TU Delft

Delft University of Technology

Probability elicitation for Bayesian networks to distinguish between intentional attacks and accidental technical failures

Chockalingam, Sabarathinam; Pieters, Wolter; Teixeira, André M.H.; van Gelder, Pieter

DOI
10.1016/j.jisa.2023.103497

Publication date
2023

Document Version
Final published version

Published in
Journal of Information Security and Applications

Citation (APA)
Chockalingam, S., Pieters, W., Teixeira, A. M. H., & van Gelder, P. (2023). Probability elicitation for Bayesian networks to distinguish between intentional attacks and accidental technical failures. *Journal of Information Security and Applications*, *75*, Article 103497. https://doi.org/10.1016/j.jisa.2023.103497

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

Journal of Information Security and Applications 75 (2023) 103497

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Probability elicitation for Bayesian networks to distinguish between intentional attacks and accidental technical failures

Sabarathinam Chockalingam [a,b,*], Wolter Pieters [a,c], André M.H. Teixeira [d], Pieter van Gelder [a]

[a] Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands
[b] Department of Risk and Security, Institute for Energy Technology, Halden, Norway
[c] Behavioural Science Institute, Radboud University, Nijmegen, The Netherlands
[d] Department of Information Technology, Uppsala University, Uppsala, Sweden

ARTICLE INFO

Keywords:
Bayesian network
DeMorgan model
Intentional attack
Probability elicitation
Technical failure

ABSTRACT

Both intentional attacks and accidental technical failures can lead to abnormal behaviour in components of industrial control systems. In our previous work, we developed a framework for constructing Bayesian Network (BN) models to enable operators to distinguish between those two classes, including knowledge elicitation to construct the directed acyclic graph of BN models. In this paper, we add a systematic method for knowledge elicitation to construct the Conditional Probability Tables (CPTs) of BN models, thereby completing a holistic framework to distinguish between attacks and technical failures. In order to elicit reliable probabilities from experts, we need to reduce the workload of experts in probability elicitation by reducing the number of conditional probabilities to elicit and facilitating individual probability entry. We utilise DeMorgan models to reduce the number of conditional probabilities to elicit as they are suitable for modelling opposing influences i.e., combinations of influences that promote and inhibit the child event. To facilitate individual probability entry, we use probability scales with numerical and verbal anchors. We demonstrate the proposed approach using an example from the water management domain.

1. Introduction

Modern societies rely on proper functioning of Critical Infrastructures (CIs) in different sectors such as energy, transportation, and water management which is vital for economic growth and societal wellbeing. Over the years, CIs have become over-dependent on Industrial Control Systems (ICSs) to ensure efficient operations, which are responsible for monitoring and steering industrial processes as, among others, electric power generation, automotive production, and flood control. ICSs were originally designed for isolated environments [1]. Such systems were mainly susceptible to technical failures. The blackout in the Canadian province of Ontario and the North-eastern and Mid-western United States is a typical example of a technical failure in which the absence of alarm due to software bug in the alarm system left operators unaware of the need to redistribute power [2]. However, modern ICSs no longer operate in isolation, but use other networks to facilitate and improve business processes [3]. This increased connectivity, however, makes ICSs more vulnerable to cyber-attacks apart from technical failures. A cyber-attack on a German steel mill is a typical example in which adversaries made use of corporate network to enter into the ICS network [4]. As an initial step, the adversaries used both the targeted email and social engineering techniques to acquire credentials for the corporate network. Once they acquired credentials for the corporate network, they worked their way into the plant's control system network and caused damage to the blast furnace.

It is essential to distinguish between attacks and technical failures that would lead to abnormal behaviour in the components of ICSs and take suitable measures. In most cases, the initiation of response strategy presumably aimed at technical failures would be ineffective in the event of a targeted attack and may lead to further complications. For instance, replacing a sensor that is sending incorrect measurement data with a new sensor would be a suitable response strategy to technical failure of a sensor. However, this may not be an appropriate response strategy to an attack on the sensor as it would not block the corresponding attack vector. Furthermore, the initiation of inappropriate response strategies would delay the recovery of the system from adversaries and might lead to harmful consequences. Noticeably, there is a lack of decision support to distinguish between attacks and technical failures.

* Corresponding author at: Department of Risk and Security, Institute for Energy Technology, Halden, Norway.
E-mail address: Sabarathinam.Chockalingam@ife.no (S. Chockalingam).

https://doi.org/10.1016/j.jisa.2023.103497

Available online 21 April 2023
2214-2126/© 2023 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Bayesian Networks (BNs) have the capacity to tackle this challenge especially based on their real-world applications in medical diagnosis [5] and fault diagnosis [6–8]. In addition, there are other BN-based applications in domains like resilience engineering [9], structural systems [10]. BNs belong to the family of probabilistic graphical models [11], consisting of a qualitative and a quantitative part [12]. The qualitative part is a Directed Acyclic Graph (DAG) of nodes and edges. Each node represents a random variable, while the edges between the nodes represent the conditional dependencies among the random variables. BN structure modelling includes determining nodes and relationships between the determined nodes [13]. The quantitative part takes the form of a priori marginal and conditional probabilities so as to quantify the dependencies between connected nodes. BN parameter modelling includes specifying prior marginal and conditional probabilities [13].

In order to address the above-mentioned research gap, we developed a framework in our previous work to help construct BN models for distinguishing attacks and technical failures [14]. Furthermore, we extended and combined fishbone diagrams within our framework for knowledge elicitation to construct the qualitative part of such BN models. However, our previous work lacks a systematic method for knowledge elicitation to construct the quantitative part of such BN models. This present study aims to provide a holistic framework to help construct BN models for distinguishing attacks and technical failures by addressing the research question: *"How could we elicit expert knowledge to effectively construct Conditional Probability Tables of Bayesian Network models for distinguishing attacks and technical failures?"*. The research objectives are:

- **RO1.** To propose an approach that would help to effectively construct Conditional Probability Tables (CPTs) for our application.
- **RO2.** To demonstrate the proposed approach using an example in the water management domain.

