Nilsson, A. (2019). Integrating UX principles and practices into software development organizations: A case study of influencing events. Journal of Systems and Software, 154, 37–58. doi:10.1016/j.jss.2019.03.066

[4] Kuniavsky, M., Goodman, E., & Moed, A. (2012). Observing the user experience: A practitioners guide to user research. Waltham, MA.

[5] Li, A. & Oppenheim, J. (2002). Nasa: Better mechanisms needed for sharing lessons learned.Washington, D.C: DIANE Publishing.

[6] Maqsood, T. & Finegan, A. (2009). A knowledge management approach to innovation and learning in the construction industry. International Journal of Managing Projects in Business, 2(2), 297–307. doi:10.1108/17538370910949310

[7] McClory, S., Read, M., & Labib, A. (2017). Conceptualising the lessons-learned process in project management: Towards a triple-loop learning framework. *International Journal of Project Management, 35*(7), 1322–1335. doi:10.1016/j.ijproman.2017.05.006

[8] Unger, R. & Chandler, C. (2012). *Project guide to UX design: For user experience designers in the field or in the making*. Berkeley, CA: New Riders.

De-learning – a challenge for risk management

F. H. Hedlund
COWI, Copenhagen, Denmark; Technical University of Denmark (DTU), Kgs. Lyngby, Denmark

Risk analysis professionals and policy-makers may wish that the state of knowledge is continuously improving – that the body of information on accident prevention is ever expanding – as if obeying a fundamental law of nature. A case is presented which shows that the opposite can occur. That awareness of hazards learned the hard way after accidental explosions with great loss of life, careful investigation of causes and dissemination of findings in scientific journals, can slip into oblivion and disappear from the body of generally recognized expert knowledge.

Wood pellets are the most common form of woody biomass, and the fuel is widely considered CO_2-neutral. The fast-growing wood pellet sector struggles with smoldering fires in storage silos. The fires are difficult to deal with. Water cannot be used. This has led to new techniques for firefighting which employ inert gases. Nitrogen and carbon dioxide are common inert gases for firefighting, and they are commercially available in large quantities. Unfortunately, the release of carbon dioxide can create electrostatic sparks. Because smoldering fires create flammable pyrolysis gases, the application of carbon dioxide for quenching of a fire may lead to explosion resulting in loss of life.

The presentation offers evidence that information on the hazardous electrostatic properties of carbon dioxide has gone unnoticed in popular wood pellet industry handbooks, reference works and even in internationally recognized standards and codes.

The presentation also covers some of the foot dragging and bureaucratic difficulties that are experienced when bodies such as the National Fire Protection Agency (NFPA) are notified of shortcomings in their publications, leading to slow progress in improvement in standards and codes.

Fragmentation in total institutions: Observations on regulatory practices and risk management

M. Björk
Department of Sociology and Work Science, Gothenburg University, Gothenburg, Sweden
C. Thodelius
Department of Architecture and Civil Engineering, Chalmers University of Technology, Gothenburg, Sweden
K. Nolbeck
Institute of Health and Care Science, Sahlgrenska Academy at Gothenburg University, Gothenburg, Sweden

Total institutions, according to Goffman, are a specific setting in everyday life, mainly defined as a social hybrid combining both work and living environmental features under prison-like conditions [5]. Therefore, as Goffman stresses, everyday life in these institutions are sequenced and formalized over a long period of time, resulting in an institutionalizing process and an adaption of social roles [5]. However, even if this is true, time and also structural context changes some of the premises of the total institution, and therefore – we argue – there is a need of rethinking how organizational, technical and risk discourses have influenced the design of and everyday life in the institutional setting.

Our main point is that total institutions have become more fragmented, or fractured, turning enclosed environments into a series of structural holes that has to be managed. Risk management has today an increased influence on the institution, compared to the 1960s. Moreover, risk is seldom a neutral term regarding probabilities, but in many cases instead social amplified and significant for a specific danger [1, 2, 6]. This raises the question about whose risk exposure that is intended, under what circumstances and at whose expense. This transformation also requires a new theoretical framework to understand institutional settings, mainly those with a high degree of risk management.

As we see it, to avoid or reduce harmful consequences of risk management in institutions, we need to acknowledge the structural design of total institutions in relation to the occurrence of (at least) three new features. Firstly, the fragmentation of social control resulting in the elusive problem of structural holes (cf. [3]). Secondly, the advent of risk management as a problem-oriented activity, or regulatory practice [8, 4]. And, thirdly, technical innovation in the built environment has changed, not least in the field of supervision, which means that building-and-dwelling-issues [7] must be theorized together with risk and regulatory management in (total) institutions.

