Multi-hazard probabilistic safety assessments using Bayesian networks – A framework and demonstration for integrating technical and human risk

Mohan, Varenya Kumar D.; van Gelder, Pieter H.A.J.M.; Gehl, Pierre; Hicks, Michael A.; Vardon, Philip J.

DOI
10.1016/j.nucengdes.2025.114558

Publication date
2026

Document Version
Final published version

Published in
Nuclear Engineering and Design

Citation (APA)
Mohan, V. K. D., van Gelder, P. H. A. J. M., Gehl, P., Hicks, M. A., & Vardon, P. J. (2026). Multi-hazard probabilistic safety assessments using Bayesian networks – A framework and demonstration for integrating technical and human risk. *Nuclear Engineering and Design*, *446*, Article 114558. https://doi.org/10.1016/j.nucengdes.2025.114558

Nuclear Engineering and Design 446 (2026) 114558

Contents lists available at ScienceDirect

Nuclear Engineering and Design

journal homepage: www.elsevier.com/locate/nucengdes

Multi-hazard probabilistic safety assessments using Bayesian networks – A framework and demonstration for integrating technical and human risk

Varenya Kumar D. Mohan [a,*], Pieter H.A.J.M. van Gelder [b], Pierre Gehl [c], Michael A. Hicks [a], Philip J. Vardon [a]

[a] Geo-Engineering Section, Faculty of Civil Engineering and Geosciences, Delft University of Technology, the Netherlands
[b] Faculty of Technology, Policy and Management, Delft University of Technology, the Netherlands
[c] BRGM, 3 av. C. Guillemin, 45060 Orléans CEDEX 2, France

ARTICLE INFO

Keywords:
Bayesian network
Safety assessment
Risk assessment
PSA
Multi-hazard
Human reliability
Fault tree

ABSTRACT

Despite the advantages of using Bayesian networks for probabilistic risk assessment, adoption in practice has been limited due to the lack of realistic, facility-scale studies. Scaling up from systems to facility-level safety assessments poses challenges in (i) integrating external hazards and their cascading effects, and (ii) resolving non-homogeneity of various technical and human reliability models. The novelty of the study is in formalising risk integration using Bayesian networks, at facility scale, and demonstrating its effectiveness in addressing associated challenges. A Bayesian network-based multi-hazard risk framework is introduced and demonstrated for a nuclear power plant subject to flooding and earthquake hazards, capturing dependencies among hazards and consequences. Individual reliability models – conventionally extraneous to facility-wide risk models – are included as subnetworks by using Bayesian network-based surrogate models for technical systems and a Bayesian networks approach for human reliability modelling. Two approaches are used for subnetwork integration – object-oriented and unified Bayesian networks. The unified approach allows for prediction, diagnostics and inter-causal reasoning since Bayesian inference is bi-directional. Conversely, in the object-oriented approach, diagnostics are limited to within individual subnetworks and as a consequence the model can potentially neglect dependencies between objects. However, the object-oriented model requires only 50 % of the computational memory and consumes less than 25% of the runtime as the unified network, while improving visual clarity of the risk model. The model reveals key insights – for example, variations in operator stress or available response time during a hazard event can result in up to a 77 % change in top event probability – demonstrating its effectiveness in capturing critical relationships in complex, facility-scale risk scenarios. These findings can be used to suitably allocate resources towards risk mitigation and plant safety management.

1. Introduction

The consequence of failure of infrastructure, such as those associated with public safety, chemical, aviation and nuclear industries, can be catastrophic (Hopkins, 2011; Lees, 2005; US NRC, 1975). Risk assessments in such high-reliability industries pose several challenges. Multi-hazard combinations of extremely low probability must be considered, along with their cascading effects, due to the potentially catastrophic consequences (Roberts, 1990). These facilities are generally composed of several interacting systems, and accounting for these interactions makes them complex to analyse. Moreover, there are very few cases of significant accidents in these industries, which precludes conventional statistical analysis to predict future risks (Leveson et al., 2009). Probability estimates of various hazards and their impact on systems,

Abbreviations: BN, Bayesian network; BN-SLIM, Bayesian network – success likelihood index method; CCF, Common cause failure; CPD, Conditional probability distribution; EDG, Emergency diesel generator; EQ, Earthquake; ESD, Event sequence diagram; ET, Event tree; FT, Fault tree; FTA, Fault tree analysis; HEP, Human error probability; JPD, Joint probability distribution; LOOP, Loss of offsite power; NPP, Nuclear power plant; OOBN, Object-oriented Bayesian network; PGA, Peak ground acceleration; PRA, Probabilistic risk assessment; PSA, Probabilistic safety assessment; PSF, Performance shaping factor; SBO, Station blackout; SCD, Secondary cooldown; SSCs, Systems, structures and components; US NRC, United States Nuclear Regulatory Commission; VPP, Virtual power plant.

* Corresponding author.
E-mail addresses: v.k.duvvurumohan@tudelft.nl (V.K.D. Mohan), P.H.A.J.M.vanGelder@tudelft.nl (P.H.A.J.M. van Gelder), p.gehl@brgm.fr (P. Gehl), m.a.hicks@tudelft.nl (M.A. Hicks), p.j.vardon@tudelft.nl (P.J. Vardon).

https://doi.org/10.1016/j.nucengdes.2025.114558
Received 11 June 2025; Received in revised form 16 October 2025; Accepted 17 October 2025
Available online 5 November 2025

structures and/or components (SSCs), are also subject to uncertainty. Finally, these infrastructures are subject to both technical as well as human risks (Fan et al., 2020). Thus, high-reliability industries require a multi-hazard risk integration framework that considers even low-probability external hazard events and their combinations. The risk framework should account for the impact of these hazards on complex, dependent systems, and allow for inclusion of expert judgement where data are sparse (Cooke, 1991). The risk framework must also be suitable for tracking uncertainties in the data and propagating them to the final risk estimate.

Multi-hazard risk assessment involves the consideration of not only different hazards but also their interactions with other hazards (Mignan et al., 2014, van Erp and van Gelder, 2015). Interactions between hazards happen in two ways: (i) hazards may independently occur within a brief time window resulting in cascading damage (Gardoni and LaFave, 2016), or (ii) the occurrence of one hazard may lead to one or more other hazards (Pescaroli and Alexander, 2018). The impact on SSCs from hazards, i.e. their fragilities, can be classified into two types: (i) the SSCs are impacted by multiple hazards at the same time (Zio, 2016) or, (ii) multiple hazards affect the SSCs at various times, progressively damaging them over time (Dong et al., 2013). Due to the tree-like structure of events that characterise such cascading effects, the resulting interdependencies, and the uncertainty associated with physical mechanisms, humans and random effects, modelling of multi-hazards is best tackled using a probabilistic approach (Koks et al., 2019).

Probabilistic safety assessment (PSA), also referred to as probabilistic risk assessment (PRA), is the most prevalent risk assessment methodology used in various industries (Bedford and Cooke, 2001). Within PSA, event sequence diagrams and event trees along with fault trees are typical tools used to integrate hazards and their impact on systems (Mosleh, 2014). An event tree is an inductive tool to define the logical sequence of events progressing to various end-states. A fault tree analysis (FTA) is a logical deductive process where the occurrence of a hazard is assumed and is often combined with event trees, to evaluate probabilities of occurrence of undesired end-states ('top events'). For example, damage to the reactor core can be a top event of interest at a nuclear power plant (NPP). The fundamental steps in FTA are: (i) qualitative development of the logical representation of states leading to the top event, and (ii) quantitative evaluation of probability of the top event based on probabilities of basic events and other intermediary events. Shen et al. (2022) and Shen et al. (2023) conducted surveys with PSA professionals which highlighted five main challenges in existing PSA modelling:

(i) Incorporating Bayesian updating
(ii) Expanding PSA to external events
(iii) Improving human reliability modelling
(iv) Improving SSC dependency modelling
(v) Incorporating dynamic modelling

Several improvements have been previously made to the basic implementation of FTA within the PSA methodology, to meet the demands of high-reliability industries and address the above challenges. Bayesian updating of probabilities has been integrated with PSA methods (Kelly and Smith, 2011). Statistical or chronological dependencies between events can be captured, at least partially, by combining FTA with event trees. In addition, correlation coefficients have been included in FTA to account for statistical dependencies (Ebisawa et al., 2015). Dynamic fault trees can also consider dependence over time and aid in the modelling of complex systems (Siu, 1994; Yazdi et al., 2023). Uncertainty propagation and tracking is not inherent to FTA, but adaptations such as incorporating the Monte-Carlo method (Durga Rao et al., 2009, Zio, 2013) and fuzzy approaches (Suresh et al., 1996) have been coupled with FTAs to handle uncertainty in PSA. However, each of these aspects often require unique implementations of FTAs limiting their use when multiple challenges occur together at facility-scale.

The advantages of Bayesian networks (BNs) over fault trees are well-established in the literature (Mohan et al., 2021). Bayesian networks (BNs) are a directed graphical probabilistic representation of events and their interdependence (Koller and Friedman, 2009). BNs have specifically been proposed for industries, such as in the chemical (Khakzad et al., 2011), oil and gas (Kanes et al., 2017), aviation (Ale et al., 2006, Mohaghegh et al., 2009) and nuclear (Lee and Lee, 2006) sectors. Literature addressing the applicability of BNs to the aforementioned five challenges to PSA is summarised below.

Bayesian updating, consideration of statistical dependencies and uncertainty propagation are all inherent to BNs, unlike fault trees where additional modifications are required to incorporate these features. Liu et al. (2015) presented a BN-based risk framework for considering multi-hazard and fragility, considering regional risk but not industrial risk. Shen et al. (2025) present a Monte Carlo augmented BN method for modelling external flood risk in nuclear PSA. Kwag and Gupta (2017) demonstrated that BNs are better suited than FTA for multi-hazard risk for nuclear power plant risk, considering earthquake, wind and flood hazards without interactions at the hazard level. Segarra et al. (2023) present a BN framework for performing multi-unit seismic PSA, which accounts for dependencies at the level of consequences. BNs have also been shown to be effective in independently modelling either the reliability of human actions (Mkrtchyan et al., 2016) or technical systems (Cai et al., 2019). Groth and Swiler (2013) use BNs for modelling human reliability, while highlighting the need to bridge human reliability modelling methods with overall PSA risk integration tools. Dynamic modelling of technical systems in nuclear power plants and other complex systems have also been implemented using BNs (Mamdikar et al., 2022; Yuan et al., 2018). Another differentiating feature of BNs is their ability to incorporate continuous random variables without the need for additional modifications (Jensen and Nielsen, 2007). Machado et al. (2023) also recommend that the incorporation of continuous variables and testing with realistic cases are also key to further development of BN use in risk assessments.

The above studies demonstrate BN capabilities to improve risk integration in PSA. However, adoption in practice has been limited due to lack of a framework and demonstration at facility scale, to transition from existing tools while simultaneously realising all the advantages of BNs. Previous studies have not jointly considered interactions between external hazard events and between their consequences. Moreover, reliability of technical systems and human actions have not been modelled together with multi-hazard interactions – this would allow for dependencies at the system level to be accounted for in the facility-wide BN risk model. Facility-scale models also have several complex systems and using continuous variables in the risk model can prohibitively increase the computation load. Modelling multi-hazard and fragility interactions can also be computationally expensive (Kameshwar et al., 2019). BN modelling solutions for complex systems, such as the object-oriented BN (OOBN) method (Koller and Pfeffer, 2013), need to be assessed in the multi-hazard context. The novelty of this study is in formalising and demonstrating the transition from existing PSAs to multi-hazard risk assessment using BNs, with simultaneous consideration of:

(i) interactions between external hazard events
(ii) reliability modelling of SSCs and operator actions
(iii) integration at facility scale, while considering dependencies and computational demands

A stepwise methodology is presented, for migrating from existing risk integration tools to a BN in a multi-hazard scenario. Subnetworks are used to model different technical systems and human actions. One of the subnetworks takes advantage of the BN's ability to incorporate continuous variables, while another incorporates expert judgement. The subnetworks are then integrated based on hazard interactions and other

induced dependencies (cascading effects). Two approaches to subnetwork integration – OOBNs and a unified BN – are presented and compared for their ability to predict risk accurately while balancing computational requirements. The entire methodology is implemented for a realistic multi-hazard accident scenario at a nuclear power plant to obtain a facility-level risk BN.

The paper is organized as follows. In Section 2, the background of BN's is presented with a focus on integrating multiple hazards. In Section 3, the proposed development steps are presented and illustrated on a case study for a nuclear power plant. The numerical results of the case study are shown in Section 4, followed by a discussion of the results, challenges and their potential solutions in Section 5. The conclusions and recommendations from the study are presented in Section 6.

2. Bayesian network-based multi-hazard risk integration methodology

A BN is a specific application of Bayesian probability theory. It is a directed acyclic graph, composed of 'nodes' that correspond to random variables and 'arcs' that link dependent variables. The directions of the arcs indicate the dependencies between the nodes (i.e., directed), and these arcs never cycle back from the child nodes to the parent nodes (i.e., acyclic). The network is a visually explicit representation of the mutual relationship between random variables and represents the joint probability distribution (JPD) of all random variables within the model (Koller and Friedman, 2009). A simple example is shown in Fig. 1. The random variables in the network may be represented by discrete or continuous probability distributions.