Empirical data is one of the data sources utilised to populate CPTs of BN models in cyber security [15]. This empirical data can be extracted from specific sources like cyber security incidents database, technical failure reports, and red team vs. blue team exercises. However, in the water management domain in the Netherlands, there is no/limited cyber-attacks on their infrastructures [16]. In addition, information corresponding to limited cyber-attacks and technical failure reports are not shareable due to the sensitivity of data [16]. Furthermore, red team vs. blue team exercises were not possible due to practicalities, especially there is a lack of testbeds which could facilitate such exercises in the Netherlands [16]. Expert knowledge is one of the predominant data sources utilised to populate conditional probability tables (CPTs) especially in domains where there is a limited availability of data like cyber security [15]. Probability elicitation is the most challenging part of constructing BN models especially when it relies on expert knowledge as we need to elicit probability for every possible combination of parent variables state to complete the CPT of a child variable from experts. The CPT size of a child variable grows exponentially with the number of parents. For instance, the CPT size of a binary child with 5 binary parents is 64 (2^{5+1}) entries. The burden of probability elicitation could be reduced by: (i) reducing the number of conditional probabilities to elicit by imposing structural assumptions, and (ii) facilitating individual probability entry by providing visual aids to help experts answer elicitation questions in terms of probabilities [17]. We evaluate several techniques for reducing the number of probabilities to elicit, and conclude that DeMorgan models is most suitable for our purpose [18]. Furthermore, we review several methods for facilitating individual probability entry and conclude that probability scales with numerical and verbal anchors is most appropriate for our application [19,20].

The main contributions of this paper are as follows:

(i) we propose an approach involving DeMorgan model and probability scales with numerical and verbal anchors that could help to effectively construct quantitative part (CPTs) of BN models for distinguishing attacks and technical failures.
(ii) we demonstrate the proposed approach using an example in the water management domain to mainly show which parameters need to be elicited from experts and corresponding questions that needs to be asked in addition to how the rest of the probabilities in the CPTs are computed.

This paper is not about "anomaly detection" (i.e., detecting whether an anomaly has occurred or not), but rather "diagnosis" (i.e., pinpointing whether the detected anomaly is due to cyber-attack or technical failure). Diagnosis is prevalent in medical and safety domains [21,22]. Furthermore, we utilised Design Science Research (DSR) method to tackle our RQ, which is widely used to create artefacts [23]. An artefact is defined as an object made by humans for the purpose of solving practical problems like distinguishing attacks and technical failures [24]. An artefact could be a construct (or concept), a model, a method, or an instantiation [25]. The practical problems can be solved using artefacts in numerous cases. There are five main phases in the DSR process: (i) problem identification, (ii) design and development, (iii) demonstration, (iv) evaluation, and (v) communication. In the problem identification phase, we gather constraints and high-level requirements using semi-structured interviews and focus group sessions with experts in safety and/or security of ICS in the water management domain in the Netherlands. The list of questions which we asked the experts in addition to constraints and requirements are provided in the Appendix. These constraints and high-level requirements are mainly for developing our holistic framework which would then help to construct BN models for distinguishing attacks and technical failures and their evaluation. This phase results in a set of high-level requirements and constraints based on the responses from experts, which are mainly used as an input for the "design and development" and "evaluation" phases of the DSR process. This paper corresponds to the "design and development" and "demonstration" phases in the DSR process. However, evaluating the performance of the proposed approach is outside the scope of this study, which corresponds to the "evaluation" phase in the DSR process. Our related work that has already been published corresponds to the "evaluation" phase in the DSR process [16]. The set of constraints and high-level requirements mentioned in the Appendix plays an important role in structuring the problem space and deriving design decisions systematically. This is used as a basis for the "design and development" and "evaluation" phase of the DSR process.

The remainder of this paper is structured as follows. In Section 2, we illustrate the different layers and the components of an ICS and describe a case study in the water management domain that is used to demonstrate our proposed approach. In Section 3, we describe our existing framework in addition to a systematic method for knowledge elicitation to construct the qualitative part of BN models for distinguishing attacks and technical failures. Section 4 provides an essential foundation of techniques to reduce the burden of probability elicitation to construct the quantitative part of BN models for distinguishing attacks and technical failures. In Section 5, we demonstrate the proposed approach using an example in the water management domain. Section 6 presents discussion followed by the conclusions and future work directions in Section 7.

2. Industrial control systems

In this section, we illustrate the three different layers and major components in each layer of an ICS. Furthermore, we provide an overview of a case study in the water management domain.