References

[1] Bauman, Z. (2006). Liquid Fear. Cambridge, UK: Polity Press.
[2] Beck, U. (1992). Risk Society: Towards a New Modernity. London: Sage.
[3] Burt, R. S. (1992). Structural Holes. The Social Structure of Competition. Cambridge, Mass.: Harvard University Press.
[4] Clarke, R.V. (2018). "Regulating Crime: The Birth of the Idea, Its Nurture, and the Implications for Contemporary Criminology." The Annals of the American Academy of Political and Social Science 679, pp. 20–35.
[5] Goffman, E. (1991 [1961]). Asylums: Essays on the Social Situation of Mental Patients and Other Inmates. New Brunswick, NJ: Aldine Transaction.
[6] Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R, Kasperson, J.X., & Ratick, S. (1998). "The Social Amplification of Risk: A Conceptual Framework." Risk Analysis 8(2), pp. 177–87.
[7] Sennett, R. (2019). Building and Dwelling. Ethics for the City. London: Allen Lane.
[8] Sparrow, M.K. (2018). "Problem-Oriented Policing: Matching the Science to the Art." Crime Science 7, pp. 1–10.

Track 11:
Issues of Digitalisation

Safety culture and security culture - Discrepancies, tensions and synergies?

M. Ylönen
Technical Research Centre of Finland, VTT
S. H. Jore
University of Stavanger, Norway

Safety culture is a relatively well-established concept within the safety-critical industry, such as nuclear, oil and gas and chemical industry. The concept was introduced in the aftermath of the Chernobyl nuclear accident by the IAEA expert group to explain the top managers' decisions and employees' performance that had contributed to the accident [1]. Safety culture refers to shared norms, values, beliefs, and practices with respect to safety, in an organization [2]. In contrast, the concept of security culture is not a well-established concept within the industry. Security refers to intentional harms, malicious acts, and the concept can be used in different domains. In the safety critical industries, it has been acknowledged that the convergence of safety and security risks may lead to major accidents, therefore there is an increasing need for integration of safety and security management, and cultures. However, despite synergies, also discrepancies and tensions between the concepts exist. The aim of the paper is to give an overview of the state of the art of the literature of safety and security culture and to discuss if it is meaningful to transfer the concept and the theories from safety culture domain to the security culture domain. The paper draws on studies and theoretical discussions of safety and security cultures.

References

[1] INSAG-4. 1991. Safety Culture. A report by the International Nuclear Safety Advisory Group. Safety Series, No 75, INSAG-4. International Atomic Energy Agency. Vienna.
[2] Pidgeon, N. F. 1991. Safety culture and risk management in organisations, Journal of Cross-Cultural Psychology, 22, 129-140.

Conceptualizing smartness of CPSs

C. Chronopoulos, I. Kozine
Department of Technology, Management and Economics, Technical University of Denmark (DTU), Kgs Lyngby, Denmark

The rapid technological advancement that enhances the smartness of cyber-physical systems (CPSs) creates the need to assure their robustness against unintended and deliberate disturbances. However, balancing smartness and robustness of CPSs is neither intuitive nor simple, but requires the definition of each concept to be formulated and established, along with the dimensions and features that make CPSs smart and robust. The goal of the study is to identify a representative set of definitions and characteristics that compose and describe a smart system in various contexts supported by a literature review in the two major digital libraries (Scopus and Web of Science). We selected the ones that are not only relevant but also crucial for characterizing a CPS as smart. This creates a foundation for our efforts towards finding a balance between smartness and robustness of CPSs, to a comprehensive safety and security risk analysis of such systems.

The focus of scientific research on smartness has increased significantly over the last decade starting from almost no publications in 2010 to 185 and 122 in 2018 in Scopus and WoS respectively. The main subject areas are Computer Science, including various specific sub-areas, such as Information Systems and Artificial Intelligence, and Engineering. Similarly, all the articles selected, based on the specific criteria, through the literature review, have been published over the last 6 years, with their vast majority to be from 2016 onwards. Smartness of modern cities including all their structural elements, such as infrastructure, transportation, education and governance, is the main concept assessed in the literature. The assessment approaches can be grouped in three categories, namely a systemic, anthropocentric and a technological one, all mentioning the importance of information and communication technologies (ICTs) to the enhancement of smartness. Several definitions of smartness and its key characteristics identified in the literature review with the most important input to be from publications assessing the term from a systemic and technological perspective, as opposed to the human-centered ones, characterizing interconnected computer-based systems that are sensing and interact with the physical environment.

Motivated by the similarities between these systems and what Carreras Guzman *et al.*, [2] define as CPS, and inspired by the recent work of Alter, [1], we define the smartness dimensions of CPSs as: (1) degree of integration, (2) real-time feedback control, (3) degree of cooperative control and (4) level of automation, describing also the smartness characteristics of each dimension. This study supplements the research efforts of our group and forms a foundation towards finding a balance between smartness and robustness of CPSs, by providing the conceptual framework to support a comprehensive safety and security risk analysis.

