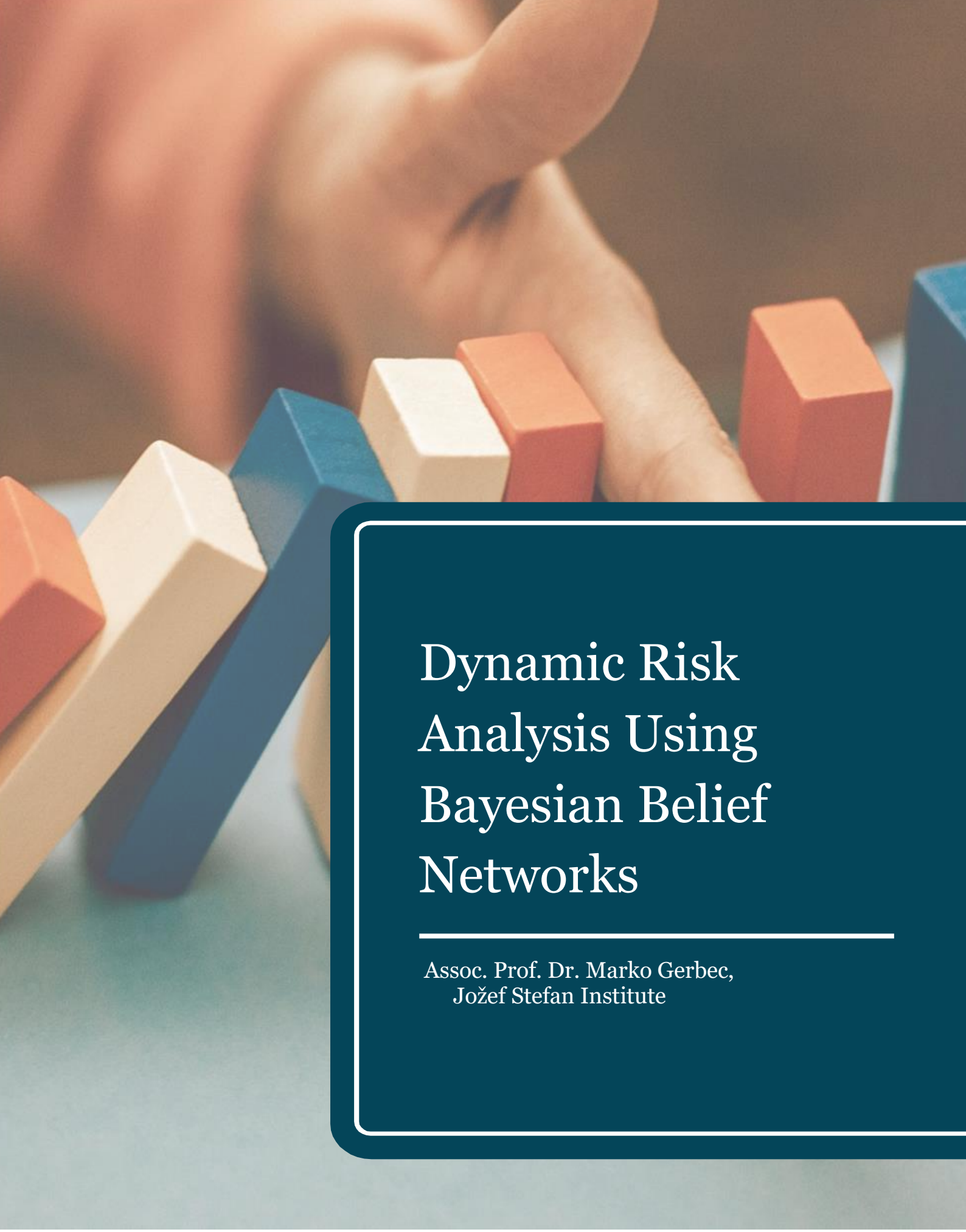

Dynamic Risk Analysis Using Bayesian Belief Networks

Assoc. Prof. Dr. Marko Gerbec,
Jožef Stefan Institute

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe Research and Innovation Programme under the Grant Agreement No. 101073909.

Dynamic Risk Analysis Using Bayesian Belief Networks

Assoc. Prof. Dr. Marko Gerbec (Jožef Stefan Institute)

Dynamic risk analysis is proposed over the conventional static quantitative risk analysis. Risk modelling shall consider available "live" data and information from sensing technologies and the performance of the organization's/Critical Infrastructure's (CI's) management system on the safety and security mitigation measures. In that context, the use of Bayesian Belief Networks (BBNs) is advocated in the EU ATLANTIS project.

