NARSIS

New Approach to Reactor Safety ImprovementS

WP3: Integration and Safety Analysis

D3.5 - PhD narrative on hazard integration and risk analysis for NPPs through a Bayesian approach

This project has received funding from the Euratom research and training programme 2014-2018 under Grant Agreement No. 755439.

Project Acronym: NARSIS

Project Title: New Approach to Reactor Safety Improvements

Deliverable: D3.5 - PhD narrative on hazard integration and risk analysis for NPPs through a Bayesian approach

Month due: M54 **Month delivered:** M54

Leading Partner: Delft University of Technology

Version: Final

Primary Author: Varenya Kumar Duvvuru Mohan (TU Delft)

Other contributors:

Deliverable Review:

- **Reviewer #1:** Phil Vardon, TU Delft **Date:** 28/02/2022

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of contents

List of Abbreviations

BN	Bayesian Network
CCF	Common Cause Failure
MGL	Multiple Greek Letter
OOBN	Object-Oriented Bayesian Network
SSC	System, Structure and Component

1 Executive Summary

A PhD thesis is being prepared based on the investigations undertaken and the findings of Work Package 3 of the NARSIS project; this deliverable presents a summary of the doctoral thesis. The thesis is to be titled “Bayesian networks for high-reliability applications” and will be defended at Delft University of Technology. The thesis will be focused on the various aspects of modelling risk in high-reliability industries (e.g., nuclear, chemical, aviation, public infrastructure), using Bayesian networks.

The BN was found to be an effective tool for risk and reliability modelling based on an extensive literature study. On comparison with existing risk integration tools such as event and fault trees, it is demonstrated that BNs can produce equivalent results but as well offer several advantages. Representation of multi-state and continuous variables, modelling of dependence between variables, Bayesian updating and diagnostic inference are identified as some of the inherent advantages of BNs – features that are well-suited to multi-risk assessment.

While BNs have been extensively used at the system level, they have rarely been applied for facility-wide multi-risk assessment, particularly in the nuclear industry. Also, the modelling of several key technical and human aspects are often extraneous to the risk integration tool. A multi-risk integration methodology using BNs is presented to include dependence between hazards and interaction of hazards with systems, structures and components (SSCs). The BN method allows for uncertainty propagation and tracking, along with sensitivity analysis that can be used to remove inconsequential variables or dependencies to increase network efficiency. The method is applied to a simplified accident scenario induced by external hazard(s), involving technical systems as well as human actions. Results indicate that the interaction of hazards can significantly impact the probability of occurrence of an accident. Similarly, changes in states of human performance shaping factors, during hazard events, can cause significant increase in top event probability.

Sensitivity analyses in the multi-risk BN indicate that common cause failure (CCF) events are a key contributor to top event probability. The Multiple Greek letter (MGL) method - a parametric model often used to model CCFs in nuclear probabilistic safety assessment – is implemented in BNs and shown to yield equal results as in fault trees. However, modelling complex systems with multiple redundancies can result in a large network that is difficult to decipher visually. Moreover, the MGL model assumes that systems are symmetrical, composed of identical components. An alternate approach to CCF modelling in BNs, using correlation between component failures, is presented. The correlation-based approach produces comparable results to the MGL model while imposing no limitations regarding system symmetry. For an n-component system, the MGL BN uses 2^{n-1} CCF nodes while the correlation-based BN uses only n+1 CCF nodes. The approach can be further improved by reducing computational cost but as well by using more complex models to define higher order dependence, such as copulas or vines, rather than a pairwise correlation.

In the aforementioned multi-risk BN, interaction between human factors and top event probability was possible due to the use of BNs for both overall risk integration as well as human reliability modelling. Similarly, if BNs can be used for surrogate modelling of advanced numerical models of technical SSCs, unforeseen dependencies can be identified, between input variables at the system level and top events at the plant level. Therefore, a surrogate BN is developed to mimic the random finite element method (RFEM) in modelling the geotechnical reliability of a flood defence embankment. The BN is found to be an effective surrogate modelling tool, which can significantly reduce computational cost associated with advanced numerical methods. The uncertainty in input soil parameters is propagated to the distribution of factor of safety of the embankment. The impact of site investigation on flood defence reliability is also directly obtained via Bayesian updating in the network.