References

[1] Alter, S. (2019). Making Sense of Smartness in the Context of Smart Devices and Smart Systems. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-019-09919-9

[2] Carreras Guzman, N. H., Wied, M., Kozine, I., & Lundteigen, M. A. (2019). Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Systems Engineering. Accepted for Publication*, (May), 1–22. https://doi.org/10.1002/sys.21509

Approaches for operationalizing digitalization strategies

B. A. Kadir, O. Broberg
Technical University of Denmark, Copenhagen, Denmark

The transition into Industry 4.0 and the increasing focus on digitalization and automation of work systems are transforming factories and introducing various organizational, technical and human-related changes, thus creating new challenges and opportunities [1]. To overcome these challenges and fully realize the benefits, there is an increasing demand for new methods, tools and guidelines that can support the alignment of business strategies and operations [4].

In this abstract, we present two approaches for operationalizing digitalization strategies and (re)designing work systems in connection to the implementation of new digital technologies and solutions. By identifying and applying the right approach at an early stage, it might be possible to mitigate risks and uncertainties related to a digital strategy. The framework was developed on empirical data collected through ten industrial case studies, conducted at different small, medium, and large industrial companies located in Denmark. These companies had all started their digitalization journey and implemented one or more new digital solutions in their factories.

The first approach is an operational excellence approach. In typical context, operational excellence deals with improving performance through existing operational modes focusing on reducing costs, delays, and errors, but without making radical changes [2]. An operational excellence approach to operationalize a digitalization strategy entails introducing using new digital technologies in conjunction with operational excellence methods to identify and implement new improvement opportunities. The introduction of the new digital technologies happens in smaller steps, starting with the definition and development a minimum viable solution (MVS), which is the smallest solution that provides the most amount of value and possibility to learn [3]. The MVS is iterated until it reaches a scalable viable solution that can be standardized.

The second approach is an operational innovation approach, which requires more efforts and resources compared to the first approach. Hammer [2] describes operational invocation as developing entirely new ways of how a company do any activities throughout their supply chain and operations. In the context of digitalization, an operational innovation approach focuses on rethinking company work systems in their entirety, and coming up with and designing new improved ways working with the incorporation of new digital technologies. Thus, the changes emerging with this approach might be much greater compared to the first approach. In addition, this approach relies on a holistic understanding of company work systems, an adequate knowledge of new digital technologies and access to potential use cases from other companies and industries.

While both of these approaches might lead to a certain amount of uncertainties, the operational innovation approach involves more risks compared to the operational excellence approach. However, if successful, an operational innovation approach might lead to greater long-term organizational and economic benefits as well as increased competitiveness.

References

[1] Becker, Till, and Hendrik Stern. 2016. “Future Trends in Human Work Area Design for Cyber-Physical Production Systems.” *Procedia CIRP - 49th CIRP Conference on Manufacturing Systems (CIRP-CMS 2016)* 57: 404–9.

[2] Hammer, Michael. 2004. “Deep Change: How Operational Innovation Can Transform Your Company.” *Harvard Business Review*.

[3] Kadir, Bzhwen A, Ole Broberg, Souza da Conceição Carolina, and Nik Grewy Jensen. 2019. “A Framework for Designing Work Systems in Industry 4.0.” *Proceedings of the Design Society: International Conference on Engineering Design* 1 (1): 2031–40.

[4] Schumacher, Andreas, Selim Erol, and Wilfried Sihn. 2016. “A Maturity Model for Assessing Industry 4.0 Readiness and Maturity of Manufacturing Enterprises.” *Procedia CIRP* 52: 161–66.

Conference Committee

Chair of the Conference
Igor Kozine (Technical University of Denmark)

Chairs of the Organising Committee
Melanie Kreye (Technical University of Denmark)
Josef Oehmen (Technical University of Denmark, IDA Risk)
Nijs Jan Duijim (DNV GL Copenhagen, IDA Risk)

Programme Committee
Marja Ylönen (VTT Technical Research Centre of Finland)
Sissel Haugdal Jore (University of Stavanger, Norway)
Sima Rastayesh (Aalborg University, Denmark)
Aiste Balzekiene (Kaunas University of Technology, Lithuania)
Sakari Kuikka (University of Helsinki, Finland)
Susanna Öhman (Mid Sweden University)
Ingibjörg Lilja Ómarsdóttir (University of Iceland)

Technical & Organisational Support
Christos Chronopoulos (Technical University of Denmark)