The dependencies between random variables are usually encapsulated within conditional probability distributions (CPDs – given by $p(\mathrm{X_i}|Parents(\mathrm{X_i}))$, where p indicates probability and | indicates conditionality) at each node. The JPD is given by the chain rule of BNs:

$$p(X_1, X_2, \cdots, X_n) = \prod_{i=1}^{n} p(X_i|Parents(X_i)) \quad (1)$$

The JPD of the example in Fig. 1 is given by:

$$p(X_1, X_2, X_3, X_4) = p(X_1)p(X_2|X_1)p(X_3|X_1, X_2)p(X_4|X_2) \quad (2)$$

The JPD can be queried to obtain the state of a random variable, given the beliefs regarding the other variables, via Bayesian inference. In other words, BNs can be used to answer probabilistic queries in a multivariate problem when one or more variables have been observed, which includes predictive-, diagnostic- and causal reasoning.

When multiple BNs need to be combined, one of two approaches may be adopted – an object-oriented Bayesian network (OOBN) or a single, unified BN. The unified BN approach is self-explanatory and is simply one large BN comprising all the subnetworks and the arcs connecting them. An OOBN (example in Fig. 2) contains instance nodes which represent a BN fragment that is called a class. Instantiating the class produces objects which are particularly useful for model re-use, encapsulation and effective model construction (Koller and Pfeffer, 2013; Kjærulff and Madsen, 2013). Using OOBNs also helps in modelling subnetworks as separate objects while distinctly visualising their interactions within the larger risk model.

Various OOBN approaches exist, each involving distinctive features and capabilities (e.g., Koller and Pfeffer, 2013; Liu et al., 2016). Dynamic OOBNs can be used in the modelling of complex systems with time dependence (Zhu et al., 2022; Weber and Jouffe, 2006). A basic OOBN approach, available in Agena.AI® – the program used for BN implementation in this study, is adopted here. Each object within the overall risk model is an individual BN. Each individual object may consist of one or more "input" and "output" nodes. In Fig. 2, Object 1 and Object 2 are individual BNs, with variable *C* acting as the output node in Object 1 and as the input node in Object 2. Objects are connected by linking the output node of the hierarchically higher object (1) to the input node of the lower (2). Hence, the interacting input and output nodes of the two connected objects are required to be identical. The link between these two nodes passes the complete set of probability values from the input node to the output node. Minor variations are possible, where a summary statistic (e.g., mean) may be passed between two continuous nodes or the value of a single state of a discrete output node may be passed as a constant value to a continuous input node. The interaction between the input and output nodes of various objects is defined in a 'master' network – the OOBN risk model. The last, child node in the hierarchically lowest object (e.g., *F* in Fig. 2), typically yields the probability distribution for the top event considered in the risk model.

In the extremes, every node in the risk model could be a separate object (or subnetwork) of its own or the entire model could be a single network, i.e. the unified BN approach. The selection of subnetworks and input and output nodes is subjective. However, the modeller has to be

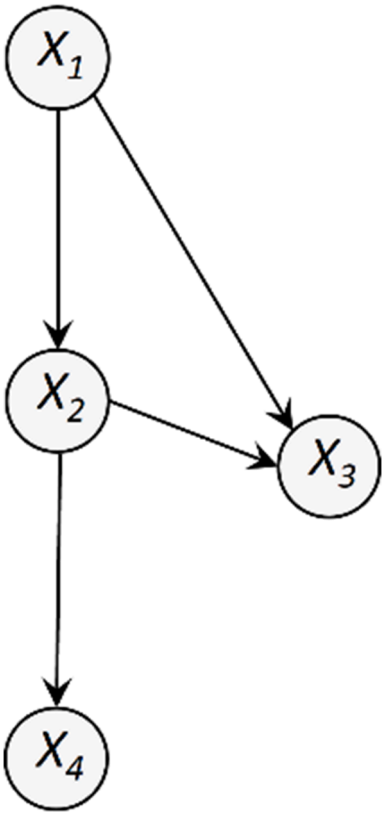


Fig. 1. Example of a Bayesian network; X_i indicates a random variable.

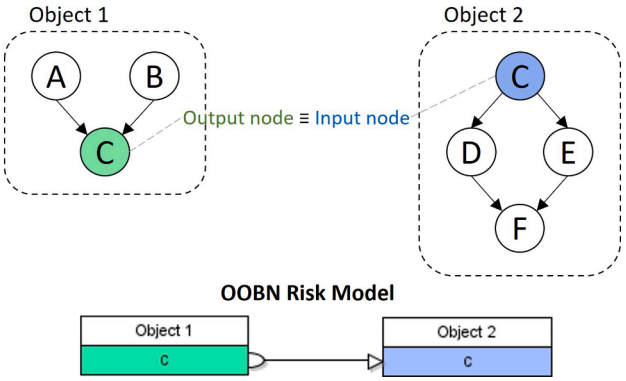


Fig. 2. Example of an object-oriented Bayesian network.

careful to ensure that impactful dependencies are not lost while breaking up the risk model into subnetworks. This is because only the marginal probabilities are passed from output nodes in one subnetwork to the input nodes in another (as in Fig. 2). Dependencies amongst output nodes may be lost when multiple output nodes from parent subnetworks are input into a child subnetwork. Hence, in such cases, it is advisable to avoid breaking up BNs into subnetworks while using the OOBN approach. If deemed beneficial despite the loss of dependencies, the impact of such dependencies must be rigorously evaluated by comparing the OOBN probability estimates with those from the unified BN approach.

3. Risk integration methodology and implementation

Fig. 3 presents the stepwise multi-hazard risk methodology using BNs that is proposed in this study. The methodology aids in transitioning from existing risk modelling tools such as event sequence diagrams (ESDs), FTs and ETs but is not limited to these tools. Its key facet is its suitability for facility-wide risk assessment, with the use of Bayesian subnetworks for integrating multi-hazards and the reliability of different systems as well as human actions. Multi-hazard and fragility analyses, such as those recommended in Daniell et al. (2019) and Foester et al. (2024), are integral to this methodology for modelling the relevant events and their marginal or conditional probabilities. Where event

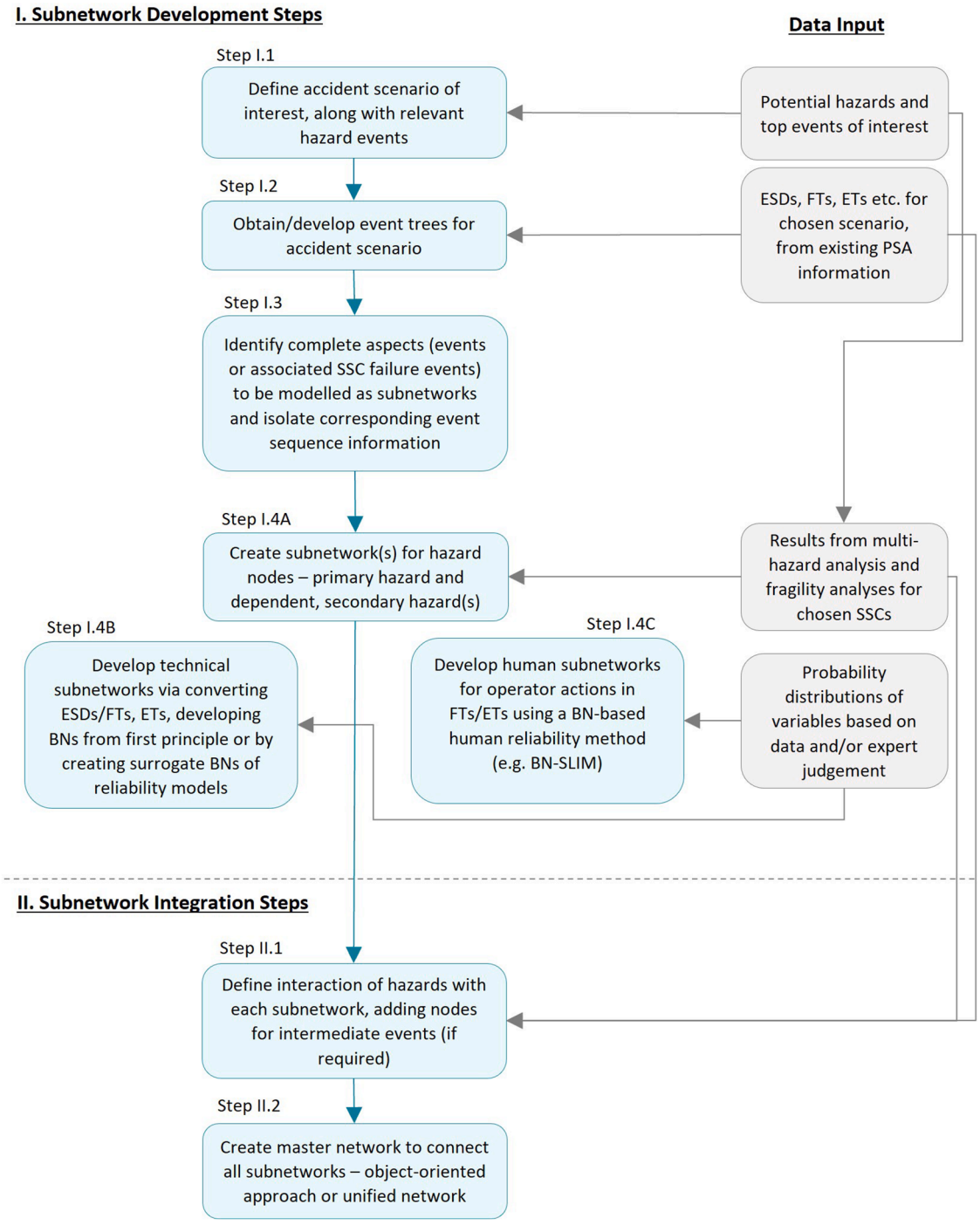


Fig. 3. Multi-hazard risk integration methodology using Bayesian networks.

probabilities are unavailable, either from historical data or physics-based models, expert judgement can be integrated through structured elicitation (Cooke and Goossens, 2008; Hemming et al., 2018).

3.1. Example implementation for a nuclear power plant

An example accident scenario from a high-reliability industry – nuclear power generation – is considered. The goal of this example is to demonstrate the above risk methodology for a realistic multi-hazard case, to obtain the probability of a facility-level top event, and to understand the sensitivity of this prediction to changes in reliability of technical systems and human actions.

The nuclear power plant (NPP) considered in this case is the virtual power plant (VPP) developed as part of the NARSIS EU H2020 project (see Acknowledgements). The VPP is a generic generation III + NPP, whose associated event and fault trees are obtained from Bruneliere et al. (2018). The VPP design is similar to other power plants in Europe and therefore, the accident scenario described below is applicable to many operational plants. Any differences that could arise at a specific power plant, do not impact the principles demonstrated in using the methodology. While the VPP was developed using a specific design, there is no specific location in Europe associated with the VPP. Thus, for the consideration of external hazard events, a decommissioned NPP based in Mülheim-Kärlich, Germany is chosen as the site of interest. The VPP does not correspond to the actual design details of the Mülheim-Kärlich NPP. This location is selected due to the prevalence of a plausible multi-hazard scenario and to reflect a realistic location where a NPP would indeed be stationed. A multi-hazard analysis for the site is presented by Daniell et al. (2019). For the purpose of this study, earthquake and flooding were the external hazard events that were considered as these were most relevant at the site. Each step of the risk integration methodology is applied to this example case.

3.2. Subnetwork(s) development

3.2.1. Step I.1 – Define accident scenario

- Loss of offsite power (LOOP) has occurred following one or more external hazard events – earthquake and/or flooding. LOOP is the initiating event for the accident scenario.
- During the LOOP situation, failure of all four emergency diesel generators (EDGs) would lead to a partial station blackout situation (referred to as SBO, hereafter). Total Station Blackout would involve failure of additional two Station Blackout Diesel Generators known as Ultimate Diesel Generators. Total station blackout is not considered in this study.
- Following SBO, failure of the steam generator used for residual heat removal (or 'partial cool down'), would lead to failure of 'secondary cool down' (SCD).

Risk assessment of the accident scenario aims to evaluate the annual probability of SBO and SCD failure following LOOP. Such a specific scenario is chosen for the following reasons:

(i) To include sufficient complexity beyond system-level, such that the use of subnetworks is necessary or potentially advantageous.
(ii) To include sufficient complexity in the risk model in terms of number of SSCs that require integration of different reliability modelling methods.
(iii) To limit the number of event and fault trees involved, as the goal of this example is to demonstrate the proposed methodology. For instance, the accident scenario could have been extrapolated to events beyond SCD failure. Nevertheless, the event and fault trees used are realistic for a real NPP and are adopted completely from Bruneliere et al. (2018).
(iv) To include operator actions so that human error probability (HEP) may be calculated within the overall risk BN.

In nuclear risk terminology, this risk assessment would constitute a Level 1 PSA – safety assessment of events leading to reactor core damage. However, the risk methodology presented in this study can be extended to Level 2 (radioactive release frequency) and Level 3 (public consequences) PSAs due to the features and versatility of BNs (Zhao et al., 2021). Furthermore, BNs can potentially function as a link to provide continuity between the various levels of PSA.

3.2.2. Step I.2 – Obtain existing PSA information, including event and fault trees

Fig. 4 shows the event progression from LOOP to SBO, while Fig. 5 shows the event progression from SBO to SCD (denoted as SCD_11 in the event tree). The description of events and corresponding codes in Figs. 4–7 can be found in Bruneliere et al. (2018) and Darnowski et al. (2022). The reliability data of various SSCs are related to their failure modes using the NUREG database (Idaho National Laboratory, 2007) and hence, the data is applicable to a real engineering context.