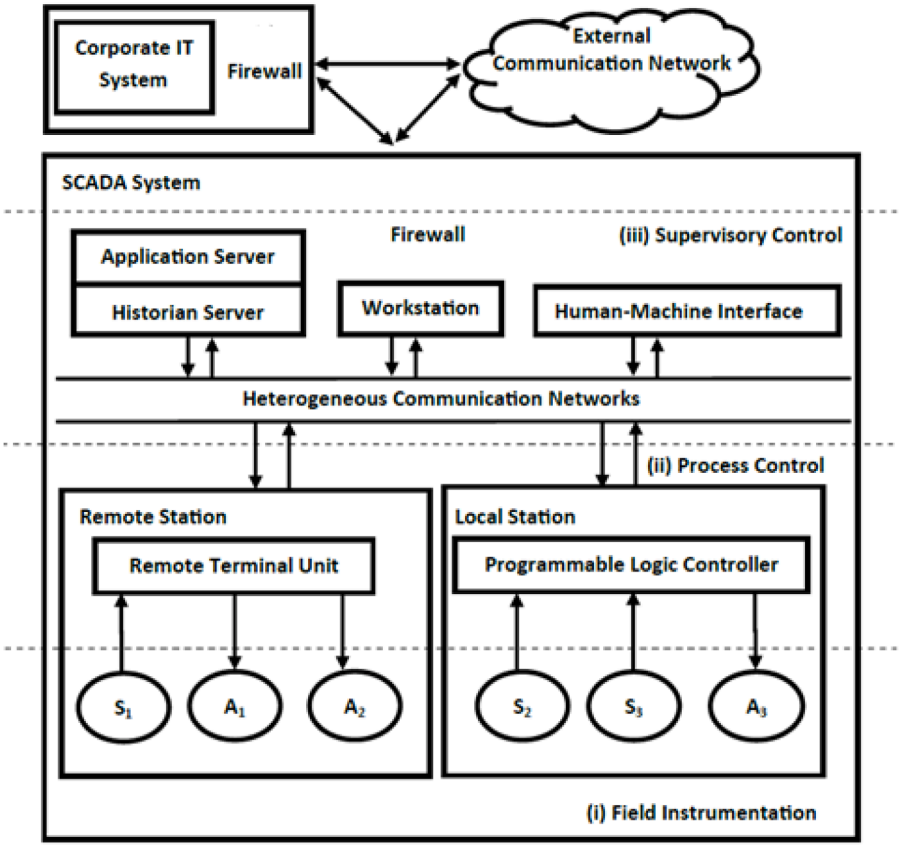


Fig. 1. Typical ICS Architecture and Layers.

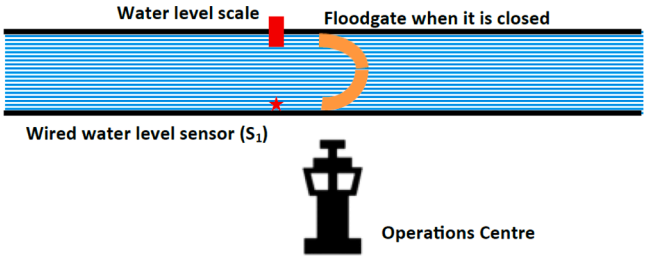


Fig. 2. Physical Layout of the Floodgate.

2.1. ICS architecture

Domain knowledge on ICSs is the starting point for the development and application of our proposed approach. A typical ICS consists of three layers: (i) Field instrumentation, (ii) Process control, and (iii) Supervisory control [26], bound together by network infrastructure, as shown in Fig. 1.

The field instrumentation layer consists of sensors (S_i) and actuators (A_i), while the process control layer consists of Programmable Logic Controllers (PLCs)/Remote Terminal Units (RTUs). Typically, PLCs have wired communication capabilities whereas RTUs have wired or wireless communication capabilities. The PLC/RTU receives measurement data from sensors, and controls the physical systems through actuators [27]. The supervisory control layer consists of historian databases, software application servers, the Human-Machine Interface (HMI), and the workstation. The historian databases and software application servers enable the efficient operation of the ICS. The low-level components are configured and monitored with the help of the workstation and the HMI, respectively [27].

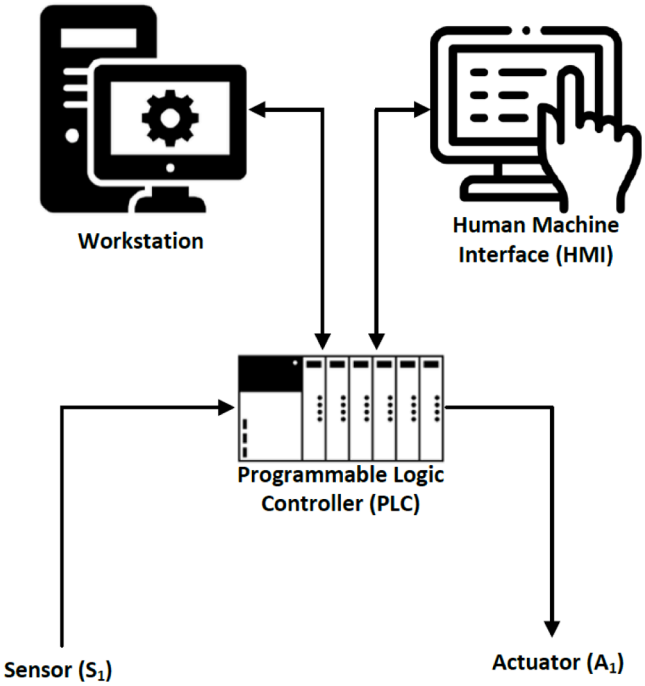


Fig. 3. SCADA Architecture of the Floodgate.

2.2. Case study overview

This case study overview is based on a site visit to a floodgate in the Netherlands. Some critical information has purposely been anonymised