DTU Management
Department of Technology, Management and Economics

Engineering Systems Design

DTU Management
Engineering Systems RiskLab

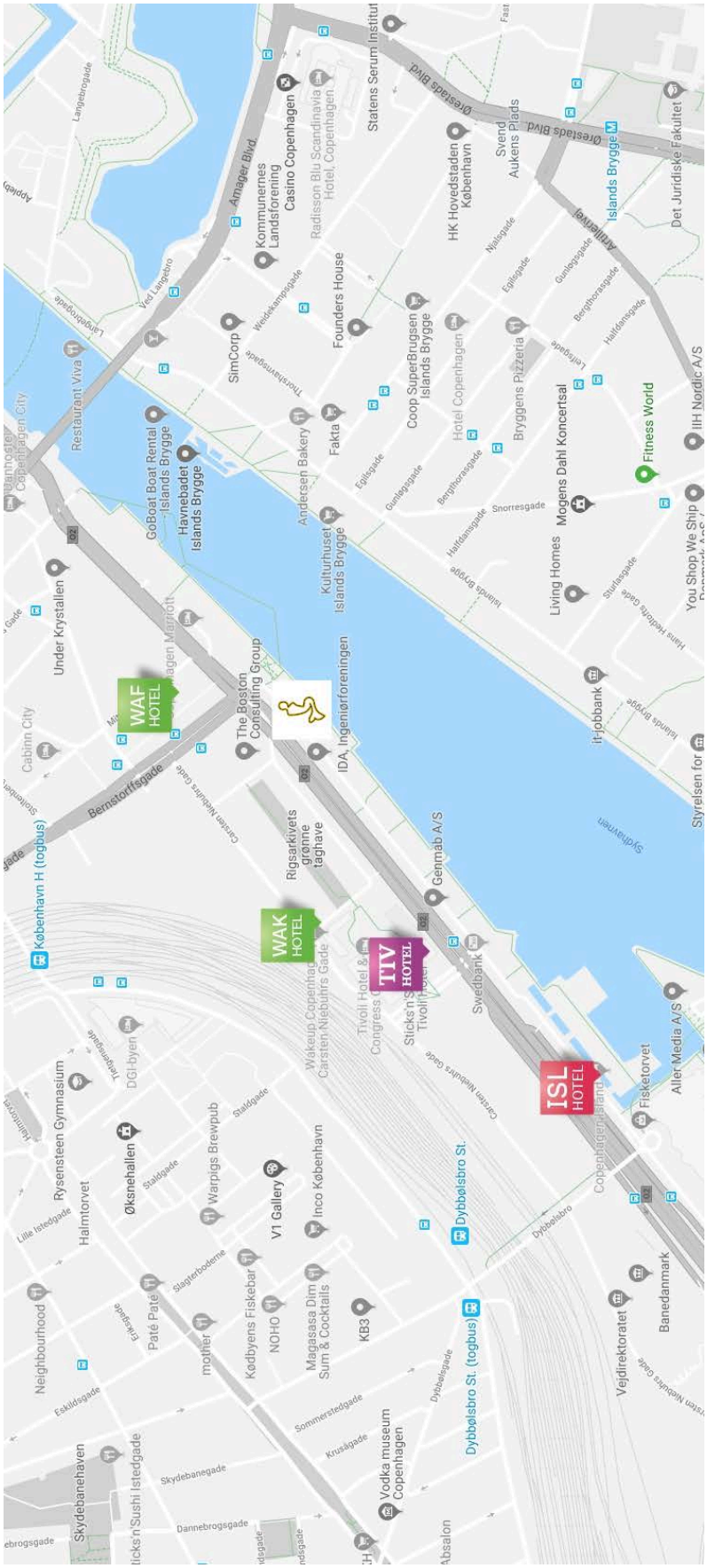
Our sponsors

IDA Risk

SRA EUROPE
Society for Risk Analysis

COWIfonden

Venue



Venue

IDA Conference Center
Kalvebod Brygge 31-33, 1780
København V

Directions

Train
Copenhagen Central Train Station

8 minutes walking distance

Bus
Bus lines 5A, 30 and 66 stop at Polititorvet,
250 meters from the venue

Airport
Copenhagen Airport 15 minutes by car or train

Accommodation

1. Wakeup Copenhagen (WAK)
Carsten Niebuhrs Gade 11, 1577
København V

2. Wakeup Copenhagen (WAF)
Bernstorffsgade 37, 1577
København V

3. Copenhagen Island Hotel (ISL)
Kalvebod Brygge 53, 1560
København V

4. Tivoli Hotel (TIV)
Arni Magnussons Gade 2, 1577
København V

Contact Information

SRA_Nordic_2019@man.dtu.dk

DTU Management
Department of Technology,
Management and Economics

Engineering Systems Design