1. Introduction

Safety and/or security aspects related to quantitative risk analyses are usually done by the construction of case-related risk modelling considering the potential basic events ultimately leading to undesired consequences to the CI, humans, and the environment. Modelling should consider both the severity of consequences and their likelihood of occurrence. The issue is that the risk models used for the analysis usually provide a static "snapshot" of the situation that is only periodically revised and updated. The proposed solution utilizes the hazards/threats sensing technologies (and other data sources) to be used by the Bayesian Belief Networks (BBNs) [1] as an alternative to the conventional Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Attack Tree analysis and other methods [2]. The updated risk results should be available in real time to the CI risk managers to support the process of risk management.

2. The Current State of Affairs in Dynamic Risk Analysis

Conventional quantitative risk analysis methods use probabilistic risk modelling of the potential hazard/threat scenarios considering consequences (phenomenological) modelling and modelling their probabilities. The point is that the probabilities modelling using methods like Fault Tree, Event Tree, Bow-Ties, Attack Tree, etc., usually uses only the static (historical) data sets on the probabilities or the frequencies of the scenario's starting events [2]. The risk analysis is more or less static and does not adequately reflect the real up-to-date state of the potential hazard/threats and applicable safety and security measures of the CI operators. The gap is recognized in the literature and methodological improvements have been proposed, which usually propose the use of BBNs as a tool of choice and to extend the risk modelling to consider also the influencing factors on the events [3][4]. So far, no risk modelling approach was proposed to directly link e.g., with hazard/threat sensing technologies [5].

3. The Role of Dynamic Risk Analysis

Dynamic risk analysis using BBNs aims to (i) develop case risk models as BBNs instead of e.g., FTA and ETA type of the models, to add flexibility in modelling the risk influencing factors; (ii) the risk case specific hazard/threat sensing data should be used to allow real-time updating of the probabilities of the starting or other events; (iii) the actual performance of the sensing technologies can be taken into consideration to account for uncertainties; (iv) the risk model is to be updated and results should be made available to the risk managers to provide them with the current situational awareness.

The risk models can easily cover the complex relationships among the disaster events (e.g., cascading events, domino accident events) and interpret the consequences per severity, damages, etc.

A conceptual example scheme of the BBN dynamic risk modelling connected with the sensing technologies is presented in Figure 1 below.

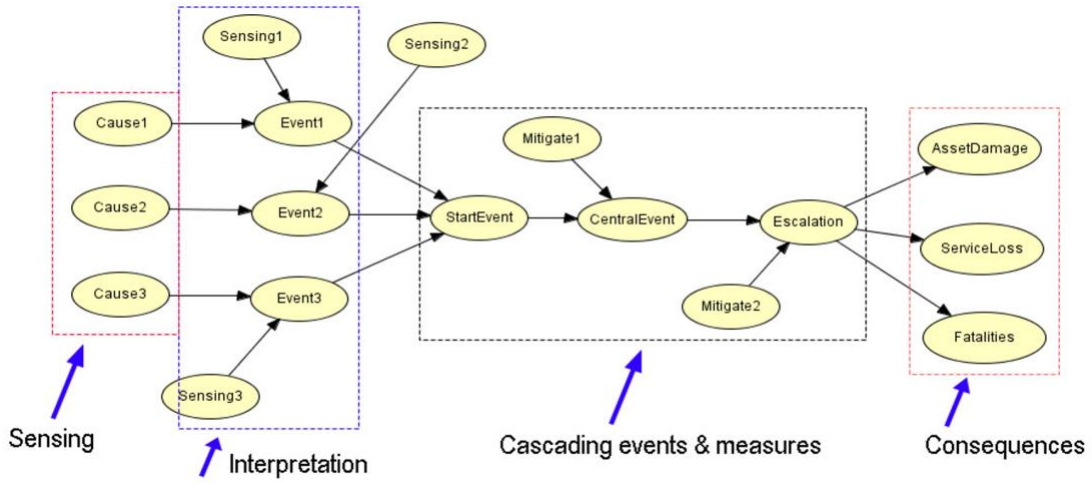

Figure 1. A conceptual scheme of proposed dynamic risk modelling approach using data from the sensing technologies.

4. The Research and Development Path in ATLANTIS

Dynamic risk analysis was brought into the ATLANTIS project from the completed EU project InfraStress [6], where it was proposed and developed in the scope of interdependency modelling and cascading effects impact assessment and tested within a pilot involving several CIs (including Luka Koper and Petrol, also partners in ATLANTIS). The theoretical foundations followed the published principles [2][3][5], consisting of hazard identification, incident scenario elaboration, consequences modelling and modelling the incident cascading events concerning the available safety & and security measures performance data (e.g., Key Performance Indicators, KPIs).

The overall pertaining research and development in ATLANTIS involves a larger modelling domain in comparison to the InfraStress project and is envisaged as:

(a) Document BBN risk modelling approach, including the Large-Scale Pilot (LSP) field safety/security-relevant data consideration into the dynamic model.