The reliability of a flood defence system is modelled using the surrogate BN for the RFEM analysis. Subnetworks are used for each flood defence section and the dependence between soil and loading parameters of each section is implicitly modelled using the correlation-based

CCF approach. Results indicate that the BN can act as an effective tool for system reliability modelling while representing advanced numerical analysis and accounting for CCFs. Such surrogate BNs can be integrated with larger, plant-wide BNs to improve risk estimates.

2 Introduction

This deliverable presents a brief summary of the doctoral thesis due to be completed after the end date of the NARSIS project. The thesis is to be titled “Bayesian networks for high-reliability applications” and is focused on the various aspects of modelling risk in high-reliability industries (e.g., nuclear, chemical, aviation, public infrastructure), using Bayesian Networks (BNs). The thesis work, addressing these different aspects, is summarized in the following sections.

3 Bayesian networks in risk assessment

BNs are identified via a literature review as an effective tool for use in risk assessments for high-reliability industries. Their features and theoretical aspects associated with their use in risk assessments are discussed. An extensive summary of BN applications for engineering risk assessments is presented, highlighting various modelling aspects, advantages and limitations. These include applications in aviation (e.g. Ale et al., 2006), chemical (e.g. Khakzad et al., 2011), and nuclear (e.g. Kwag and Gupta, 2017) industries. Nevertheless, there have been few plant-wide applications, particularly in the nuclear industry. A station blackout event scenario at a nuclear power plant is assumed to compare BNs with event and fault trees – widely used tools for risk assessment. The advantages of the BN are demonstrated using this example, justifying further exploration into their use for multi-risk integration in high-reliability industries. The key advantages are:

- BNs provide an added advantage in fault diagnostics over fault trees, in that new evidence can be easily incorporated into the model as Bayesian updating is inherent to BNs.
- Diagnostic inference in the BN enables more direct evaluation of individual component contribution to system failure, as opposed to the cutset approach adopted in fault tree analyses.
- The posterior joint probability of all basic events given top event occurrence provides information regarding both occurrence and non-occurrence of all the basic events. Hence, unforeseen dependencies may be identified during fault diagnosis in BNs as compared to fault tree analysis where cutsets follow predetermined paths to failure and provide no information about the occurrence or non-occurrence of basic events that are not included in these cutsets.
- Multi-state variables can more directly be incorporated into BNs. Unlike fault trees, BNs can directly incorporate continuous random variables without the need for additional modifications. BNs also inherently consider statistical dependencies between variables. Hence, uncertainty representation and propagation are native to BNs. Thus, expert judgement can be easily incorporated into BNs along with associated uncertainties.
- As more complex systems are modelled, with increased common cause effects, BNs can grow in size, making visualisation and computation challenging. This is a significant downside of BNs, as the logical interaction between components becomes visually indecipherable. An alternate approach is proposed, later in this study, for considering CCFs in BNs, to curb the proliferation of nodes and links due to CCF events.

Hence, BNs are a suitable tool for multi-risk assessments to consider dependencies between various hazards, their interaction with SSCs, integrate technical and human aspects, and incorporation of expert judgement when data is scarce.

4 Multi-Risk integration using Bayesian networks

High-Reliability industries require a multi-hazard risk integration framework that considers even low-probability external hazard events. The risk framework should account for the impact of these hazards on complex, dependent systems, and also allow for inclusion of expert judgement where data is sparse. The risk framework must also be suitable for tracking uncertainties in the data and propagating them to the final risk estimate. BNs are presented as a suitable tool for multi-risk integration. A step-wise methodology is proposed, which accounts for dependencies between the hazards, but as well between hazards and various SSCs (Figure 1). Inference in the network allows for uncertainty propagation and Bayesian updating of probabilities. Sensitivity analyses, based on inference, can be used to remove inconsequential variables and dependencies, to make the model more efficient. A simplified accident scenario at a virtual power plant is used to demonstrate the BN-based risk assessment methodology. Multiple hazards, their dependencies and vector-valued fragilities are modelled within the risk network. In addition, the above technical aspects are combined with human aspects by including a BN-based human reliability estimation method.