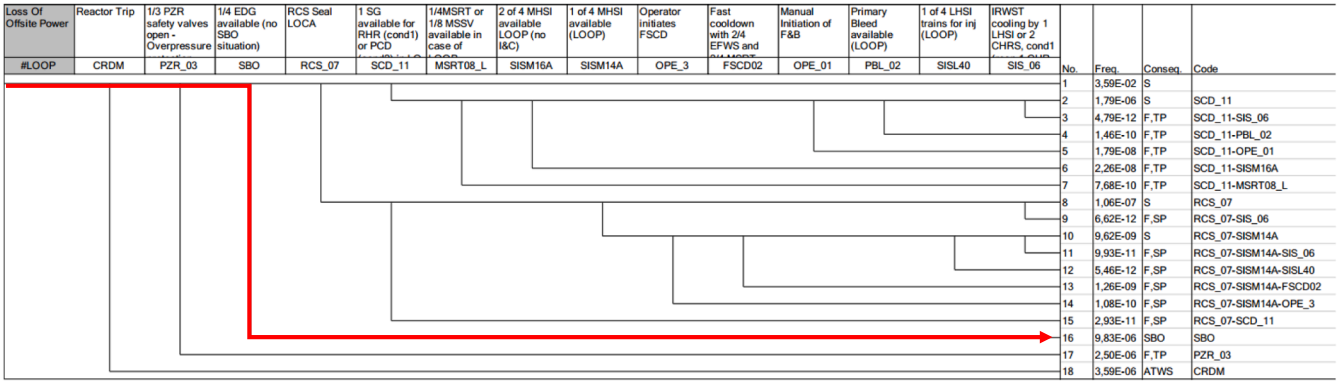
NPPs typically have specific external event PSAs where separate event and fault trees are used to model interaction with external hazards. However, within the VPP developed in Bruneliere et al. (2018), the PSA method was applied only for internal events. Often, even when external events are modelled, the interactions between different hazard trees are ignored, resulting in underestimation of top event risk in a multi-hazard scenario (Choi et al., 2021). Hence, multi-hazard and fragility analyses (Daniell et al., 2019; Gehl and Rohmer, 2018) are recommended to enhance existing event and fault trees. While several systems and components are considered in the above fault trees, no structures are involved. One structure that can be critical in this accident scenario is the flood defence whose performance determines if the plant will be subject to internal flooding. Hence, the flood defence dike is considered as an example structure whose multi-hazard fragility induces cascading effects that consequently impact the internal event and fault trees. Other buildings that house the above systems and components are not considered for ease of demonstration. Fig. 8 shows an example event tree representation of the accident sequence when there is a flood event only. Similar event trees can be developed, including occurrence or non-occurrence of hazard events.

The following assumptions are also made regarding the impacted SSCs:

(i) The interaction of hazards is limited to the flood defence dike, EDGs and a chosen operator action. While the fragilities of other SSCs will impact the top event probability, they are superfluous for the purpose of demonstration.
(ii) The bottom of the dike is at datum and the crest is at height 5 m. The two EDGs each are set at an elevation of 4 m and 12 m from the datum. The topography in the plant interior is assumed to be flat between the dike and the EDGs.
(iii) If an EDG is flooded, it is assumed to have failed completely. This also implies that flooded equipment cannot be damaged by earthquakes and hence these EDGs and associated common cause failure (CCF) events would not feature in the sequence of earthquake-based failure events.

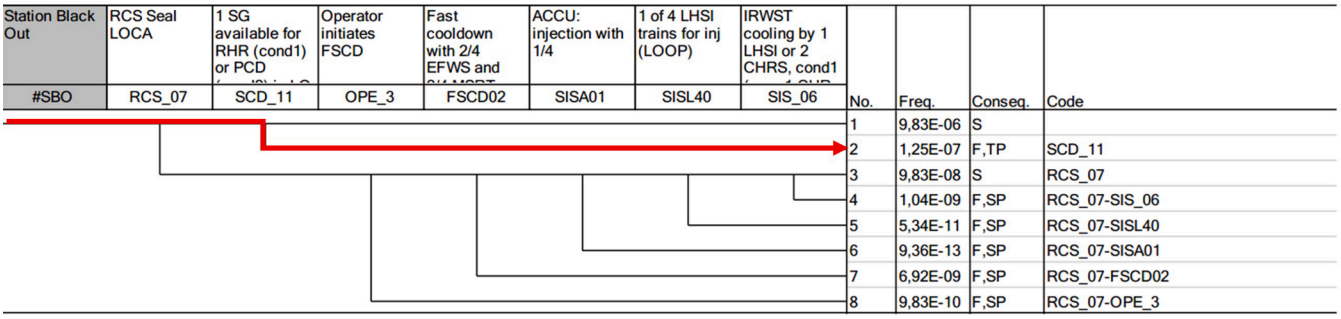
3.2.3. Step I.3 – Identify subnetworks to be built

In general, the choice of which systems, sub-systems or events must be confined within a single subnetwork is subjective and depends on the risk model and modeller. These choices influence the visual complexity of the integrated risk model, its computational time and its diagnostic capabilities. If dependencies are lost during division of subnetworks, this can also impact the (calculated) probability of the top event. The impact on these aspects, for the subnetwork choices made in this study, are discussed later with the results.



ID	Description	ID	Description
CRDM	Reactor Trip	OPE_3	Operator initiates FSCD
PZR_03	1/3 PZR safety valves open - Overpressure protection	FSCD02	Fast cooldown with 2/4 EFWS and 2/4 MSRT
SBO	1/4 EDG available (no SBO situation)	OPE_01	Manual initiation of F&B
RCS_07	RCS seal LOCA	PBL_02	Primary Bleed available (LOOP)
SCD_11	1 SG available for RHR (cond1) or PCD (cond2) in LOOP	SISL40	1 of 4 LHSI trains for inj (LOOP)
MSRT08_L	1/4MSRT or 1/8 MSSV available in case of LOOP	SIS_06	IRWST cooling by 1 LHSI or 2 CHRS, cond1 (resp 1 CHRS cond2) in LOOP
SISM16A	2 of 4 MHSI available LOOP (no I&C)		
SISM14A	2 of 4 MHSI available (LOOP)		

Fig. 4. Event tree with loss of offsite power as initiating event, leading to station blackout, with event descriptions below (after Bruneliere et al., 2018).



ID	Description
RCS_07	RCS Seal LOCA
SCD_11	1 SG available for RHR (cond1) or PCD (cond2) in LOOP
OPE_3	Operator initiates FCSD
FCSD02	Fast cooldown with 2/4 EFWS and 2/4 MSRT
SISA01	ACCU: injection with 1/4
SISL40	1 of 4 LHSI trains for inj (LOOP)
SIS_06	IRWST cooling by 1 LHSI or 2 CHRS, cond1 (resp 1 CHRS cond2) in LOOP

Fig. 5. Event tree showing progression from station blackout to secondary cooldown failure, with event descriptions below (after Bruneliere et al., 2018).

In Fig. 5, the SCD_11 event has the highest frequency within the event tree, which is a reason for the choice of this event within the accident scenario. Another reason is that the fault tree associated with the SCD_11 event contains two operator actions, one of which is modelled as a separate subnetwork using the BN-SLIM approach (Abrishami et al., 2020). The fault trees corresponding to each of the above events, in Fig. 6 (SBO) and Fig. 7 (SCD), are both obtained from Bruneliere et al. (2018) and are modelled as separate subnetworks. Apart from the SSCs involved in these event trees, the flood defence at the NPP is likely to be a key structure influencing the accident scenario, since flooding is one of the hazards being considered. Therefore, the geotechnical stability of an earthen dike is modelled as one of the subnetworks of interest. Unlike

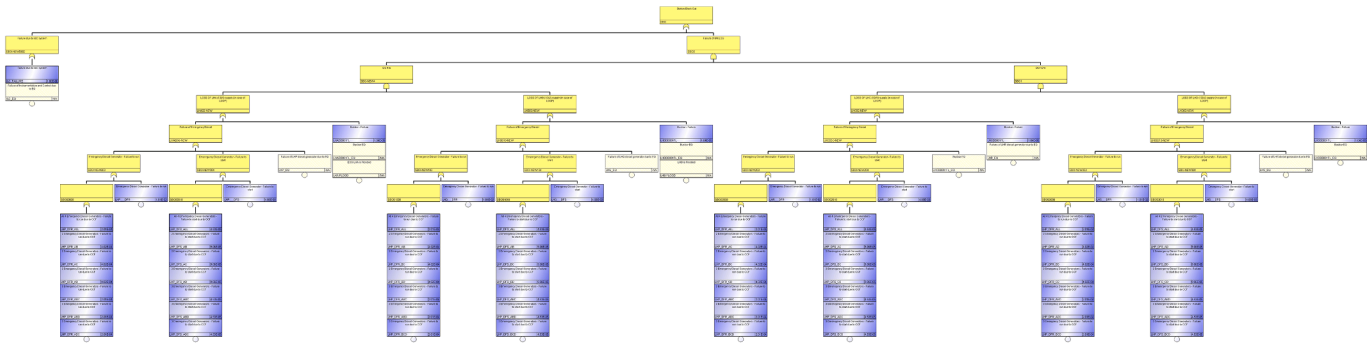


Fig. 6. Complete station blackout fault tree – see Supplementary Fig. S1 (after Darnowski et al., 2022).

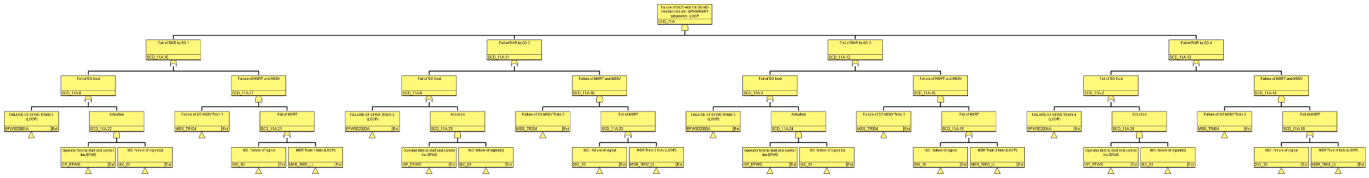


Fig. 7. Secondary cooldown failure main fault tree, without sub-fault trees – see Supplementary Fig. S2 (after Darnowski et al., 2022).

the other subnetworks, the flood defence subnetwork also requires the use of continuous variables. In addition to the above subnetworks that model the failure of systems or groups of systems, subnetworks are developed for modelling hazards and their interactions, and for LOOP. More subnetworks can be included to add further detail to the facility-level risk assessment. For instance, the structural failure of either the EDG building or the reactor building may be modelled. However, for the simplicity of demonstration further SSCs are not considered in this study.

3.2.4. Step I.4A – Building multi-hazard subnetworks

As mentioned previously, earthquake and flooding hazards are considered. According to the multi-hazard analysis in Daniell et al. (2019), flooding is considered as the primary hazard. The plausible multi-hazard scenario is that, post an extreme rainfall event, the adjacent Rhine River could be in flood. While flood water is banked against the flood defence of the power plant, an earthquake event could simultaneously damage the flood defence, leading to flooding of the power plant. Hence, in addition to only the flood risk, it is necessary to consider the dependence between earthquake and flooding. Firstly, a primary hazard subnetwork with only the flooding node is created. Next, a multi-hazard subnetwork is created consisting of flood water level as the parent node and the earthquake peak ground acceleration (PGA) as the child node. The conditional dependence of earthquake PGA with the flood water level, as derived from Daniell et al. (2019), is based on the multi-hazard curve shown in Fig. 9.

3.2.5. Step I.4B – Building technical subnetwork(s)

3.2.5.1. LOOP 'subnetwork'. As described in the accident scenario, LOOP is the initiating event that sets off internal plant events. The initiating event (or sequence of events) is typically modelled as a subnetwork of its own. In this case the LOOP event is an initiating event external to the NPP, and there are no preceding internal events. Hence, LOOP is represented as a subnetwork with just a single node. The annual probability of occurrence of LOOP is assumed to be 3.59×10^{-2} based on data (Schroeder, 2015) which includes the impact of various external events. The dependence of the probability of occurrence LOOP on earthquake and flooding is not explicitly considered in this example but can be easily included where data are available.

3.2.5.2. Flood defence subnetwork. The details of the development of the flood defence subnetwork and its results are presented in Mohan et al. (2019) and Mohan et al. (2021). This subnetwork (shown in Fig. 10) acts as a surrogate model to an advanced numerical model – following the random finite element method (Fenton and Griffiths, 2008; Hicks and Samy, 2004) – used to estimate reliability of the flood defence dike.

The concepts demonstrated using the flood defence subnetwork may be used in building surrogate models for any system (Mohan et al., 2019). The BN was shown to be a convenient tool for reliability updating while providing a visual representation of the interaction of model parameters, both amongst themselves as well as with the final reliability estimate. The value of additional testing for maintenance of the dike was also evaluated from the BN. This subnetwork also demonstrates the capability of BNs to incorporate continuous probability distributions and the use of hybrid BNs in risk assessment.

3.2.5.3. SBO subnetwork. This subnetwork pertains to the fault tree leading to SBO, during LOOP, where a system of four EDGs must fail simultaneously. Since existing information from a traditional PSA approach is available, it is efficient to use this to construct a BN. The subnetwork is constructed by converting the fault tree shown in Fig. 6 following the algorithm given by Bobbio et al. (2001). Fig. 11 shows the BN corresponding to the SBO fault tree, including CCF events.