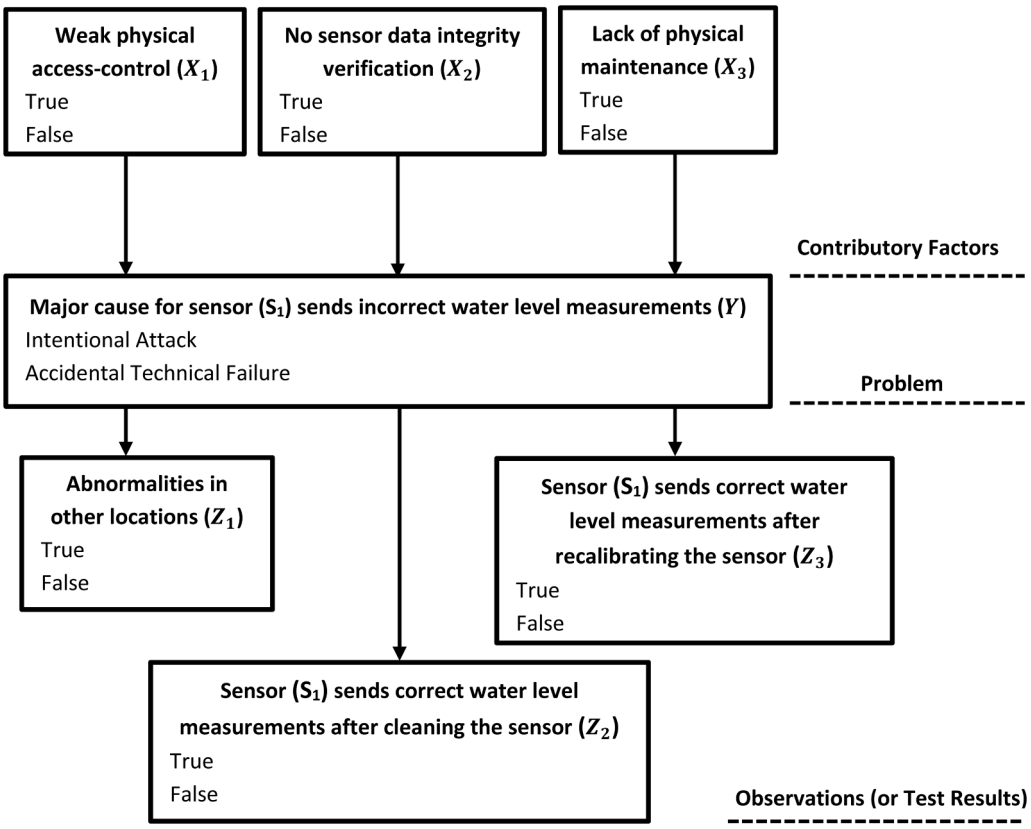


Fig. 4. Framework for Distinguishing Attacks and Technical Failures: Example.

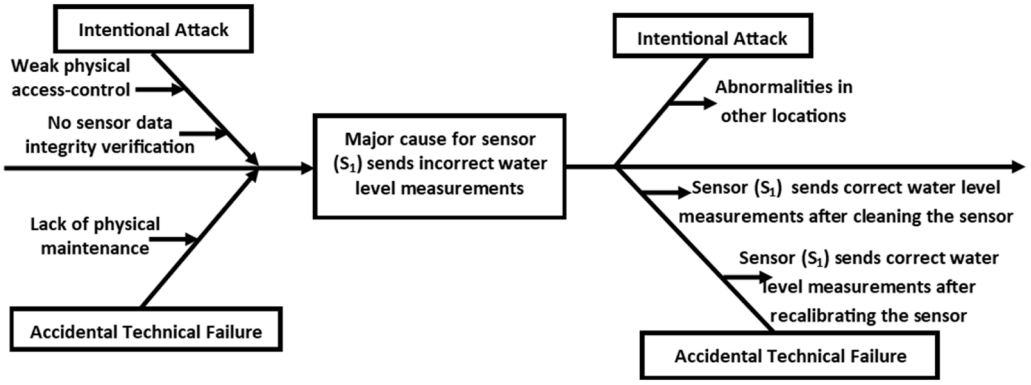


Fig. 5. Extended Fishbone Diagram: Example.

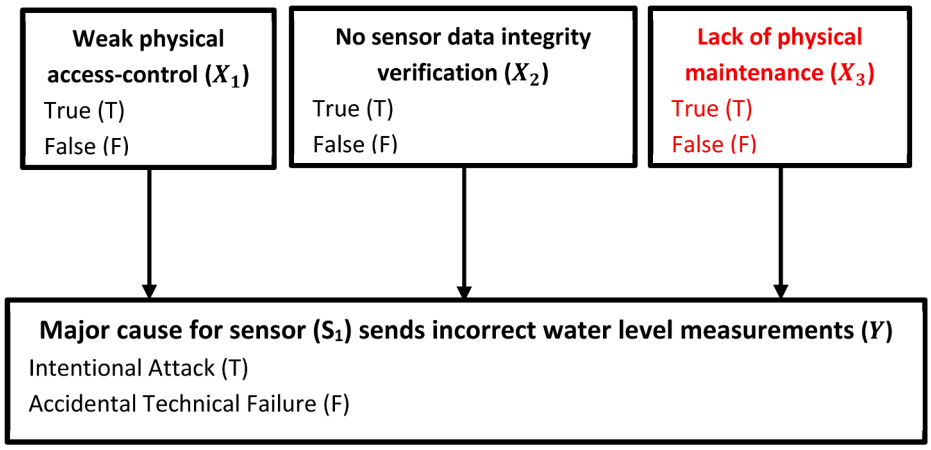
for security concerns. This case study is also used in our previous work [14]. Fig. 2 schematises a floodgate being primarily operated by Supervisory Control and Data Acquisition (SCADA) system along with an operations centre.

Fig. 3 illustrates the SCADA architecture of the floodgate. The sensor (S_1), which is located near the floodgate, is used to measure the water level. There is also a water level scale which is visible to the operator from the operations centre. The sensor measurements are then sent to the PLC. If the water level reaches the higher limit, PLC would send an alarm notification to the operator through the HMI, and the operator would need to close the floodgate in this case. The HMI would also provide information such as the water level and the current state of the floodgate (open/close). The actuator opens/closes the floodgate. This case study would be used to demonstrate our proposed approach that would help to effectively construct CPTs involving domain experts.

3. Framework for distinguishing attacks and technical failures

This section describes the proposed framework including extended fishbone diagrams in our previous work with an example that could help to construct qualitative part (DAG) of BN models for distinguishing attacks and technical failures [14], which corresponds to structural modelling of BNs.

The framework consists of three layers as shown in Fig. 4, which mainly shows different type of variables (i.e., contributory factors, problem, and observations (or test results)) and their relationships. The middle layer consists of a problem variable which is the major cause for an abnormal behaviour in a component of the ICS (observable problem). In the example shown in Fig. 4, we considered "Sensor (S_1) sends incorrect water level measurements" as the problem, which is observable. For instance, this problem could be observed by comparing the water level measurements sent by the sensor (S_1) against the



X_1	X_2	X_3	Y	
			Intentional Attack (Y = True)	**Accidental Technical Failure (Y = False)**
True	**True**	**True**	Calculated	$1 - P(Y = T \mid X_1 = T, X_2 = T, X_3 = T)$
True	**True**	**False**	Calculated	$1 - P(Y = T \mid X_1 = T, X_2 = T, X_3 = F)$
True	**False**	**True**	Calculated	$1 - P(Y = T \mid X_1 = T, X_2 = F, X_3 = T)$
True	**False**	**False**	Elicited	$1 - P(Y = T \mid X_1 = T, X_2 = F, X_3 = F)$
False	**True**	**True**	Calculated	$1 - P(Y = T \mid X_1 = F, X_2 = T, X_3 = T)$
False	**True**	**False**	Elicited	$1 - P(Y = T \mid X_1 = F, X_2 = T, X_3 = F)$
False	**False**	**True**	Elicited	$1 - P(Y = T \mid X_1 = F, X_2 = F, X_3 = T)$
False	**False**	**False**	**0**	**1 (based on the property of accountability)**

Fig. 6. Application of Noisy-OR: Problem.

measurements in the water level scale. We considered the major causes of the problem (intentional attack and accidental technical failure) as the states of the problem variable. In our work, we assume that problem (example: "Sensor (S_1) sends incorrect water level measurements") is already identified by the operator. The scope of our proposed approach is to distinguish between the major causes (i.e., intentional attack vs. accidental technical failure).