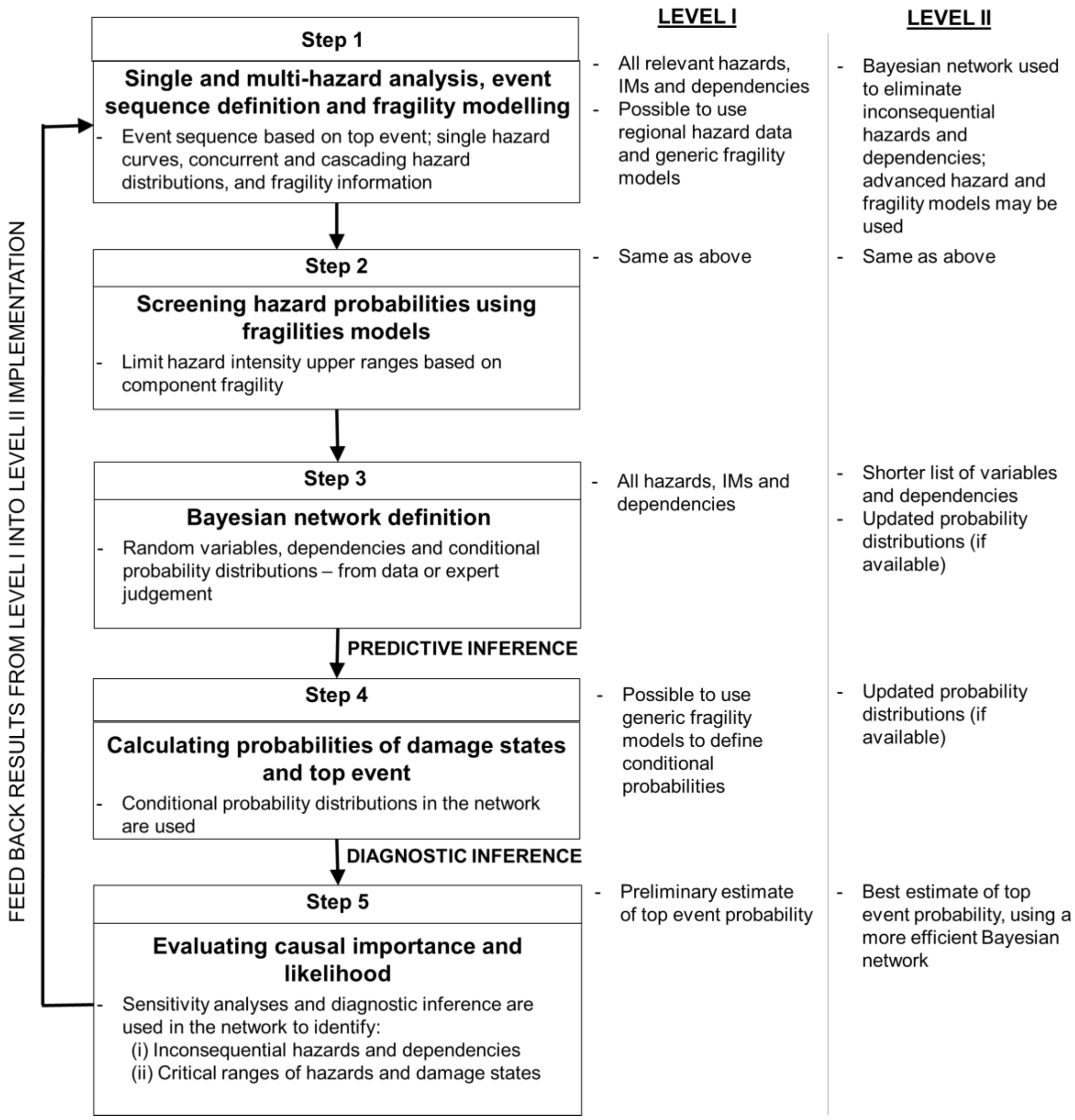


Figure 1: Step-wise multi-risk integration methodology using Bayesian networks

The risk integration using BNs is performed using two approaches. The first method is an object-oriented BN (OOBN) approach where basic fault trees and hazard trees in existing probabilistic safety assessment, can be individually converted to BNs - risk objects (or subnetworks). These separate risk objects are integrated by defining their interactions as per the associated event trees. In the second approach, a unified BN is constructed by combining hazards and all subnetworks within a single BN. Both these approaches are demonstrated using the station blackout event scenario.