3.2.5.4. SCD subnetwork. As with the SBO subnetwork, the SCD subnetwork is constructed by converting the corresponding event and fault trees. The SCD subnetwork, including all CCFs, comprises 742 nodes and 1155 arcs, making legible visualisation with node labels difficult. Therefore, the subnetwork is not presented here as a figure. Since SBO is a precursor event to SCD, there are dependencies between the two subnetworks derived from the event tree. In such a case, it is important to evaluate whether it is beneficial to keep the subnetworks separate or merge them together. When there are only a few interactions between the nodes of two subnetworks, it is more feasible to keep the subnetworks as separate objects, since only a few input and output nodes

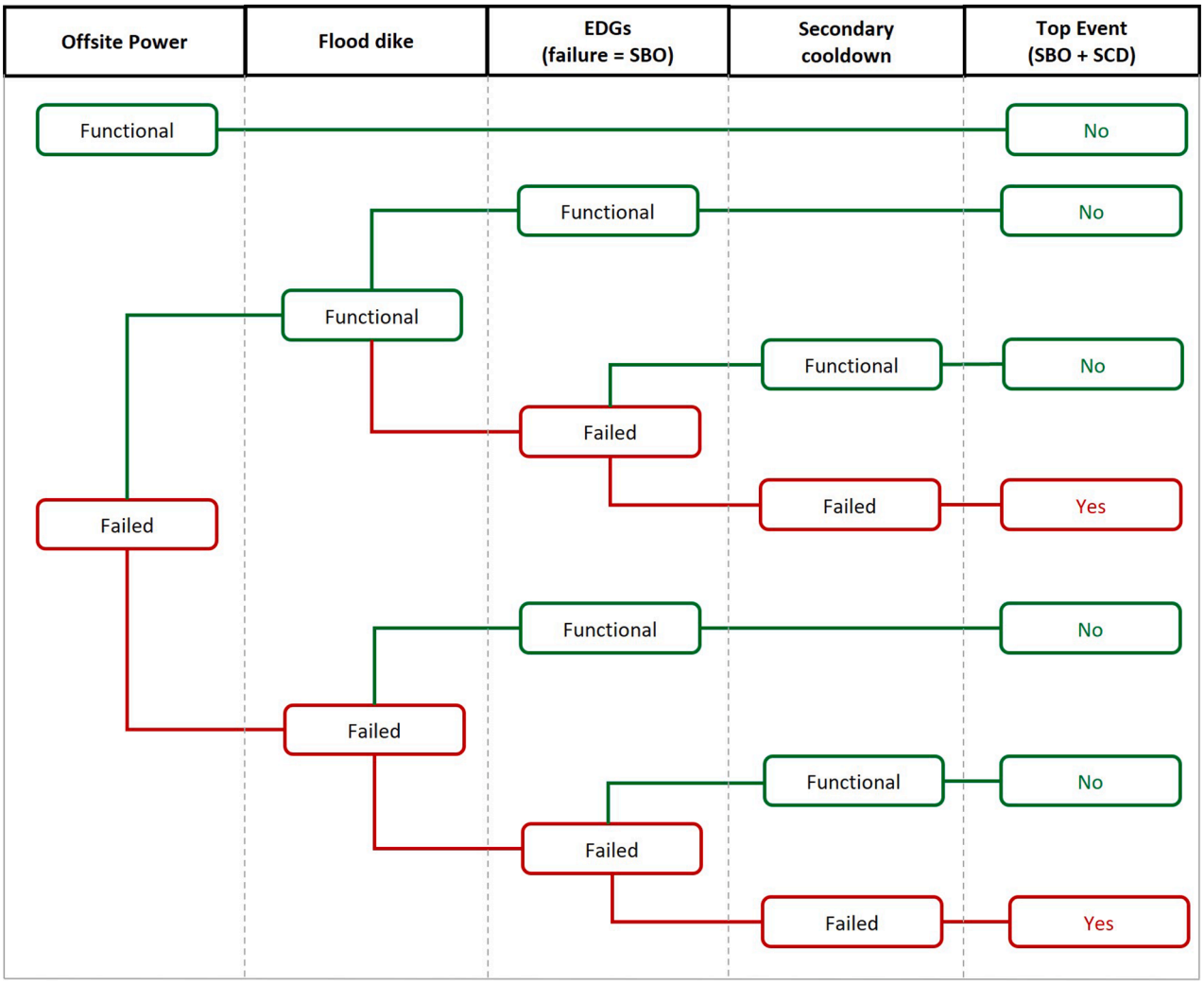


Fig. 8. Example accident scenario event tree (during flood event).

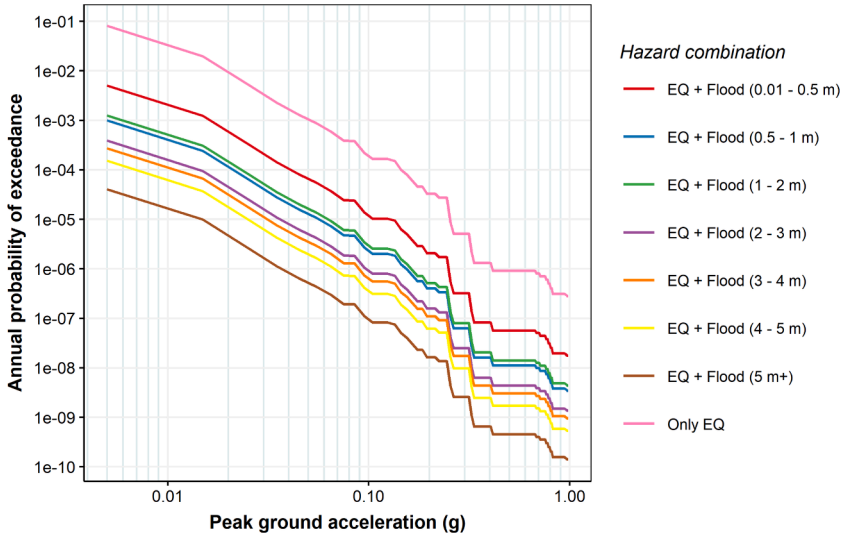


Fig. 9. Combined hazard curves for earthquake and flooding events.

would be required in the OOBN risk model, which in turn aids in better visual understanding. However, when many or most nodes in a subnetwork share dependencies with another subnetwork, it is often easier to merge the subnetworks rather than repeat several nodes in both objects. This avoids the near redundancy of one of the objects and prevents a busy visualisation of the OOBN risk model. In this case, the SCD

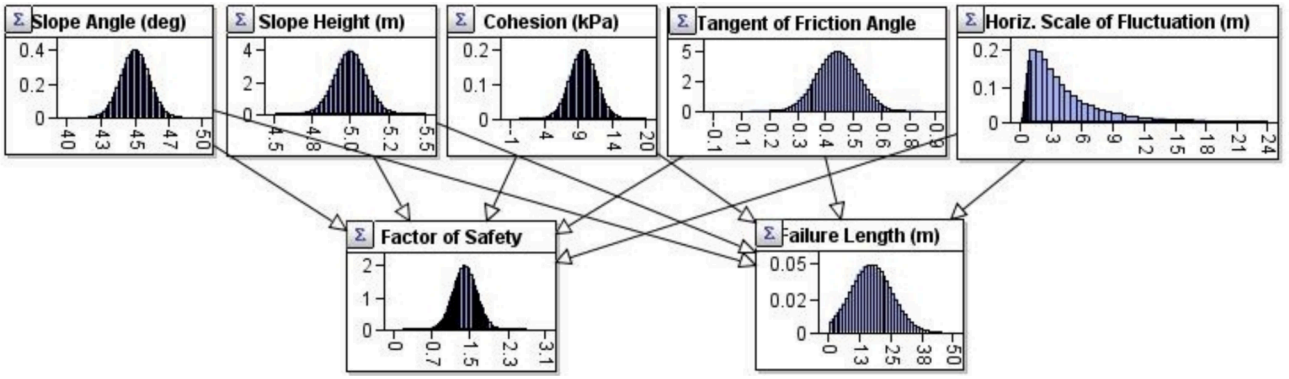


Fig. 10. Flood defence Bayesian network.

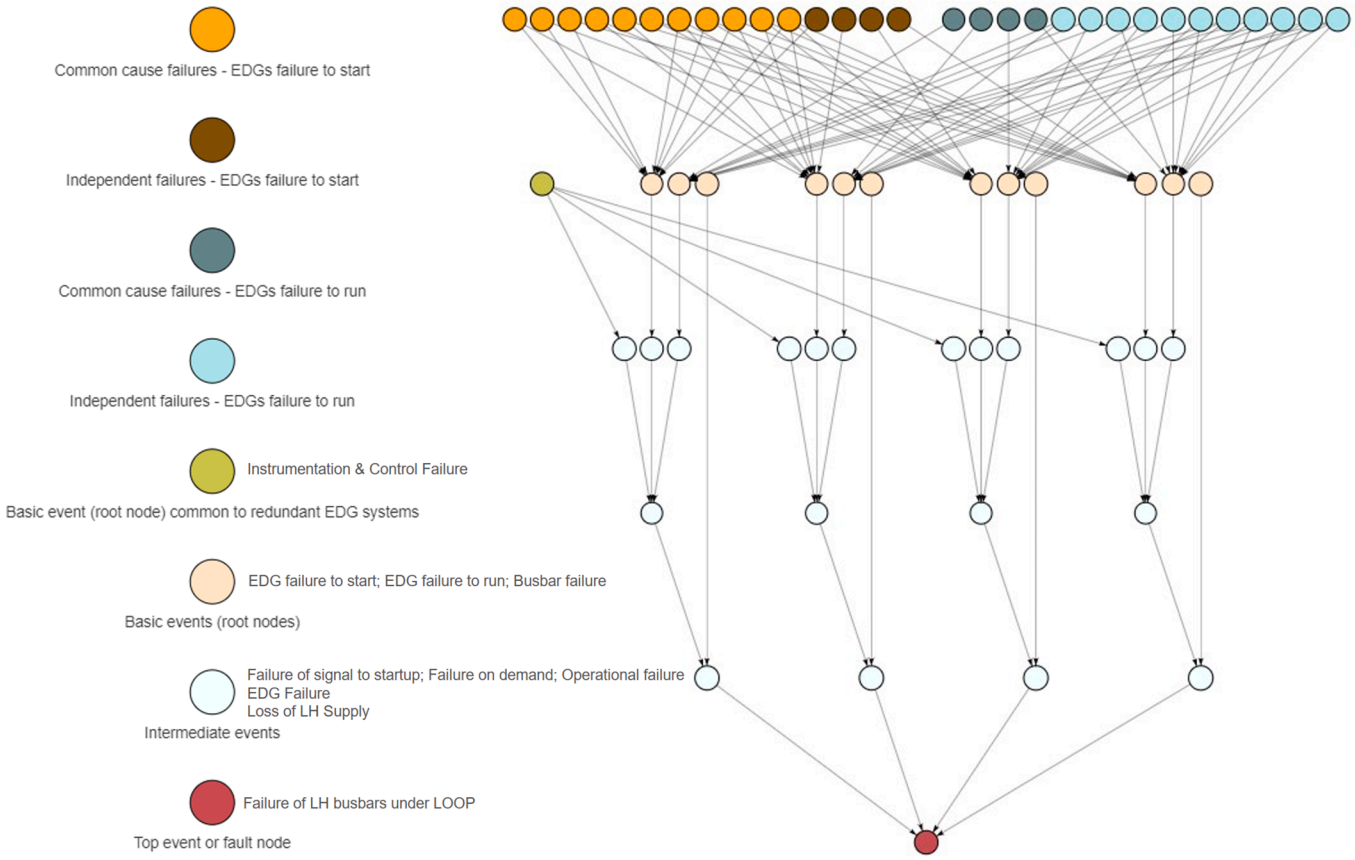


Fig. 11. SBO subnetwork – equivalent of fault tree in Fig. 6 with 4 redundant EDG systems.

subnetwork has numerous interactions involving all the basic and intermediate event nodes of the SBO subnetwork. Hence, the SBO subnetwork is merged into the SCD subnetwork and is presented as the SBO + SCD network by including the top event of the SBO subnetwork. Thus, this subnetwork consists of the SBO subnetwork as well as the operator action that is modelled in the human subnetwork discussed later.

3.2.6. *Step I.4C – Human subnetwork(s)*

3.2.6.1. Human subnetwork. The last subnetwork is a BN estimating the human error probability (HEP) associated with an operator action in the SCD subnetwork – operator fails to start and control the emergency feedwater system (EFWS). The BN-SLIM procedure developed as part of the NARSIS project is used for HEP estimation (Abrishami et al., 2020). Such a BN-based method allows for direct integration of the HEP estimation model with the overall risk assessment BN for the accident scenario. In addition, structured expert judgement elicitation was used in populating the probability distributions of performance shaping factors (PSFs) for the operator action. This demonstrates the ability of BNs to easily integrate expert opinion while representing and tracking the associated uncertainty, as opposed to the over-reliance on deterministic expert judgement in the conventional SLIM method. The details of the human subnetwork, including the expert elicitation process, are presented in Abrishami et al. (2020) and Mohan et al. (2021). When new data becomes available through events or simulations, the PSFs may be adjusted as required or the HEP may be validated against other models; however, this is beyond the scope of the current study. The description

of ratings for each PSF (R1–R9) are provided in Appendix A. Fig. 12 shows the human subnetwork.

3.3. Subnetwork integration

3.3.1. Step II.1 Hazard interaction with subnetworks

In this step, the interaction of the hazards subnetwork(s) with each of the other subnetworks is defined. In some cases, as described below, the inclusion of intermediate events/subnetworks may be necessary to define these interactions. The interaction within hazards was already modelled previously as a separate, multi-hazard subnetwork.

3.3.1.1. Hazard interaction with flood defence. Failure of the flood defence dike can be attributed to two main causes: random failure and hazard induced failure. In either case, flood defence failure leads to internal flooding – an intermediate event included as the output node of the flood defence subnetwork, indicating that the inside of the plant is flooded.