(b) Establishing a link for software integration of the BBN software tool (Hugin Expert [7], Commercial Off the Shelf) using API specification by the chosen (dashboard) application in ATLANTIS.

(c) Prepare an example risk case where the risk model will be developed according to the needs of the industrial partners involved (data availability, risk management needs).

(d) Develop, test and report on a fully prepared risk model (likely in a mock-up setup) in the context of the pilot cases.

5. The Challenges and Barriers

The main challenge in developing risk models is in assuring that they are logically correct (faithfulness) and in the use of the correct and up-to-date quantitative data. In developing dynamic risk models, that issue is even more demanding, as additional data and information are needed due to the complexity of the models (in comparison to the static models). Thus, the comprehensiveness of the models is usually limited by the availability of the data needed. This is usually approached by using the subject expert judgements in addition to the actual data. Thus, the term "belief" in BBN's name.

Related to the security domain, the historical data on the likelihood of the specific attack modes to the specific types of industries are very hard to obtain, as well as one needs to consider potential target attractiveness in time/situation. In addition, less severe cyber-attacks pose a reputation challenge to the target victim organizations, who are usually reluctant to publish or at least share information on the circumstances of the attack, thus hindering the opportunity to learn from it.

6. The Benefits and Impact

Organizations could benefit from the dynamic risk assessment through better comprehension of the risk from related hazards and threats. Improved situational awareness for the risk managers can be obtained via availability e.g., of the sensing technologies and interpretation of the obtained data in near real-time. Risk modelling can forecast likely disaster propagation paths, cascading events and ultimate consequences to the various risk targets (e.g., CI assets, CI services, humans, environment, etc.). Subject to availability, the performance of the existing or proposed mitigation measures (safety and security barriers) can be easily taken into account and linked to the performance of the organization's management system.

In the piloting activities of the InfraStress project, we successfully evaluated the monetary value of risk reduction for the envisaged candidate physical mitigation measures (e.g., drone detection and neutralization). This helped in understanding the costs and benefits of candidate mitigation actions for CI management.

The challenge is the acceptance of the proposed approach to the dynamic risk analysis by the organization's management. On one side the quantitative data are available only from the historical compilations, on the other side, the organization's personnel and management are usually not used to the probabilistic methods and the concept of the risk as a whole. The

proposed way is to include the organization's personnel from the start in the evaluations and modelling efforts to gain trust in the structure of the models and in the quantitative data used.

7. Future Outlook

The dynamic risk analysis (risk modelling with BBNs) is generally applicable and can be applied to any scale and any safety or security (or both) case application. The only, but serious, limitation is in the actual availability of (i) risk case description (e.g., technology and organization details needed), (ii) quantitative probabilistic data (historical or case specific) to allow the events and consequences modelling, (iii) determination of the client (end users) to ensure the data and information needed to obtain a comprehensive risk modelling tool that will be of use to them.

8. Conclusions

Conventional risk analysis (risk modelling) provides a rather static (snapshot in time) risk result. There is a need for dynamic risk modelling that constantly receives information about the observed hazards and threats, as well as about the performance of the organization's mitigation measures.

Dynamic risk modelling is advocated that should utilize the sensing technologies (including those proposed by the ATLANTIS project), their logical interpretation and construction of Bayesian Belief Network (BBN) based models.

While comprehensive risk models can be developed, there is a constant challenge to the required quantitative data and required complexity to adequately represent reality. Close cooperation is required with the target organization (CI).

References

[1] Kjærulff Uffe B., Madsen Anders L., 2013. Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis. Second Edition, Springer. ISBN 978-1-4614-5103-7.

[2] Guidelines for chemical process quantitative risk analysis, Second edition. Center for Chemical Process Safety, AIChE, 2000. ISBN 0-8169-0720-X.

[3] Gerbec M., Kontić B., 2017. Safety related key performance indicators for securing long-term business development – A case study. Safety Science, 98, 77–88.

[4] Gerbec, M., Baldissone, G., Demichela, M., 2017. Design of procedures for rare, new or complex processes: Part 2 – Comparative risk assessment and CEA of the case study. Safety Science, 100, Part B, 203-215.

[5] Gerbec, Marko, Giunta, Gabriele. InfraStress approach on risk modelling of cascading events with live data for decision support. In: SOLDATOS, John (Ed.), PRAÇA, Isabel (Ed.), JOVANOVIĆ, Aleksandar (Ed.). Cyber-physical threat intelligence for critical infrastructures security : securing critical infrastructures in air transport, water, gas, healthcare, finance and industry, (NowOpen). Hanover: Now Publishers. 2021, 2-21, DOI: 10.1561/9781680838237.

[6] InfraStress project, https://cordis.europa.eu/project/id/833088

[7] Hugin Expert, https://www.hugin.com/

Front cover image by Olexandr Pidvalnyi via Pixabay.
https://pixabay.com/users/oleksandrpidvalnyi-4638469/