The two approaches for multi-risk integration using BNs compare as follows:

Utilising the advantages of BNs

- Diagnostic inference and Bayesian updating are inherent advantages of BNs. In OOBNs, these features are limited to within risk objects and cannot be performed across objects. Thus, unified BNs better preserve some key advantages of BNs over fault trees.
- The unified integration of subnetworks with external hazards can help understand links between the top event of interest and various SSCs in the nuclear power plant, and reveal unforeseen dependencies. While using many hazard trees as in OOBNs, dependencies may be missed between different variables across scenarios. Using a unified BN could possibly limit such omissions.

Using existing PSA information

- Event trees and fault trees in existing PSA can be equivalently modelled as OOBNs, allowing for easy transition with parallel application as opposed to the unified BN approach, where the logical interactions of event trees are housed in conditional probability tables of hazard nodes. Hence, OOBNs can also be more easily implemented for plant-wide applications.

Computational load

- Multi-hazard integration under a unified BN, with several variables influenced by hazards and complex subnetworks, can result in significant computational challenges.
- One solution to manage the computational requirements may be to combine the OOBN and unified BN approach to integration, where subnetworks are integrated only where necessary while other subnetworks remain as separate risk objects.

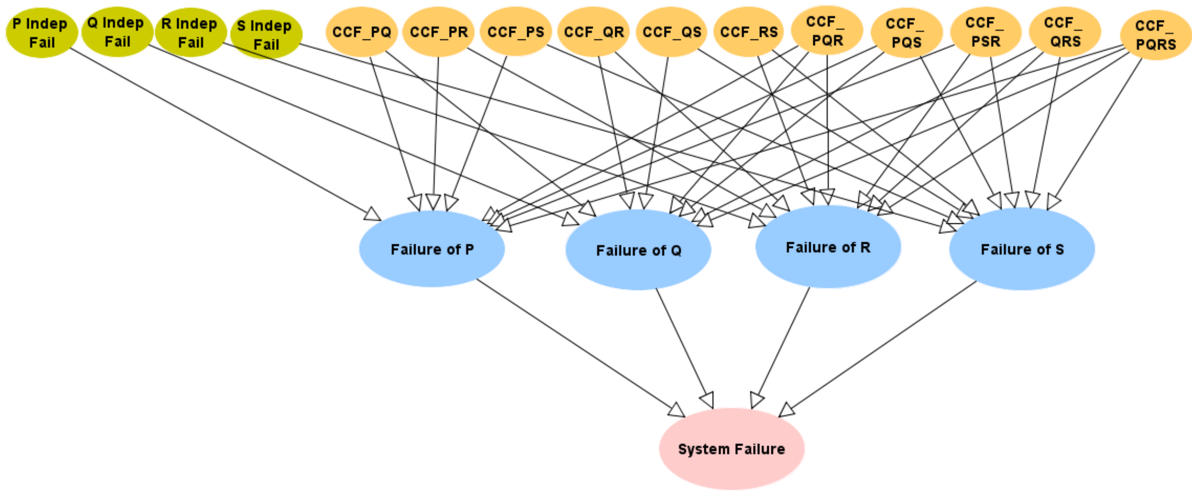
General conclusions based on the multi-risk BN (either approach) include:

- A stepwise, iterative multi-risk framework for risk integration using BNs was proposed. The methodology was applied to the accident scenario of interest – external hazard induced station blackout event.
- Technical and human aspects were successfully integrated in a multi-hazard scenario using BNs. Multiple hazards, surrogate models for systems, human reliability methods and existing PSA information were all integrated under one risk framework, allowing for understanding of various dependencies.
- BNs can directly incorporate continuous random variables without the need for additional modifications as in the case of fault trees. Also, it is easy to integrate expert judgement in BNs. These advantages, demonstrated in the subnetworks, are also carried over into the unified BN.
- Sensitivity analyses in the multi-risk BN (either approach) indicate that common cause failure (CCF) events are a key contributor to top event probability. As more complex systems are modelled, with increased common cause effects, BNs can grow in size, making visualisation and computation challenging. Dependencies between components can become visually indecipherable. The next section presents an alternate method to model CCFs using BNs.