The flood defence subnetwork yields the probability of random failure via global stability failure, without hazard exposure, via the distribution of factor of safety. The hazard induced failure is assumed to occur via three modes – overtopping due to flooding, piping failure due to flooding and global stability failure due to the joint impact of flooding and earthquake. The fragility functions used for the piping and global stability failure modes are of the form:

$$F_R(x) = \Phi\left[\frac{\ln(IM/m_R)}{\beta_R}\right] \quad (3)$$

where $\Phi[.]$ is the standard normal probability integral, IM is the intensity measure for the respective hazard, m_R is the median fragility, and $\beta_R = \sigma_{lnR}$ is the logarithmic standard deviation (or dispersion) of the fragility. The fragility parameters used for piping and global stability are presented in Table 1. Overtopping failure occurs, simply, if the flooding level is higher than 5 m (the height of the dike). Fig. 13 shows the part of the overall risk BN (unified or OOBN) that pertains to the flood defence dike.

Table 1
Single and multi-hazard fragility models for piping and global stability failure modes.

Dike failure mode	Water level range (m)	IM	m_R	β_R
Piping (after Bachmann et al. (2013))	–-	Water level	3.48	0.22
Global Stability (after Tyagunov et al. (2018))	WL (0–1 m)	PGA	0.1182	0.2786
	WL (1–2 m)		0.1587	0.2778
	WL (2–3 m)		0.1899	0.2783
	WL (3–4 m)		0.2209	0.2797
	WL (4–5 m)		0.2620	0.2775

3.3.1.2. Hazard impact on human subnetwork. For the purposes of demonstration, simplified assumptions are made to integrate the human subnetwork within the accident scenario. Two PSFs – "Stressor" and "Available Time" – are assumed to be impacted by the occurrence of the hazard. It is beyond the scope of this study to investigate, in detail, the impact of hazards on PSFs. Instead, it is assumed that if a hazard – earthquake ground motion or internal flooding of the plant – were to occur, the PSFs would be similarly impacted, irrespective of the intensity of the hazards. Hence, a "hazard occurrence" node is introduced which is True when at least one of an earthquake PGA (>0.15 g) or an internal flood water level (>0.01 m) were to occur. The conditional probability distributions (CPDs) of the two chosen PSFs based on occurrence or non-occurrence of hazards are assumed, as shown in Table 2 and Table 3.

3.3.2. Step II.2 – Master network integrating all subnetworks

As discussed earlier, both approaches to subnetwork integration are implemented. The unified BN is a straightforward merging of all subnetworks. The entire SBO subnetwork is effectively comprised in the SCD subnetwork, as the SBO event is a precursor to the failure of the secondary cool down system. Hence, the SBO subnetwork integrated with hazards can directly be transposed into the SCD subnetwork. The

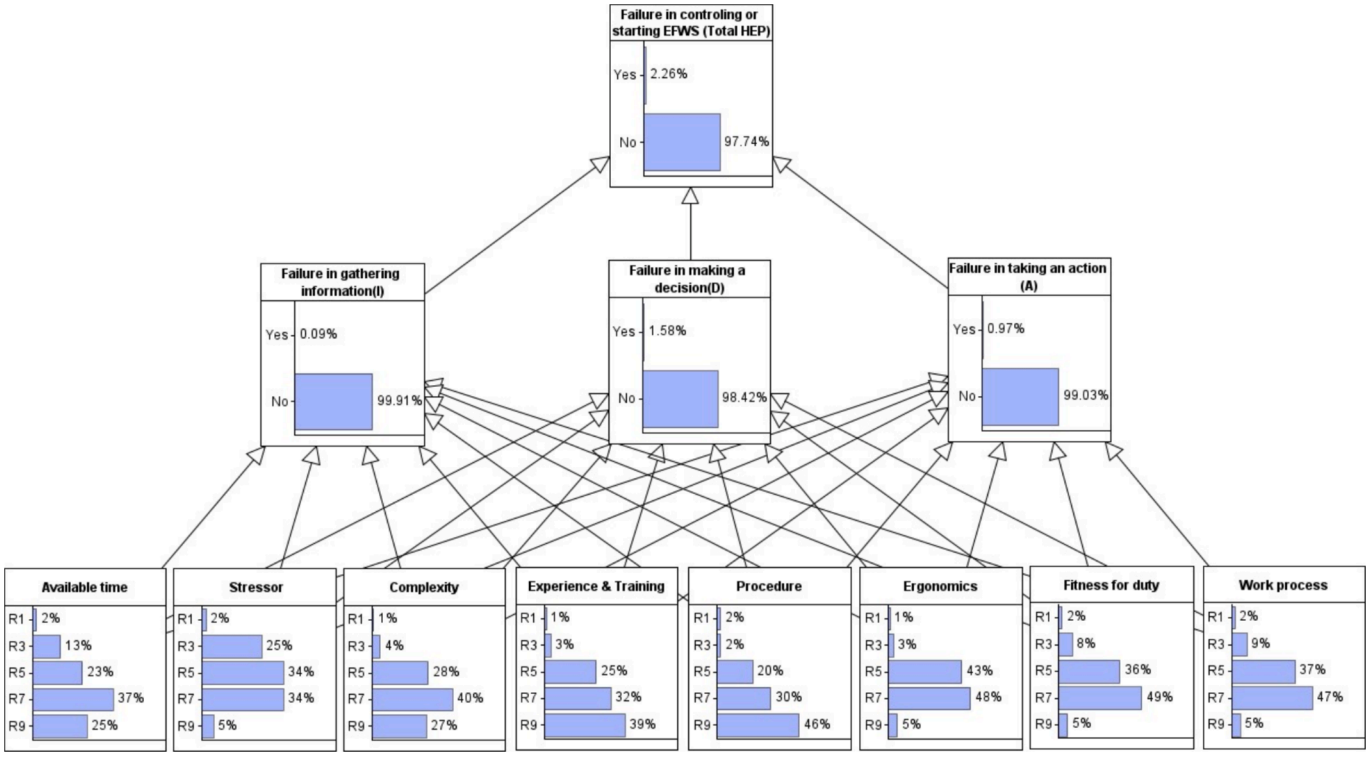


Fig. 12. Human subnetwork for operator action.

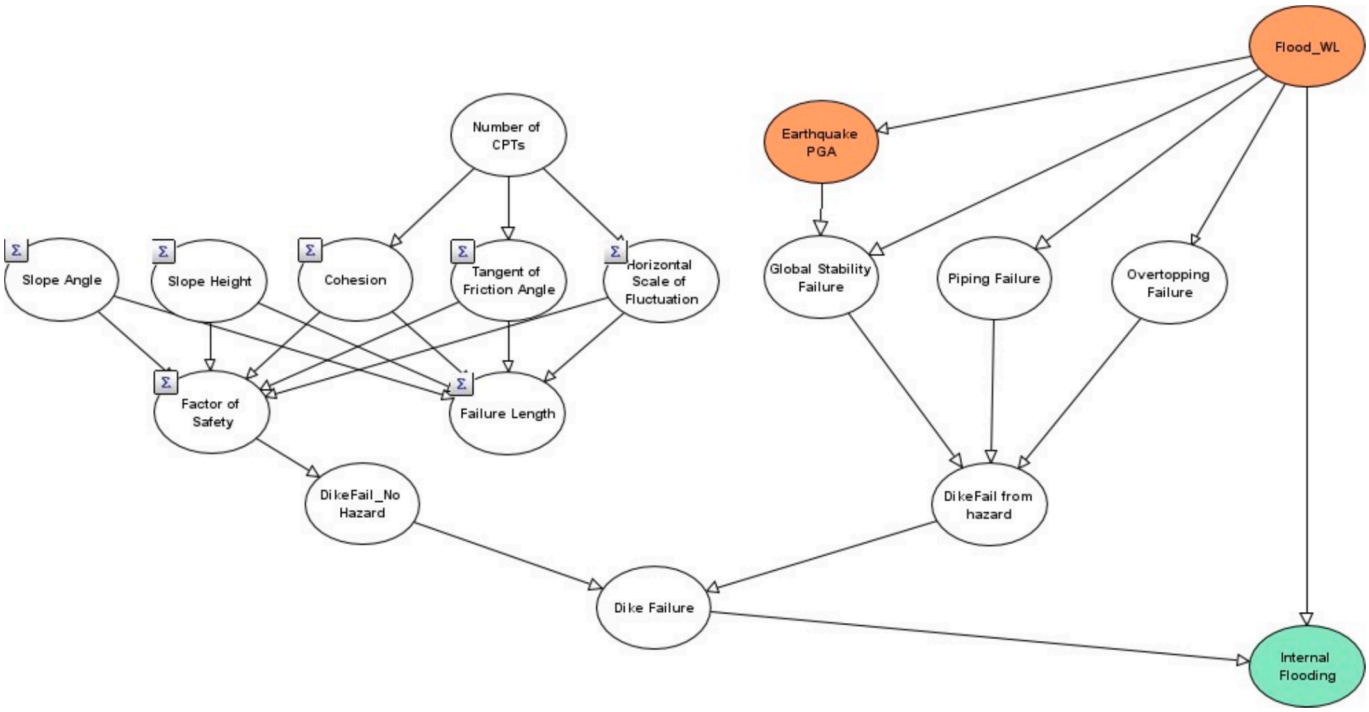


Fig. 13. Hazard integration with flood defence subnetwork.

Table 2
Conditional probability table of the PSF "Available Time" given hazard occurrence.

PSF rate	Hazard occurrence	
	False	True
R1	0.02	0.20
R3	0.13	0.40
R5	0.23	0.30
R7	0.37	0.08
R9	0.25	0.02

Table 3
Conditional probability table of the PSF "Stressor" given hazard occurrence.

PSF rate	Hazard occurrence	
	False	True
R1	0.02	0.20
R3	0.25	0.40
R5	0.34	0.40
R7	0.34	0.00
R9	0.05	0.00

flood defence subnetwork is connected to the SBO subnetwork via the hazards as well as the "internal flooding" node. This node is required to identify if flooding outside the plant has resulted in flooding within the plant due to failure of the flood defence. Further, the human subnetwork is integrated with hazards via the "hazard occurrence" node and the calculated HEP is the probability of "Operator failure to start and control EFWS" node being *True* in the SCD network. The "hazard occurrence" node is necessary since human behaviour is expected to change during hazard events, irrespective of whether earthquake, flooding or both hazards are occurring. Hence, the human subnetwork directly fits into the SCD subnetwork. Thus, the 4 subnetworks – SBO, SCD, flood defence and the human subnetworks – are all integrated with multiple external hazards. The accident scenario is completed by defining a top event "LOOP + SBO + SCD" which effectively checks for the joint occurrence of LOOP, SBO and SCD. Hazard interactions and corresponding failure progressions implied by the "internal flooding" and "hazard occurrence" nodes are idealised to simplify demonstration of the overall methodology. Alternatively, continuous nodes that are more sensitive to changes in hazard intensity can be readily integrated within the BN method, at the cost of increased computation.

The OOBN model is presented in Fig. 14. This approach is implemented using the same intermediary nodes, i.e., "hazard occurrence" and "internal flooding" nodes. The "earthquake PGA" node features in subnetwork "1_Multi-Hazard (Flood + EQ)" (subnetwork 1) as an output node. It also features in the "2_Dike_InternalFlooding" subnetwork (subnetwork 2) since internal flooding is dependent on both flooding and earthquake hazards. However, it is neither an input or output node in subnetwork 2 and, hence, does not appear in this subnetwork within the OOBN representation. Connecting the "earthquake PGA" output node from subnetwork 1 to subnetwork 2 would result in loss of dependence with its parent node, "Flood_WL". For this reason, another instance of the "earthquake_PGA" node is used within subnetwork 2. Such unique instantiations of hazard nodes, within the OOBN approach, can result in loss of some dependencies. "Hazard occurrence" features in both its own subnetwork (as output node) as well as in the human subnetwork (as input node). The "internal flooding" event node is part of the flood defence subnetwork as an output node, but also within the SCD subnetwork, as an input node.

4. Results

Table 4 lists the marginal probabilities of the top event of the unified BN (LOOP + SBO + SCD) as well as top events of each of the subnetworks within the unified BN. Also shown are their marginal probabilities without consideration of hazards. As expected, the marginal probabilities are not widely different, as the hazard events are rare at the considered site. However, if they were to occur, there could be a significant rise in conditional top event probabilities as shown in Fig. 15, which shows predictions from the unified BN for various multi-hazard intensities.

From Fig. 15 it is evident that the conditional top event probability

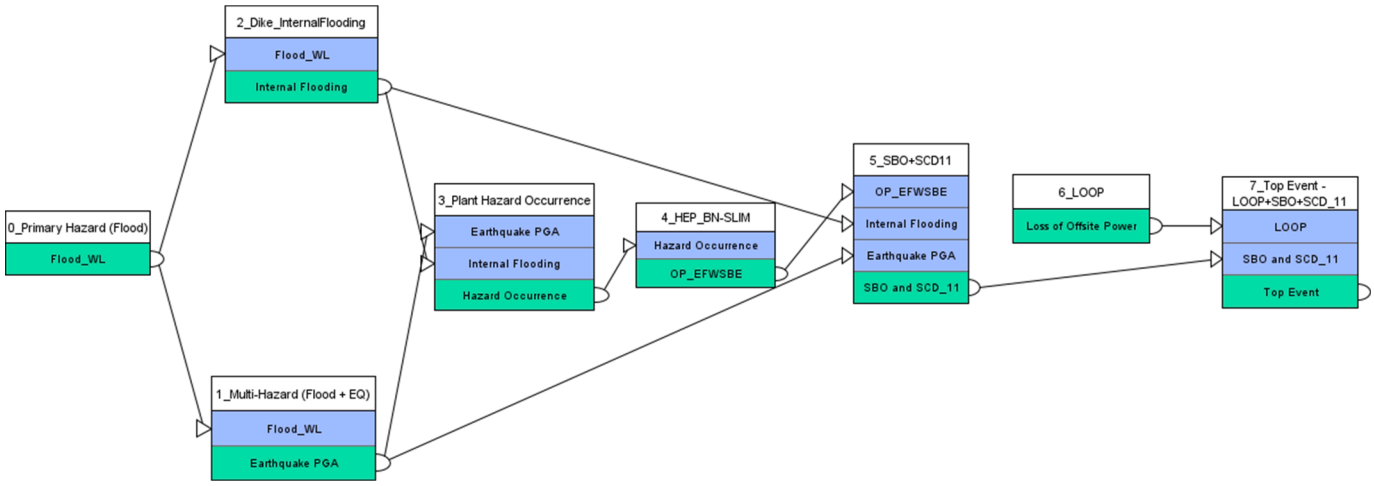


Fig. 14. Object-oriented Bayesian Network for the entire example accident scenario.