The upper layer consists of factors contributing to the major causes of the problem. For instance, the factor "Weak physical access-control" contributes to "Sensor (S_1) sends incorrect water level measurements" due to intentional attack, whereas "Lack of physical maintenance" contributes to "Sensor (S_1) sends incorrect water level measurements" due to accidental technical failure. The lower layer consists of observations (or test results) which is defined as any information useful for determining the major cause of the problem based on the outcome of tests. For instance, the outcome of the test whether "Sensor (S_1) sends correct water level measurements after cleaning the sensor" would provide additional information to determine the major cause (accidental technical failure or intentional attack) of the problem accurately.

The framework which we proposed in our previous work includes a systematic method based on fishbone diagrams for knowledge elicitation to construct the qualitative part of BN models [14]. We adopted this approach because there are challenges to solely rely on BNs for knowledge elicitation to construct the qualitative part of BN models. It is not easy-to-use for knowledge elicitation involving domain experts as it could be time-consuming for elicitors to explain the notion of BNs [14]. Furthermore, it could not encourage and guide data collection by showing where knowledge is lacking as it is not well-structured. On the other hand, fishbone diagrams help to systematically identify and organise the possible contributing factors (or sub-causes) of a particular problem [28–32]. We extended fishbone diagrams to incorporate observations (or test results) in our previous work, which needs to be elicited for our application in addition to contributory factors.

Fig. 5 shows an example extended fishbone diagram which consists of a problem ("Major cause for sensor (S_1) sends incorrect water level measurements"), contributing factors (or sub-causes) sorted and related under different categories on the left side of the problem. Each category on the left side of the problem represents the major causes of the problem (intentional attack and accidental technical failure). Our example shows that "Lack of physical maintenance" is the contributing factor to the problem ("Sensor (S_1) sends incorrect water level measurements") due to accidental technical failure. Furthermore, the observations (or test results) on the right side of the problem would provide additional information to determine the major cause of the problem accurately. Each category on the right side of the problem are used for reference to elicit observations (or test results) that would be useful for determining the particular major causes of the problem [14]. Our example shows that the observation "abnormalities in other locations" would increase the probability of the problem ("Sensor (S_1) sends incorrect water level measurements") due to intentional attack.

Once the extended fishbone diagram is developed, it would be translated into a corresponding qualitative BN model based on the mapping scheme in our previous work [14]. However, the proposed framework lacked a systematic method for knowledge elicitation to construct the quantitative part of BN models (the CPTs), which we address in the current work.

4. Techniques for reducing the burden of probability elicitation

Probability elicitation is a challenging task in building BNs, especially when it relies heavily on expert knowledge [17]. The extensive workload for experts in probability elicitation could affect the reliability

of elicited probabilities. However, the workload for experts in probability elicitation could be reduced by reducing the number of conditional probabilities to elicit and facilitating individual probability entry.

4.1. Technique for reducing the number of conditional probabilities to elicit

This section analyses well-known techniques and describes the most suitable technique for our application, which would help to reduce the number of conditional probabilities to elicit.

In order to reduce the number of conditional probabilities to elicit, we could exploit the causal independence models [17]. Causal independence refers to the situation where the contributory factors (causes) contribute independently to the problem (effect) [33]. By utilising these models, only a number of parameters that is linear in the number of contributory factors is needed to be elicited to define a full CPT for the problem variable as the total influence on the problem is a combination of the individual contributions [34]. As an example, we shall consider the BN model depicted in Fig. 4, where the problem variable (Y) is a binary discrete variable with the states "Intentional Attack" and "Accidental Technical Failure". In the CPT shown in Fig. 6, Y = "Intentional Attack" denotes Y = "True", and Y = "Accidental Technical Failure" denotes Y = "False". We translated the states of Y into "True" and "False" to comply with the inherent assumptions of the noisy-OR model with regard to the states of variables. The typical state of each variable in the noisy-OR model is "False". For instance, the typical state of a child variable (Fever) in the noisy-OR model is "False" as it is normal. Therefore in our application, we assigned Y = "False" for Y = "Accidental Technical Failure" as this is the a priori expected major cause, based on the higher frequency of technical failures compared to the intentional attacks [14].

In our application, we are dealing with a combination of promoting and inhibiting influences. In case of a promoting influence, the presence (or absence) of the parent will result in the child event with a certain probability. When the parent is absent (or present), it is certain not to cause the child event. In other words, the presence (or absence) of the contributory factor will result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "intentional attack" with a certain probability as it denotes "True" state. For instance, the presence of "Weak physical access-control" will result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "intentional attack" with a certain probability, whereas the absence of "Weak physical access-control" will not certainly result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "intentional attack". This type of promoting influence is defined as a cause [18]. On the other hand, the absence of "Sensor data integrity verification" will result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "intentional attack" with a certain probability, whereas the presence of "Sensor data integrity verification" will not certainly result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "intentional attack". This type of promoting influence is defined as a barrier [18].

In case of an inhibiting influence, the presence (or absence) of the parent will inhibit the child event with a certain probability. When the parent is absent (or present), it is certain not to inhibit the child event. In other words, the presence (or absence) of the contributory factor will result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "accidental technical failure" with a certain probability as it denotes "False" state. For instance, the presence of "Lack of physical maintenance" will result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "accidental technical failure" with a certain probability, whereas the absence of "Lack of physical maintenance" will not certainly result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "accidental technical failure". This type of inhibiting influence is defined as an inhibitor [18]. On the other hand, the absence of "Well-written maintenance procedure" will result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "accidental technical failure" with a certain probability, whereas the presence of "Well-written maintenance procedure" will not certainly result in the problem ("Sensor (S_1) sends incorrect water level measurements") due to "accidental technical failure". This type of inhibiting influence is defined as a requirement [18].