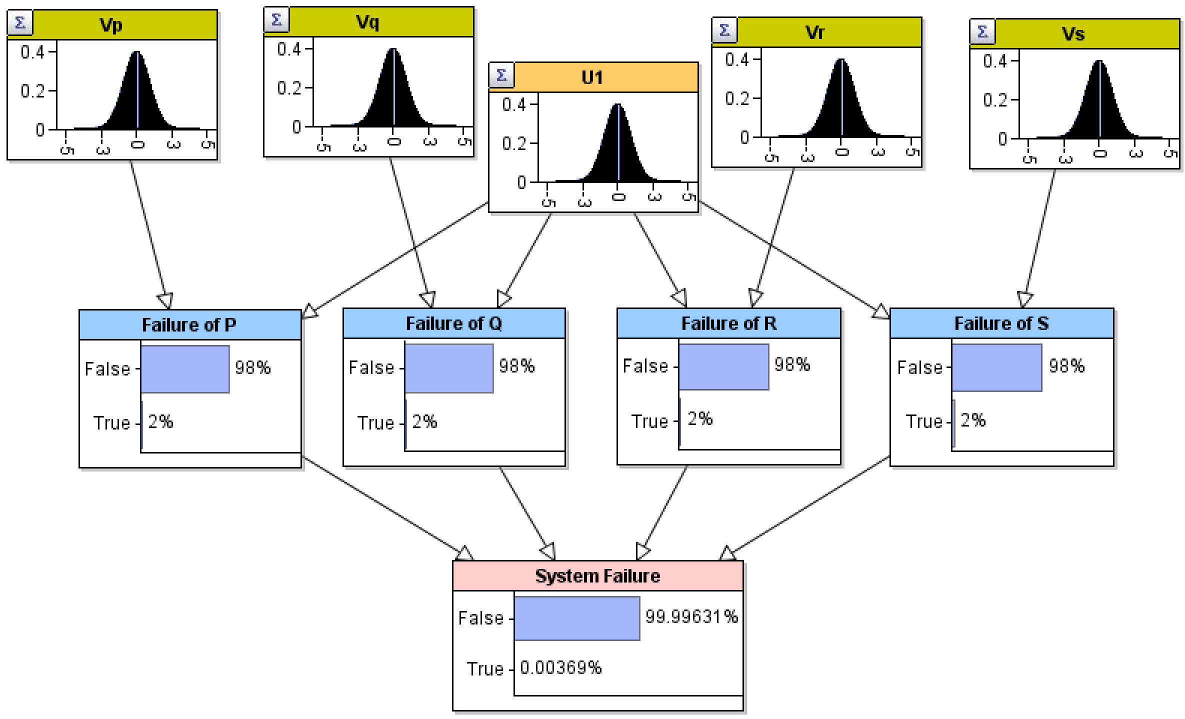
5 Dependence modelling in system reliability estimation

An important aspect of accounting for statistical dependence in high-reliability applications, is the modelling of common cause failures (CCFs). CCFs are often key contributors to accidents and their inaccurate modelling can lead to significant errors in the overall risk estimate. CCFs are currently represented in risk integration using parametric models such as the Multiple Greek Letter (MGL) model. The MGL model is implemented in BNs for an example 4-component system and is shown to give equal results. The representation of the MGL model, particularly for systems with multiple redundancies, can result in a large network that is difficult to decipher visually. In addition, the MGL model assumes systems to be symmetrical, composed of identical components. This, of course, need not be the case in real systems and can be an excessively conservative assumption. Hence, an alternate approach is proposed to model CCFs in BNs. This method is based on correlation between component failures as opposed to conditional probability relations captured by the MGL model. The correlation-based approach makes no assumptions regarding system symmetry, but as well, significantly reduces the number of nodes in the network. Thus, the differences between the MGL method and the correlation-based approach are demonstrated using an example of a flood defence system. The following are the key findings from this comparison:

- The MGL model is extensively used in probabilistic safety assessment and its typical implementation in fault trees is directly transposable to BNs.
- The number of nodes in the MGL-BN can increase exponentially with increasing size of the common cause component group (2^{n-1} nodes for an n-component system), making visualisation of the BN cumbersome. In contrast, the correlation-based approach allows for easier visualisation as CCF effects for a system of n components is represented using $n + 1$ nodes in the BN. Figure 2 shows the MGL BN and the correlation-based BN for an example 4-component system.
- The MGL approach demands the assumption of a symmetric system where the failure probability of the weakest component is assumed for the entire component group. The correlation-based approach needs no such assumption and can provide a more accurate estimate by considering the actual failure probabilities of each component.
- The correlation-based approach could be conservative due to its consideration of coincident failures. All coincident events are considered as CCFs, as opposed to the MGL model which depends on the correct classification of joint failures in the failure dataset as CCFs, even when the exact common cause may not be apparent.
- The computational effort for the correlation-based approach is relatively higher due to the use of continuous nodes in the BN. For instance, within a convergence tolerance range of 1×10^{-3} to 1×10^{-4} for the dynamic discretization of the standard normal nodes in the correlation-based BN, the MGL BN is 5 to 25 times faster than the correlation-based BN.
- The correlation-based method assumes pairwise dependence and could miss higher order dependence between variables, although this can be tested.
- The correlation-based approach is suitable when component failure probabilities are either normally distributed or have been converted to a Bernoulli distribution by thresholding a normal distribution. This is an inherent assumption of the method.
- If variables in the failure data are normally distributed, the phi correlation coefficient can be used in the correlation-based approach. If the normal variables have been converted to binary (for example, the component is considered to be functional below, and failed at and above, a threshold value), then the tetrachoric correlation, computed between binary variables, can be directly used.



(a)



(b)

Figure 2: (a) MGL model represented in a Bayesian network for a 4-component system; (b) Correlation-based approach in the BN for the 4-component system

6 Surrogate modelling and reliability updating using Bayesian networks

BNs are proposed as a tool to integrate reliability and influential variables relating to the slope stability of an idealized, flood-defence embankment. The site investigation (extent) and slope geometry, as well as the material properties and their spatial variability, are considered within a BN. The random finite element method (RFEM) is used to quantify the slope reliability and demonstrate the overall methodology. Prior probabilities of geometry, material parameters and their heterogeneity are obtained from 'initial' site investigation data. Probabilistic distributions of slope performance (factor of safety) are obtained by Bayesian inference in the network to investigate the impact of additional site investigation. The amount of additional site investigation required to increase the geotechnical reliability is assessed. Figure 3 shows the skeletal structure of the BN. This work illustrates the applicability of BNs as an effective reliability and uncertainty assessment tool that can aid decision making for site investigation (cone tests) and during maintenance, where new observations can be readily integrated to obtain updated reliability estimates. In addition, the representation of advanced numerical models of SSCs using BNs allows for the interaction of input variables at the system level with the top event of accident scenarios at the plant level.

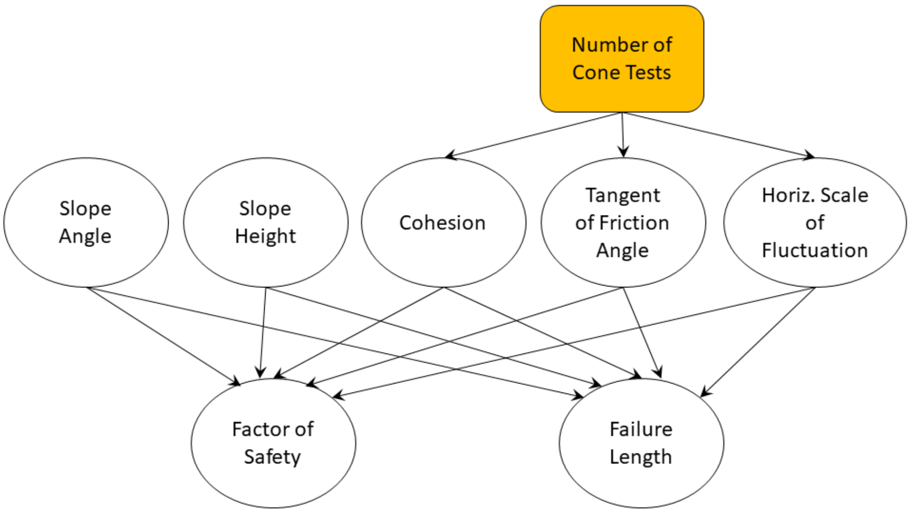


Figure 3: Bayesian network for reliability updating of flood defence embankment acting as a surrogate model for RFEM analyses