Table 4
Marginal probabilities of annual occurrence of key events before and after multi-risk integration.

Event	Marginal probability of occurrence		
	Before hazard and subnetwork integration	Subnetworks integrated with hazards – unified BN	Subnetworks integrated with hazards – OOBN
SBO	2.73×10^{-4}	2.77×10^{-4}	2.76×10^{-4}
SCD	5.38×10^{-4}	5.47×10^{-4}	5.45×10^{-4}
Dike failure	4.26×10^{-2}	4.66×10^{-2}	4.66×10^{-2}
Operator fails to start and control EFWS	2.26×10^{-2}	2.79×10^{-2}	2.79×10^{-2}
Top event – LOOP + SBO + SCD (unified BN)	1.25×10^{-7}	1.32×10^{-7}	1.31×10^{-7}

increases significantly with PGA. The plant is relatively safer against flooding until a flood level of 5 m, beyond which the impact of flooding is greater. This is expected as the height of the flood defence dike is at 5 m. Based on the assumed dike parameters and fragilities, it can also be seen that the dike is less resistant to earthquake PGA > 0.3 g. Also, global stability and piping failure mechanisms increase failure likelihood significantly beyond 3 m flooding, before overtopping occurs at 5 m flooding. Operator action HEP follows the trend of the dike since the PSFs are dependent on hazard occurrence within the plant – which is partly determined by whether the dike is in the functional or failed states.

Table 4 also shows that the plant-wide OOBN risk model yields nearly the same probability estimates as the unified BN, with notable underestimation of the impact of hazards when compared to the unified BN. This is expected as the hazard nodes are common parent nodes (explicit common cause of failure) to all the subnetworks in the unified BN, while they interact individually with each subnetwork, one at a time, in the OOBN. This results in the loss of some interdependency, since the interaction of hazards with each subnetwork is treated via a unique instantiation as opposed to a single hazard node, in the unified BN, which houses all dependencies. Further, every time the configuration of the overall risk BN – structure, CPDs or evidence – is changed, these losses in dependence could be significantly different. Therefore, for every configuration of the BN, it must be verified that probability estimates from the OOBN model remain comparable to those from the more accurate unified BN. This implies that both models will always have to be generated, while the OOBN can be used in practice, where suitable, to capitalise on the advantages discussed below.

Despite the loss of some dependencies, it may be still attractive to use the OOBN approach due to the ease of visualisation and model construction. The subnetworks and their interactions are often visually intelligible (as in Fig. 14) with OOBNs as opposed to a large, unified BN. Crucially, the OOBN approach also offers computational benefits over the unified BN. Table 5 provides the computational requirements for time and memory space for the various BNs featured in this study. The models were executed on a Windows Desktop x-64 based PC – Intel® Xeon® CPU E5-1620 v3 @3.50 GHz, 3501 MHz, 4 Core(s), 8 Logical Processor(s) with 32 GB physical RAM. For the plant-wide risk model, the OOBN consumes less than 25 % of the time and less than 50 % of the memory as the unified BN for this specific example, which can be significant when further complexities are introduced.

4.1. Sensitivity analysis

Sensitivity analysis can be performed in several ways using BNs, including global sensitivity methods developed as part of the NARSIS project (Rohmer and Gehl, 2020). Here, we simply use the diagnostic inference capabilities of the unified BN. Evidence of occurrence and non-occurrence of the top event is provided to the BN, and posterior probabilities of other events in the network are calculated using Bayesian inference. Hazard interaction was also assumed only for the EDGs (in the SBO subnetwork), the flood defence and human reliability of one operator action. Hence, the focus here is on the ability to link the top event (LOOP + SBO + SCD) to the hazards, but also to the other subnetworks – the flood defence and human subnetworks. The response of the top event probability of the SBO subnetwork to multiple hazards is presented in Appendix B.

The variations in posterior distributions of HEP and flood defence failure nodes, based on evidence of the top event, are shown in Fig. 16. Overtopping failure probability is negligible due to the extremely low probability of the flood level exceeding the height of the dike at the site. While piping failure is as determined by the fragility functions, the probability of global stability failure of the dike undergoes the maximum change.

Fig. 16 also shows that the posterior probability of human error changes by almost two orders of magnitude, indicating the considerable influence of human reliability on plant safety, in this scenario. To further understand its impact on the top event, evidence of occurrence and non-occurrence of operator error was provided to the network to check the posterior probability of the top event. If operator action were to be correctly performed, the annual top event probability was calculated to be 1.22×10^{-7}, as compared to 5.79×10^{-7}, when there was an operator error – an increase of over 4 times while all other variables in the

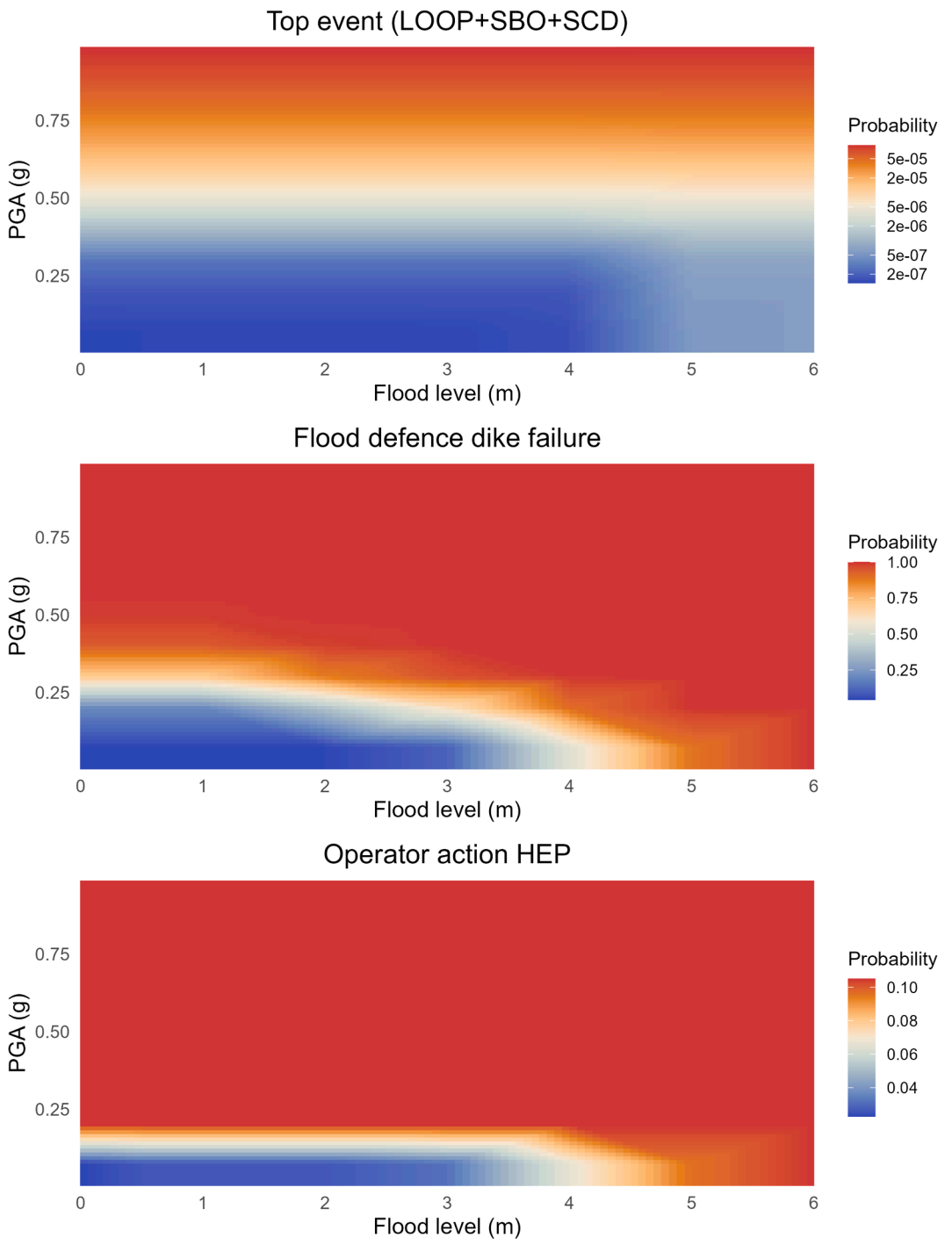


Fig. 15. Multi-hazard probability of key failure events (from unified BN).

unified BN remained unchanged.

Fig. 17 shows the sensitivity of HEP to various PSFs in the human subnetwork, prior to hazard integration. Change in rating level from PSF R9 (relatively safe) to R1 (relatively unsafe) in the "Procedure" and "Experience/Training" PSFs has maximum impact over the probability of human error. Based on hazard interactions with the human subnetwork, "Available Time" and "Stressor" are the PSFs most impacted by hazard occurrence. With these facts as background, the posterior impact at the level of PSFs, when evidence is provided to the top event in the unified BN, is examined. Fig. 18 (a) gives the posterior probability of the eight PSFs given evidence of top event occurrence, indicating the relative influence of various rating levels. The change in probabilities of individual rating levels within PSFs is relatively minor, while we already observed a notable change in HEP in Fig. 16. This is because the change in total HEP is distributed as shifts between rating levels – a degradation of PSFs as probability shifts from R9 (relatively safe) towards R1 (relatively unsafe). As a result, a meaningful change in HEP and top event probability is possible, even with a relatively minor change in the state of PSFs. Fig. 18 (b) shows the difference in posterior probabilities of PSF ratings when evidence of top event (LOOP + SBO + SCD) is changed from "Failure" to "O.K." in the unified BN. As expected, the Available Time and Stressor PSFs undergo maximum change due to their hazard interactions, with a rating level drop to R3 being most likely to cause top event failure. During hazard occurrence within the plant, changes in

Table 5
Computational load for BNs in this study.

BN reference	Run-time (seconds)	Maximum memory used (MB)
SBO	~1	272
SBO with hazards – OOBN	~1	272
SCD	45	680
Flood defence	28	524
Human reliability	4	1088
Plant-wide unified BN (LOOP + SBO + SCD)	840	2536
Plant-wide OOBN (LOOP + SBO + SCD)	180	1204

these PSFs, from R5 to R1, could result in a 77 percent increase in top event probability.

Thus, the unified BN clearly demonstrates the ability of the BN-based risk model to understand multi-hazard dependencies that are typically not considered in design or are not readily obtained from existing PSA tools. This is also possible because the top event is linked to various SSCs, including input parameters of their individual BN-based reliability models.

5. Discussion

The results indicate that the global stability failure mode most affects top event probability – a deduction that is easily possible because of the association of dike reliability with accident states of the NPP, via the unified BN. Hence, solutions such as buttressing the flood dike would be

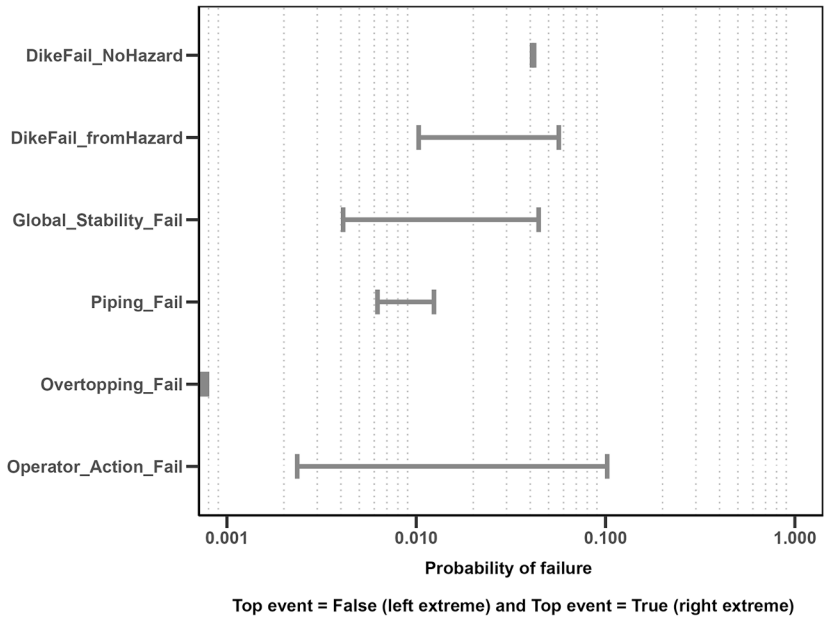


Fig. 16. Posterior annual probability of flood defence failure and operator error given evidence of non-occurrence and occurrence of top event (LOOP + SBO + SCD).