Our example BN model shows that it possesses a mixture of promoting and inhibiting influences (causes and inhibitors) especially with regard to the interaction between the contributory factors and the problem. Therefore, we need a technique that would help to model opposing influences as we deal with a mixture of promoting and inhibiting influences in our application, which would help to reduce the number of conditional probabilities to elicit.

We analysed several techniques and chose the most suitable technique for our application which would be described in Section 4.1.1. The description of techniques that are unsuitable for our application can be found in Appendix which includes the noisy-OR model and Causal Strength (CAST) logic. The noisy-OR model is one of the most commonly used causal independence models which helps to reduce the number of conditional probabilities to elicit [5,35]. The noisy-OR model inherently assumes binary variables [36]. The noisy-MAX model is an extension of the noisy-OR model which is suitable for multi-valued variables [37]. We analysed the noisy-OR model as we deal with only binary variables in our application.

The noisy-OR model assumes that the properties of exception independence and accountability hold true [38]. In case all the modelled contributory factors of the problem ("Sensor (S_1) sends incorrect water level measurements") are false, the property of accountability requires that the problem be presumed false ("Sensor (S_1) sends incorrect water level measurements" due to "accidental technical failure"). However, this would not work for inhibiting influences such as "Lack of physical maintenance" in the noisy-OR model as shown in Fig. 6. In case "Lack of physical maintenance" is absent, it is certain not to inhibit the problem which is incompatible with the property of accountability. Therefore, we found that the noisy-OR model is unsuitable for the purposes of our application because the property of accountability does not hold true.

Alternatively, CAST logic is one of the techniques mainly developed for modelling opposing influences [39]. CAST logic assumes all the variables in the model are binary. The parameters which need to be elicited to completely define CPTs using CAST logic are: (i) causal strengths for each edge, and (ii) baseline probability for each variable. The baseline probability of a parent variable can be interpreted as the prior probability of the corresponding parent variable. However, it would not be appropriate to interpret the baseline probability of the child variable as a prior probability or a leak probability, as the parent variables have no state in which they are guaranteed to have no influence on the child variable [40]. As the definition of baseline probability of child variable is not clear, we cannot formulate appropriate question to elicit baseline probability of child variable. This is the major disadvantage of CAST logic which resulted in the lack of practical applications [18,40]. We conclude that neither the noisy-OR model nor the CAST logic is suitable for the purposes of our application.

4.1.1. DeMorgan model

As an alternative to the previously discussed models, the DeMorgan model can potentially be used to tackle the challenge of modelling opposing influences, which would help to reduce the number of conditional probabilities to elicit. This section explains the DeMorgan model. This section corresponds to parameter modelling of BNs, which show parameters that needs to be elicited from experts and corresponding questions that needs to be asked to experts during this elicitation process in addition to how the rest of the parameters in the CPTs are computed.

The DeMorgan model is a technique mainly developed for modelling opposing influences, which would help to reduce the number of conditional probabilities to elicit [18,40]. The DeMorgan model is applicable when there are several parents and a common child. The DeMorgan

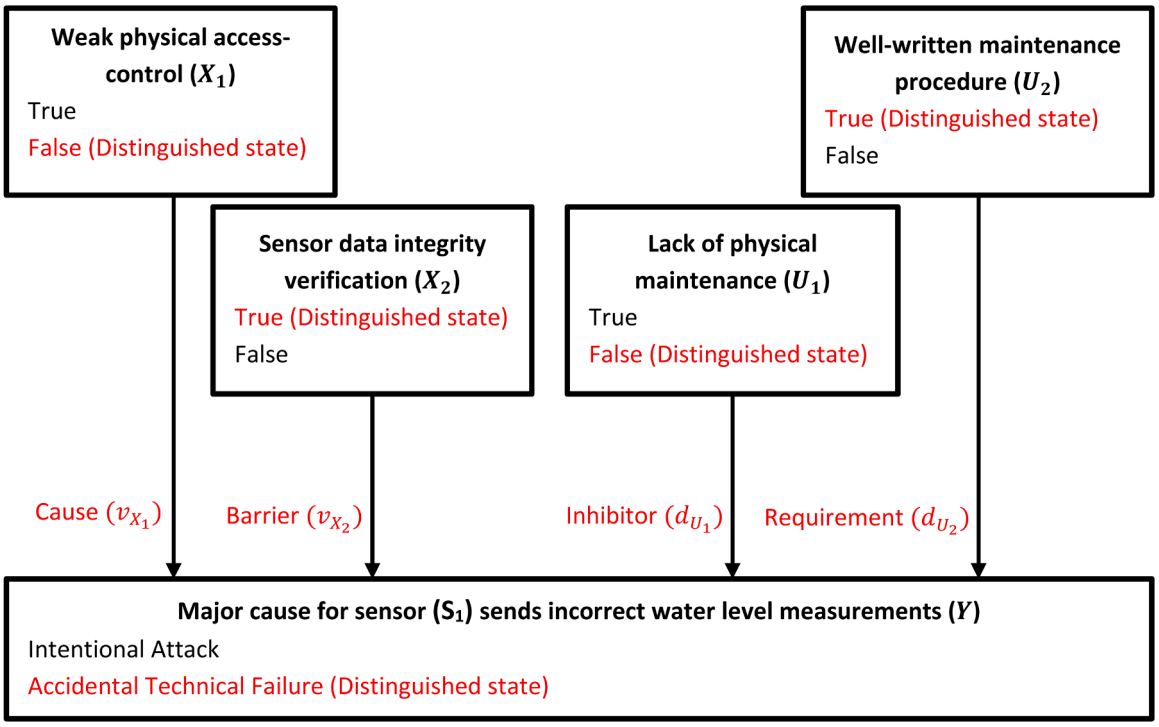


Fig. 7. DeMorgan Model: Causal Interaction Types.