7 System reliability modelling using Bayesian networks – a geotechnical application

The reliability of a flood levee system is estimated using BNs. The reliability of individual levee sections is modelled using surrogate networks that represent RFEM models of each of the levee sections. The levee sections share several dependencies between their material parameters, geometry and loading. Rather than modelling each of these dependencies and associated mechanisms in the system reliability network, implicit CCF modelling using a correlation-based approach is adopted. The results indicate the significant influence of dependencies between sections on levee system reliability. BNs are shown to be an effective surrogate method, to represent levee systems, which can be used for uncertainty tracking and reliability updating.

8 Conclusions

BNs have been shown to be a powerful tool which is suitable for multi-risk integration in high-reliability industries. The following overall conclusions are made from this study:

- BNs present several advantages over conventional risk integration tools such as event and fault trees.
- Statistical dependencies between hazards, fragilities and human aspects can be modelled under one framework, while incorporating expert judgement where data is scarce.
- A multi-risk, iterative integration methodology using BNs is proposed starting from hazard integration to top event probability estimation, including sensitivity analysis.
- BNs can also act as surrogate models of more advanced numerical models, reducing computational costs for reliability updating. BN-based surrogate models also enable direct modelling of dependencies between input variables at the system level or component level, to events at the plant-level.
- The network can become large, unintelligible and computationally demanding for large systems and plant-level risk models, particularly using the unified BN approach. These challenges can be reasonably overcome by utilising the sensitivity analysis in the network to remove inconsequential variables and dependencies. Correlation-based modelling of CCFs can further reduce the number of nodes while allowing representation of asymmetric systems.

9 References

Ale, B. J. M., Bellamy, L. J., Cooke, R. M., Goossens, L. H. J., Hale, A. R., Roelen, A. L. C., & Smith, E. (2006). Towards a causal model for air transport safety—an ongoing research project. *Safety science, 44*(8), 657-673. doi:https://doi.org/10.1016/j.ssci.2006.02.002

Khakzad, N., Khan, F., & Amyotte, P. (2011). Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering & System Safety, 96*(8), 925-932. doi:https://doi.org/10.1016/j.ress.2011.03.012

Kwag, S., & Gupta, A. (2017). Probabilistic risk assessment framework for structural systems under multiple hazards using Bayesian statistics. *Nuclear Engineering and Design, 315*, 20-34. doi:https://doi.org/10.1016/j.nucengdes.2017.02.009

Mohan, V. K. D., Vardon, P. J., Dusic, M., van Gelder, P. H. A. J. M., Hicks, M. A., & Burgazzi, L. (2018). Risk integration methods for high risk industries (Technical Report D3.1). Retrieved from http://www.narsis.eu/page/deliverables

Mohan, V. K. D., Vardon, P. J., Hicks, M. A., & van Gelder, P. H. A. J. M. (2019). Uncertainty tracking and geotechnical reliability updating using Bayesian networks. Paper presented at the 7th International Symposium on Geotechnical Safety and Risk (ISGSR), Taipei, Taiwan.

Mohan, V. K. D., Vardon, P. J., van Gelder, P. H. A. J. M., Abrishami, S., Guldenmund, F., & Gehl, P. (2021). Development of risk sub-networks for technical and social/organisational aspects (Technical Report D3.2). Retrieved from http://www.narsis.eu/page/deliverables

Mohan, V.K.D., Vardon, P.J., Hicks, M. A. (*in preparation*). Surrogate modelling of the random finite element method using Bayesian networks for reliability updating

Mohan, V.K.D., Vardon, P.J., Hicks, M. A. (*in preparation*). System reliability modelling using Bayesian networks – a geotechnical application for levees

Mohan, V.K.D., Vardon, P.J., Rohmer, J., Gehl, Pierre (*in preparation*). Common cause failure modelling using Bayesian networks – A comparison between existing parametric models and a correlation-based approach

Mohan, V. K. D., Vardon, P. J., van Gelder, P. H. A. J. M., Abrishami S. (*in preparation*). Multi-risk integration of technical and human reliability aspects in probabilistic safety assessments using Bayesian networks