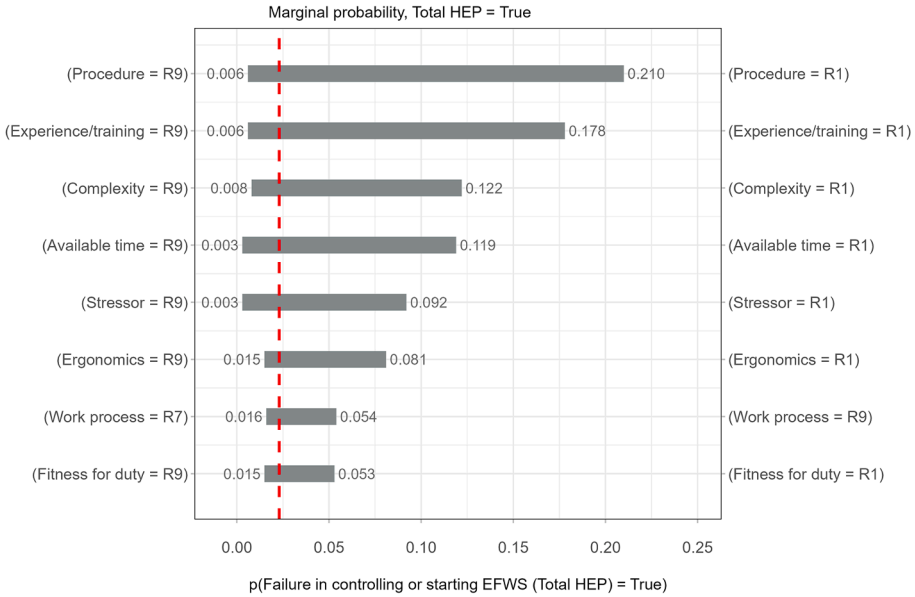
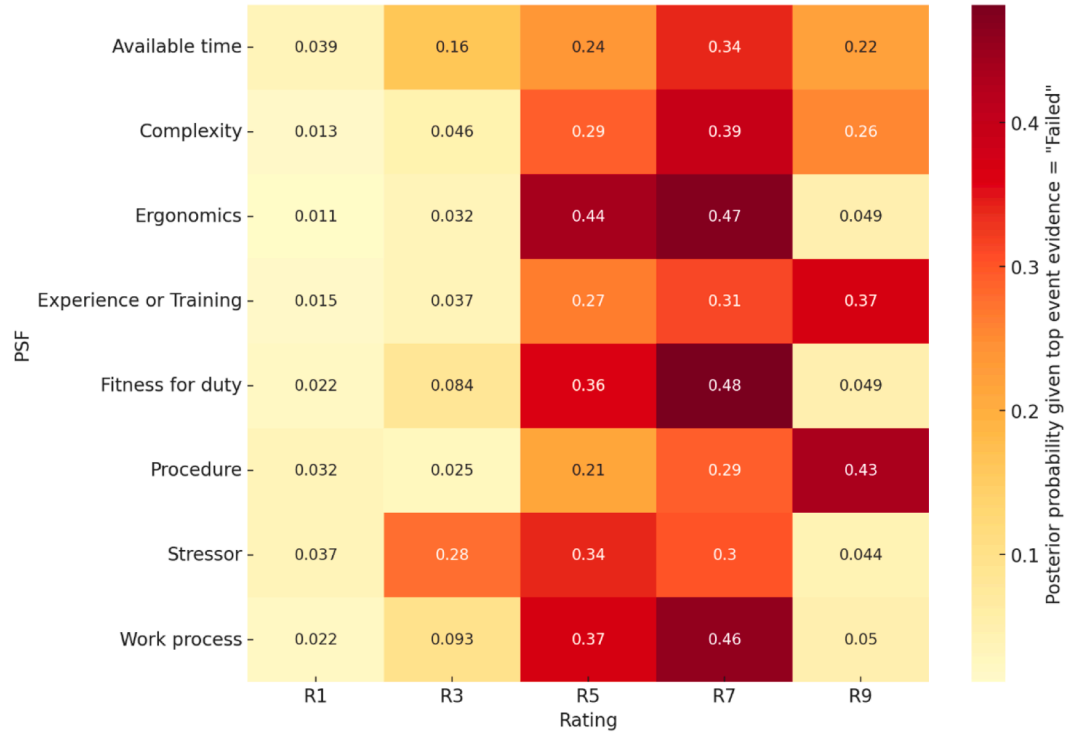
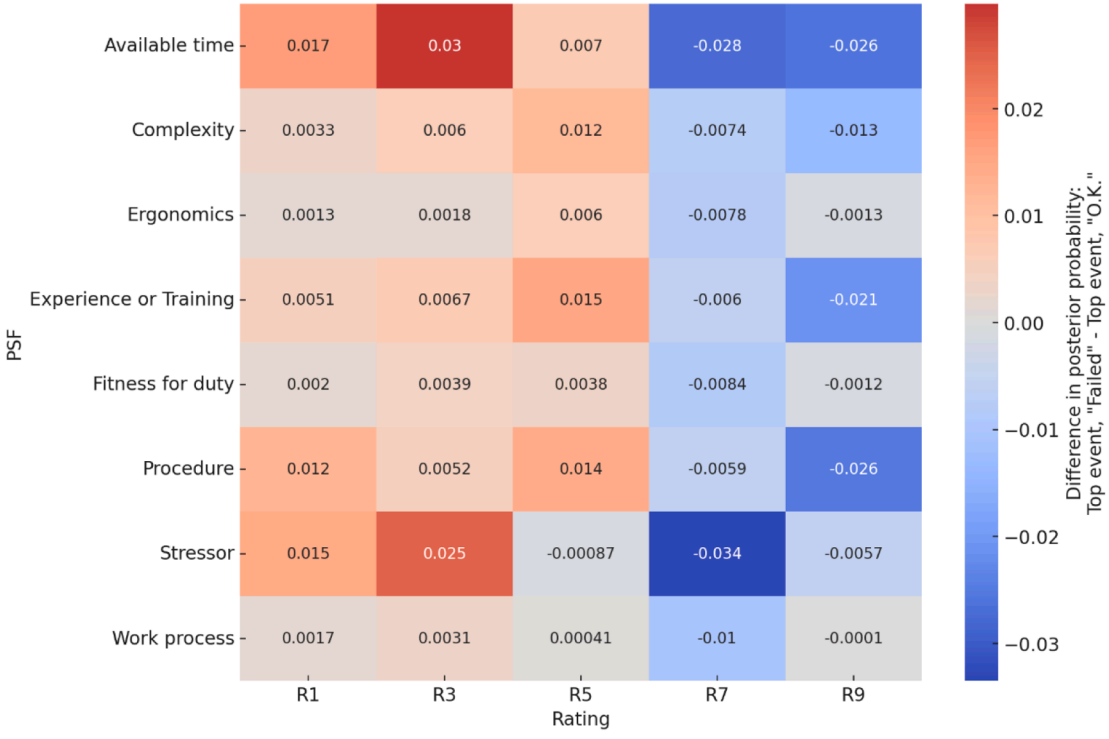


Fig. 17. Sensitivity of HEP to variation in different PSFs: tornado plot based on the human reliability subnetwork (without hazard interaction).



(a)



(b)

Fig. 18. Posterior probability distributions of PSFs in the unified BN, given evidence at the top event (LOOP + SBO + SCD).

more effective in improving dike reliability, thereby reducing top event probability. The required extent of such risk mitigation measures can be planned by using the unified BN to assess impact on top event probability. Given the modelling assumptions, the results from the unified BN also imply that top event risk can be reduced by improving operator clarity in emergency procedures. This may be achieved both by improving the procedures but also by investing in further training of operators during normal operating conditions. More emphasis on operator stress management and on training efficient action within a short span of time can reduce top event risk during hazard events. Expert judgement elicitation for the BN-SLIM method may be suitably revised following such risk mitigation measures.

One significant challenge in the implementation of unified BNs is the large computational load (run-time and/or memory used) due to discretised hazard nodes, detailed uncertainty representation of fragility parameters, continuous variables (such as in the flood defence subnetwork) or other large CPDs due to multi-state variables (such as in the human subnetwork). As a rule of thumb, representing continuous variables increases run-time, while larger CPDs increase the file size of the model and its memory usage. The computational load on the network can potentially be eased by removal of inconsequential hazards and dependencies, a step that was already done during hazard analysis in Daniell et al. (2019). Furthermore, the filtering of less important hazard ranges based on fragility parameters was also performed separately – e.g., by limiting the earthquake impact on human reliability to PGA $>$ 0.15 g. Despite such efforts, the unified BN approach is computationally more intensive as seen in Table 5.

Another potential solution to manage the computational requirements is 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. This, of course, needs a thorough analysis of dependence across the various SSCs in the industrial facility and a judicious application of the BN method to maximise its advantages. Firstly, all the ET/FTs at the facility may be converted to risk objects using the OOBN approach, to first reproduce the results of existing PSA. Next, subnetworks may be integrated using unified BNs as required. While this would not represent a complete solution by modelling every dependence in the facility, it would still complement and improve existing PSA results. Other minor, technical improvements include the divorcing of discrete nodes where possible (Pearl, 1988; Henrion, 1987). Also, much of the computational time often comes from the static discretisation of hazard nodes which impact several SSCs across the risk model. Fitting parametric distributions to hazard curves can avoid inefficient static discretisation of nodes, and instead, take advantage of dynamic discretisation of continuous nodes. Similarly, the use of non-parametric BNs can also significantly reduce the computational load of large BNs, with the necessary assumption of dependence between variables following the Gaussian copula (Hanea et al. 2015; Morales-Nápoles and Steenbergen, 2015). In some cases, the diagnostic abilities in the OOBN approach may be improved by advanced inference methods as in Koller and Pfeffer (2013). However, these methods are generally intended for encapsulation of variables within an object and the repeated use of model fragments in different contexts, aspects which are not relevant to the example in this study.

Another challenge may be the large amount of time and workload involved in eliciting expert judgements regarding various probability distributions of variables. A significant and dedicated effort would be needed to transform existing PSA to BNs and improve it by eliciting expert judgements where needed. Again, the risk analyst must determine areas where there is value in such an exercise. The sensitivity results from the BN can be useful in this regard.

6. Conclusions

Below are a summary of this study and its findings, regarding the use of BNs for multi-risk integration:

- A stepwise multi-risk framework for risk integration using BNs was proposed. The methodology was applied to an example accident scenario of LOOP-induced SBO and failure of SCD.
- 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. This allows for understanding of various dependencies that are normally lost in a facility-wide risk model. Thus, the risk model can be particularly useful in plant safety management, for determining specific areas of risk mitigation that are most impactful in reducing top event probability.
- 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 facility-wide risk model.
- 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 methodology is shown to be applicable using existing PSA information such as event and fault trees. Hence, the method can be used to enhance existing PSA methods, without the need for additional data. However, including BN-based reliability models such as those in this study, may require additional information. Any surrogate BN models will have to be developed individually based on underlying numerical or analytical models. Structured expert judgement elicitation, in the absence of PSF data, is required for implementing the BN-based human reliability model. Such additional data acquisition is not expected to introduce unique regulatory considerations that are not already applicable to existing PSAs, but this must be checked on a case-by-case basis.

Unified BN vs. OOBN

Maximising the advantages of BNs:

- Diagnostic inference and Bayesian updating are inherent advantages of BNs. In OOBNs, diagnostic inference is limited to within risk objects and cannot be performed across objects. Thus, unified BNs better preserve this key advantage of BNs over existing tools such as FTs.
- The unified integration of subnetworks with external hazards can help understand links between the top event of interest and various SSCs at the facility and reveal unforeseen dependencies. While using many hazard trees as in OOBNs, dependencies may be missed between different variables across scenarios. Especially, the impact of dependencies related to explicit common causes of failures such as hazards may be underestimated. Using a unified BN limits such omissions.

Using existing PSA information:

- ET and FTs in existing PSA can be equivalently modelled as OOBNs, allowing for easy transition and parallel application as opposed to the unified BN approach, where the logical interactions of event trees are forcibly housed in CPDs 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. Using the OOBN approach improves computational speed and decreases computational memory

requirements, but each OOBN model must be verified against a unified BN.

CRediT authorship contribution statement

Varenya Kumar D. Mohan: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Pieter H.A.J.M. van Gelder:** Writing – review & editing, Project administration, Methodology. **Pierre Gehl:** Writing – review & editing, Project administration, Methodology, Conceptualization. **Michael A. Hicks:** Writing – review & editing, Supervision. **Philip J. Vardon:** Writing – review & editing, Supervision, Project administration, Investigation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This study has been conducted within the NARSIS project, which has received funding from the European Union's H2020-Euratom Program under grant agreement N° 755439.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.nucengdes.2025.114558.

Data availability

Data will be made available on request.

References

Abrishami, S., Khakzad, N., Hosseini, S.M., 2020. A data-based comparison of BN-HRA models in assessing human error probability: an offshore evacuation case study. Reliab. Eng. Syst. Saf. 202, 107043.

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. Saf. Sci. 44 (8), 657–673.

Bachmann, D., Huber, N.P., Johann, G., Schüttrumpf, H., 2013. Fragility curves in operational dike reliability assessment. Georisk: Assessm. Manage. Risk Eng. Syst. Geohaz. 7 (1), 49–60.

Bedford, T., Cooke, R.M., 2001. Probabilistic Risk Analysis: Foundations and Methods. Cambridge University Press.

Bobbio, A., Portinale, L., Minichino, M., Ciancamerla, E., 2001. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliab. Eng. Syst. Saf. 71 (3), 249–260.

Bruneliere, H., Rastiello, G., Barry, T., Brandelet, J.-Y., Perrichon, L., Duflot, N., Guigeno, Y., Darnowski, P., Mazgaj, P., & Stepień, M., 2018. Definition of a simplified theoretical NPP representative of the European fleet (Technical Report D4.1). Confidential deliverable.