Table 1
Type of Causal Interaction: Cause.

X	Y	
	Intentional Attack	Accidental Technical Failure
True	$\boldsymbol{v_X}$	$1 - v_X$
False	**0**	1

Table 2
Type of Causal Interaction: Barrier.

X	Y	
	Intentional Attack	Accidental Technical Failure
True	**0**	1
False	$\boldsymbol{v_X}$	$1 - v_X$

Table 3
Type of Causal Interaction: Inhibitor.

X	Y	
	Intentional Attack	Accidental Technical Failure
True	$1 - d_X$	$\boldsymbol{d_X}$
False	1	**0**

model inherently assumes binary variables. The DeMorgan model assumes that one of the two states of each variable is always the distinguished state as shown in Fig. 7. Usually such state of the child variable depends on the modelled domain [41]. This is a typical state of the corresponding child variable [42]. In case the child variable consists of two states ("disease", "no disease") in the medical domain, the distinguished state of the corresponding child variable is chosen as "no disease" as it is normal [41]. In our application, the distinguished state of the problem variable ("Major cause for sensor (S_1) sends incorrect water level measurements") is chosen as "accidental technical failure" as this is the a priori expected major cause, based on the higher frequency of technical failures compared to the intentional attacks [14]. The distinguished state of a parent variable is relative to the type of causal interaction with the child variable [18]. The same parent variable can have different distinguished states in different interactions that it participates in with the different child variables.

There are 4 different types of causal interactions between an individual parent (X) and a child (Y) in the DeMorgan model: (i) cause, (ii) barrier, (iii) inhibitor, and (iv) requirement.

(i) Cause: X is a causal factor and has a positive influence on Y. In this type of causal interaction between an individual parent (X) and a child (Y), the distinguished state of the corresponding parent variable is "False" [18]. Consequently, when the parent variable is "False", it is certain not to trigger a change from the typical state of the child variable as shown in Table 1. When the parent variable is "True", it will trigger a change from the typical state of the child variable, with a certain probability (v_X) as shown in Table 1.

(ii) Barrier: This is a negated counterpart of cause, i.e., X' is a causal factor and has a positive influence on Y. In this type of causal interaction between an individual parent (X) and a child (Y), the distinguished state of the corresponding parent variable is "True" [18]. Accordingly, when the parent variable is "True", it is certain not to trigger a change from the typical state of the child variable as shown in Table 2. When the parent variable is "False", it will trigger a change from the typical state of the child variable, with a certain probability (v_X) as shown in Table 2.

(iii) Inhibitor: X inhibits Y. In this type of causal interaction between an individual parent (X) and a child (Y), the distinguished state of the corresponding parent variable is "False" [18]. As a result, when the parent variable is "False", it is certain not to prevent a change from the typical state of the child variable as shown in Table 3. When the parent variable is "True", it will prevent a change from the typical state of the child variable, with a certain probability (d_X) as shown in Table 3.

(iv) Requirement: The relationship between an inhibitor and requirement is similar to the relationship between a cause and

Table 4
Type of Causal Interaction: Requirement.

X	Y	
	Intentional Attack	Accidental Technical Failure
True	1	**0**
False	$1 - d_X$	$\boldsymbol{d_X}$

barrier. X' inhibits Y. In this type of causal interaction between an individual parent (X) and a child (Y), the distinguished state of the corresponding parent variable is "True" [18]. Hence, when the parent is "True", it is certain not to prevent a change from the typical state of the child variable as shown in Table 4. When the parent variable is "False", it will prevent a change from the typical state of the child variable, with a certain probability (d_X) as shown in Table 4.

The DeMorgan model is an extension and a combination of the noisy-OR and noisy-AND model which supports modelling the above-mentioned types of causal interactions [18]. Maaskant et al. modelled promoting influences which includes causes and barriers by mimicking the noisy-OR model [18]. Furthermore, Maaskant et al. modelled inhibiting influences which includes inhibitors and requirements by mimicking the noisy-AND model [18]. Finally, Maaskant et al. modelled the combination of promoting and inhibiting influences by combining the noisy-OR and noisy-AND model.

The property of accountability in the noisy-OR model is applicable to the DeMorgan model with a slight modification as it also exploits causal independence: In case all the modelled parents of the child are in their distinguished state, the property of accountability requires that the child be presumed their distinguished state. However, in many cases, this is not a realistic assumption as it is difficult to capture all the possible parents of the child [34]. Specifically, this is not realistic in our example as it is difficult to capture all the possible contributory factors of the problem ("Sensor (S_1) sends incorrect water level measurements") due to "intentional attack". In the DeMorgan model, the leak parameter (v_{X_L}) deals with the possible parents of the child that are not previously known and explicitly modelled.

In general, the size of the CPT of a binary variable with n binary parents is 2^{n+1}. However, only $n + 1$ parameters are sufficient to completely define CPT using the DeMorgan model as it exploits causal independence. In the example shown in Fig. 7, only 5 parameters are sufficient to completely define the CPT of child variable (Y) using the DeMorgan model instead of 64 entries. There are 2 different parameterisations for the Noisy-OR model with a leak parameter (the Leaky Noisy-OR model) proposed by Henrion [43] and Diez [37] which are mathematically equivalent. These 2 parameterisations differ only in the type of question that needs to be asked to the experts for knowledge elicitation. Henrion's parameterisation is supported by a question like: *"What is the probability that the effect is true given that a cause (X_i) is true and all the modelled causes are false?"*. On the other hand, Diez's parameterisation is supported by a question like: *"What is the probability that the effect is true given that a cause (X_i) is true and all other modelled and unmodelled causes are false?"*. The DeMorgan model utilised the Diez's parameterisation with a slight modification.

We could find the values for required parameters from the experts to completely define CPT using the DeMorgan model based on appropriate question for each type of causal interaction detailed below:

(i) The leak parameter: To find the value for the leak parameter, the elicitor could ask experts: "What is the probability that the child is in their non-distinguished state given that the parents are in their distinguished states?". In our example shown in Fig. 7, the elicitor could ask experts to find the value for parameter (v_{XL}): "What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written?".