Cai, B., Kong, X., Liu, Y., Lin, J., Yuan, X., Xu, H., Ji, R., 2019. Application of Bayesian networks in reliability evaluation. IEEE Trans. Ind. Inf. 15 (4), 2146–2157.

Choi, E., Ha, J.-G., Hahm, D., Kim, M.K., 2021. A review of multihazard risk assessment: progress, potential, and challenges in the application to nuclear power plants. Int. J. Disaster Risk Reduct. 53, 101933.

Cooke, R., 1991. Experts in Uncertainty: Opinion and Subjective Probability in Science. Oxford University Press, New York.

Cooke, R.M., Goossens, L.L.H.J., 2008. TU Delft expert judgment data base. Reliab. Eng. Syst. Saf. 93 (5), 657–674.

Daniell, J., Schaefer, A., Wenzel, F., Hacker, E., & Edrich, A.-K., 2019. Development of single and secondary hazard assessment methodologies including uncertainty quantification and comparison - Characterization of potential physical threats due to different external hazards and scenarios (D1.6). (NARSIS EU Project (New Approach to Reactor Safety ImprovementS), Grant No. 755439., Issue. http://www.narsis.eu/page/deliverables.

Darnowski, P., Mazgaj, P., Kaszko, A., Potempski, S., Spirzewski, M., Hortal, J., Dusić, M., Prošek, A., Mohan, V. K. D., Vardon, P. J., Karanta, I., Tyrväinen, T., Lo Frano, R., & Cancemi, S. A., 2022. Reactor safety analysis results useful for, severe accident analysis, considering, deterministic and probabilistic approaches (Technical Report D4.5). http://www.narsis.eu/page/deliverables.

Dong, Y., Frangopol, D.M., Saydam, D., 2013. Time-variant sustainability assessment of seismically vulnerable bridges subjected to multiple hazards. Earthquake Eng. Struct. Dyn. 42 (10), 1451–1467.

Durga Rao, K., Gopika, V., Sanyasi Rao, V.V.S., Kushwaha, H.S., Verma, A.K., Srividya, A., 2009. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliab. Eng. Syst. Saf. 94 (4), 872–883.

Ebisawa, K., Teragaki, T., Nomura, S., Abe, H., Shigemori, M., Shimomoto, M., 2015. Concept and methodology for evaluating core damage frequency considering failure correlation at multi units and sites and its application. Nucl. Eng. Des. 288, 82–97.

Fan, S., Blanco-Davis, E., Yang, Z., Zhang, J., Yan, X., 2020. Incorporation of human factors into maritime accident analysis using a data-driven Bayesian network. Reliab. Eng. Syst. Saf. 203, 107070.

Fenton, G., Griffiths, D.V., 2008. Risk Assessment in Geotechnical Engineering, Vol. 461. John Wiley & Sons Inc.

Foester, E., Daniell, J., Gehl, P., Vardon, P.J., 2024. Multi-hazard probabilistic safety assessment of nuclear sites. Japanese Geotechnical Soc. Spec Publ. 10 (50), 1859–1864.

Gardoni, P., LaFave, J.M., 2016. Multi-Hazard Approaches to Civil Infrastructure Engineering: Mitigating Risks and Promoting Resilence. Springer.

Gehl, P., Rohmer, J., 2018. Vector intensity measures for a more accurate reliability assessment of NPP sub-systems Technological Innovations in Nuclear Civil Engineering, France, Paris-Saclay.

Groth, K.M., Swiler, L.P., 2013. Bridging the gap between HRA research and HRA practice: a Bayesian network version of SPAR-H. Reliab. Eng. Syst. Saf. 115, 33–42.

Hanea, A., Morales Napoles, O., Ababei, D., 2015. Non-parametric Bayesian networks: improving theory and reviewing applications. Reliab. Eng. Syst. Saf. 144, 265–284.

Hemming, V., Burgman, M.A., Hanea, A.M., McBride, M.F., Wintle, B.C., 2018. A practical guide to structured expert elicitation using the IDEA protocol. Methods Ecol. Evol. 9 (1), 169–180.

Henrion, M., 1987. Some practical issues in constructing belief networks. In: Proceedings of Uncertainty in Artificial intelligence (Vol. 3, pp. 161–173).

Hicks, M.A., Samy, K., 2004. Stochastic evaluation of heterogeneous slope stability. Italian Geotech. J. 38 (2), 54–66.

Hopkins, A., 2011. Risk-management and rule-compliance: decision-making in hazardous industries. Saf. Sci. 49 (2), 110–120.

Idaho National Laboratory, 2007. Industry-Average performance for components and initiating events at US commercial nuclear power plants, Technical Report No. NUREG/CR-6928 INL/EXT-06-11119, Report to the U.S. Nuclear Regulatory Commission, Idaho National Laboratory.

Jensen, F.V., Nielsen, T.D., 2007. Bayesian Networks and Decision Graphs, Vol. 2. Springer, New York, NY.

Kameshwar, S., Cox, D.T., Barbosa, A.R., Farokhnia, K., Park, H., Alam, M.S., van de Lindt, J.W., 2019. Probabilistic decision-support framework for community resilience: Incorporating multi-hazards, infrastructure interdependencies, and resilience goals in a Bayesian network. Reliab. Eng. Syst. Saf. 191, 106568.

Kanes, R., Marengo, M.C.R., Abdel-Moati, H., Cranefield, J., Véchot, L., 2017. Developing a framework for dynamic risk assessment using Bayesian networks and reliability data. J. Loss Prev. Process Ind. 50, 142–153.

Kelly, D.L., Smith, C., 2011. Bayesian Inference For Probabilistic Risk Assessment : A Practitioner's Guidebook. Springer, New York, NY, USA http://www.books24x7.com/marc.asp?bookid=70726.

Khakzad, N., Khan, F., Amyotte, P., 2011. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliab. Eng. Syst. Saf. 96 (8), 925–932.

Kjærulff, U.B., Madsen, A.L., 2013. Solving probabilistic networks. bayesian networks and influence diagrams: a guide to construction and analysis, 111–142.

Koks, E.E., Rozenberg, J., Zorn, C., Tariverdi, M., Vousdoukas, M., Fraser, S.A., Hall, J., Hallegatte, S., 2019. A global multi-hazard risk analysis of road and railway infrastructure assets. Nat. Commun. 10 (1), 2677.

Koller, D., Friedman, N., 2009. Probabilistic Graphical Models: Principles and Techniques. MIT Press.

Koller, D., Pfeffer, A., 2013. Object-oriented Bayesian networks. In: Proceedings of the Thirteenth conference on Uncertainty in artificial intelligence. Morgan Kaufmann Publishers Inc (1997), pp. 302–313.

Kwag, S., Gupta, A., 2017. Probabilistic risk assessment framework for structural systems under multiple hazards using Bayesian statistics. Nucl. Eng. Des. 315, 20–34.

Lee, C.-J., Lee, K.J., 2006. Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal. Reliab. Eng. Syst. Saf. 91 (5), 515–532.

Lees, F., 2005. 2 – Hazard, incident and loss. In: Mannan, S. (Ed.), Lees' Loss Prevention in the Process Industries, third ed. Butterworth-Heinemann, pp. 2/1–2/27.

Leveson, N., Dulac, N., Marais, K., Carroll, J., 2009. Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems. Organ. Stud. 30 (2–3), 227–249.

Liu, Q., Tchangani, A., Pérès, F., 2016. Modelling complex large scale systems using object oriented Bayesian networks (OOBN). IFAC-PapersOnLine 49 (12), 127–132.

Liu, Z., Nadim, F., Garcia-Aristizabal, A., Mignan, A., Fleming, K., Luna, B.Q., 2015. A three-level framework for multi-risk assessment. Georisk: Assessm. Manage. Risk Eng. Syst. Geohazards 9 (2), 59–74.

Machado, P.G., de Oliveira Ribeiro, C., do Nascimento, C.A.O., 2023. Risk analysis in energy projects using Bayesian networks: a systematic review. Energ. Strat. Rev. 47, 101097.

Mamdikar, M.R., Kumar, V., Singh, P., 2022. Dynamic reliability analysis framework using fault tree and dynamic Bayesian network: a case study of NPP. Nucl. Eng. Technol. 54 (4), 1213–1220.

Mignan, A., Wiemer, S., Giardini, D., 2014. The quantification of low-probability–high-consequences events: part I. a generic multi-risk approach [journal article]. Nat. Hazards 73 (3), 1999–2022.
Mkrtchyan, L., Podofillini, L., Dang, V.N., 2016. Methods for building conditional probability tables of Bayesian belief networks from limited judgment: an evaluation for human reliability application. Reliab. Eng. Syst. Saf. 151, 93–112.
Mohaghegh, Z., Kazemi, R., Mosleh, A., 2009. Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: a hybrid technique formalization. Reliab. Eng. Syst. Saf. 94 (5), 1000–1018.
Mohan, V. K. D., Vardon, P. J., Hicks, M. A., van Gelder, 2019. Uncertainty Tracking and Geotechnical Reliability Updating Using Bayesian Networks 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). http://www.narsis.eu/page/deliverables.
Morales-Nápoles, O., Steenbergen, R.D.J.M., 2015. Large-scale hybrid bayesian network for traffic load modeling from weigh-in-motion system data. J. Bridg. Eng. 20 (1), 04014059.
Mosleh, A.L.I., 2014. PRA: a perspective on strengths, current limitations, and possible improvements. Nucl. Eng. Technol. 46 (1), 1–10.
Pearl, J., 1988. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Morgan Kaufmann Publishers Inc., San Francisco.
Pescaroli, G., Alexander, D., 2018. Understanding compound, interconnected, interacting, and cascading risks: a holistic framework. Risk Anal. 38 (11), 2245–2257.
Roberts, K.H., 1990. Some characteristics of one type of high reliability organization. Organ. Sci. 1 (2), 160–176.
Rohmer, J., Gehl, P., 2020. Sensitivity analysis of Bayesian networks to parameters of the conditional probability model using a Beta regression approach. Expert Syst. Appl. 145, 113130.
Schroeder, J.A., 2015. Analysis of loss-of-offsite-power events 1998–2013 (No. INL/EXT-15-34443). Idaho National Lab.(INL), Idaho Falls, ID (United States).
Segarra, J.D.J., Bensi, M., Modarres, M., 2023. Multi-unit seismic probabilistic risk assessment: a Bayesian network perspective. Reliab. Eng. Syst. Saf. 234, 109169. https://doi.org/10.1016/j.ress.2023.109169.
Shen, J., Bensi, M., Modarres, M., 2022. Synthesis of questionnaire insights regarding current PRA and additional tools. In: Proceedings of Probabilistic Safety Assessment and Management Conference (PSAM16), Honolulu, Hawaii.
Shen, J., Bensi, M., Modarres, M., 2023. Synthesis of insights regarding current PRA technologies for risk-informed decision making. Proceedings of the 18th International Probabilistic Safety Assessment and Analysis. American Nuclear Society.
Shen, J., Bensi, M., Modarres, M., 2025. A Monte Carlo augmented Bayesian network approach for external flood PRAs. Nucl. Eng. Des. 433, 113840.
Siu, N., 1994. Risk assessment for dynamic systems: an overview. Reliab. Eng. Syst. Saf. 43 (1), 43–73.
Suresh, P.V., Babar, A.K., Raj, V.V., 1996. Uncertainty in fault tree analysis: a fuzzy approach. Fuzzy Set. Syst. 83 (2), 135–141.
Tyagunov, S., Vorogushyn, S., Muñoz Jimenez, C., Parolai, S., Fleming, K., 2018. Multi-hazard fragility analysis for fluvial dikes in earthquake-and flood-prone areas. Nat. Hazards Earth Syst. Sci. 18 (9), 2345–2354.
USNRC, 1975. WASH 1400: Reactor safety study - An assessment of accident risks in U.S. commercial nuclear power plants . N.R.C.; National Technical Information Service {{URL. https://www.nrc.gov/reading-rm/doc-collections/nuregs/knowledge/km0010/}.
van Erp, N., van Gelder, P. H. A. J. M. (2015). Risk Analysis framework for single and multiple hazards. Technical Report D5.1, RAIN Project (Risk Analysis of Infrastructure Networks in Response to Extreme Weather). Grant No. 608166.
Weber, P., Jouffe, L., 2006. Complex system reliability modelling with dynamic object oriented Bayesian networks (DOOBN). Reliab. Eng. Syst. Saf. 91 (2), 149–162.
Yazdi, M., Mohammadpour, J., Li, H., Huang, H.Z., Zarei, E., Pirbalouti, R.G., Adumene, S., 2023. Fault tree analysis improvements: a bibliometric analysis and literature review. Qual. Reliab. Eng. Int. 39 (5), 1639–1659.
Yuan, X., Cai, B., Ma, Y., Zhang, J., Mulenga, K., Liu, Y., Chen, G., 2018. Reliability evaluation methodology of complex systems based on dynamic object-oriented Bayesian networks. IEEE Access 6, 11289–11300.
Zhao, Y., Tong, J., Zhang, L., 2021. Rapid source term prediction in nuclear power plant accidents based on dynamic Bayesian networks and probabilistic risk assessment. Ann. Nucl. Energy 158, 108217.
Zhu, K., Zhao, X., Zhang, L., Yu, H., 2022. Research on aging-related degradation of control rod drive system based on dynamic object-oriented Bayesian network and hidden Markov model. Nucl. Eng. Technol. 54 (11), 4111–4124.
Zio, E., 2013. System reliability and risk analysis. In: Zio, E. (Ed.), The Monte Carlo Simulation Method for System Reliability and Risk Analysis. Springer, London, pp. 7–17.
Zio, E., 2016. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliab. Eng. Syst. Saf. 152, 137–150.