(ii) Cause: To find the value for parameter corresponding to a cause, the elicitor could ask experts: "What is the probability that the child is in their non-distinguished state given that all the parents are in their distinguished states, except $X_i$and no other unmodelled causal factors are present?". In our example shown in Fig. 7, the elicitor could ask experts to find the value for parameter (v_{X1}): "What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written, and no other unmodelled causal factors are present?".

(iii) Barrier: To find the value for parameter corresponding to a barrier, the elicitor could ask experts: "What is the probability that the child is in their non-distinguished state given that all the parents are in their distinguished states, except X_i and no other unmodelled causal factors are present?". In our example shown in Fig. 7, the elicitor could ask experts to find the value for parameter (v_{X2}): "What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is not performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written, and no other unmodelled causal factors are present?".

(iv) Inhibitor: Maaskant et al. did not directly determine the value for parameters corresponding to inhibitors similar to causes and barriers as it is not practical for the example which they considered [40]. Specifically, it makes less sense to ask for the effect of presence of parent ("Rain") on the child ("Bonfire"), when the child ("Bonfire") is "False". Therefore, they determined the value for parameter corresponding to each inhibitor by determining the negative influence relative to an arbitrary (non-empty) set of causes/barriers/leak parameter. However, in our application, it is possible to determine the value for parameter corresponding to inhibitors directly as we ask for the effect of presence of parent ("Lack of physical maintenance") on the child ("Major cause for sensor (S_1) sends incorrect water level measurements"), when the latter ("Major cause for sensor (S_1) sends incorrect water level measurements") is "Accidental technical failure". In order to find the value for parameter corresponding to an inhibitor directly, the elicitor could ask the experts: "What is the probability that the child is in their distinguished state given that the parents are in their distinguished states, except U_i and no other unmodelled causal factors are present?". In our example shown in Fig. 7, the elicitor could ask experts to find the value for parameter d_{U1}: "What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is accidental technical failure given that the physical access-control for sensor (S_1) is strong, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is well-written and no other unmodelled causal factors are present?".

(v) Requirement: Maaskant et al. did not directly determine the value for parameters corresponding to requirements similar to causes and barriers as it is not practical for the example which they considered [40]. Specifically, it makes less sense to ask for the effect of absence of parent on the child, when the child is "False".

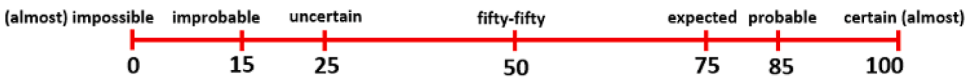


Fig. 8. Probability Scale with Numerical and Verbal Anchors.

Therefore, they determined the value for parameter corresponding to each requirement by determining the negative influence relative to an arbitrary (non-empty) set of causes/barriers/leak parameter. However, in our application, it is possible to determine the value for parameter corresponding to requirements directly as we ask for the effect of absence of parent ("Well--written maintenance procedure") on the child ("Major cause for sensor (S_1) sends incorrect water level measurements"), when the latter ("Major cause for sensor (S_1) sends incorrect water level measurements") is "Accidental technical failure". In order to find the value for parameter corresponding to a requirement directly, the elicitor could ask the experts: "What is the probability that the child is in their distinguished state given that the parents are in their distinguished states, except U_i and no other unmodelled causal factors are present?". In our example shown in Fig. 7, the elicitor could ask experts to find the value for parameter d_{U2}: "What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is accidental technical failure given that the physical access-control for sensor (S_1) is strong, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is not well-written and no other unmodelled causal factors are present?".

Once we determine the required parameters based on appropriate elicitation questions, we can completely define the CPT of the child variable using (1):

$$P(y|\boldsymbol{X},\ \boldsymbol{U}) = \left(1-(1-v_{X_L})\prod_{X_i\in\ +\boldsymbol{X}}(1-v_{X_i})\right)\prod_{U_i\ \in\ +\boldsymbol{U}}(1-d_{U_i}) \tag{1}$$

In the Eq. (1), Y represents the effect variable which has values y for the effect being in the non-distinguished state ("Intentional attack") and y' for the effect being in the distinguished state ("Accidental technical failure"). $\boldsymbol{X}$ denotes the set of parents which interact with the effect variable as promoting influences, $\boldsymbol{U}$ denotes the set of parents which interact with the effect variable as inhibiting influences, $+\boldsymbol{X}$ denotes the subset of $\boldsymbol{X}$ that contains all parents that are in their non-distinguished states, $+\boldsymbol{U}$ denotes the subset of $\boldsymbol{U}$ that contains all parents that are in their non-distinguished states. v_{XL} denotes the leak parameter which expresses the probability of y ("Intentional attack") given all parents are in their distinguished states, v_{Xi} denotes the probability of y ("Intentional attack") given that the parent X_i is not in its distinguished state and all other parents are in their distinguished states, d_{Ui} denotes the probability of y' ("Accidental technical failure") given that the parent U_i is not in its distinguished state and all other parents are in their distinguished states.

We choose the DeMorgan model for our application to reduce the number of conditional probabilities to elicit as they support modelling opposing influences with clear parameterisations.

4.2. Technique for facilitating individual probability entry

This section explains our chosen technique for facilitating individual probability entry for our application.

Our systematic method for knowledge elicitation to construct CPTs of BN models would be incomplete without a technique that facilitates individual probability entry. The DeMorgan models would help to reduce the number of conditional probabilities to elicit and allow elicitors to ask appropriate questions during probability elicitation. In addition, there should be a suitable technique which would make it easy for experts to answer elicitation questions in terms of probabilities.

There are well-known methods such as probability scale [19,44], and probability wheel [45] which would help to facilitate individual probability entry [17,46]. The basis for choosing a particular method includes accuracy, less probability elicitation time, and usability [46]. Wang et al. compared three different methods: (i) direct estimation, (ii) probability wheel and (iii) probability scale in terms of their accuracy and time taken to elicit probabilities from experts [47]. They pointed out that probability scale is better in terms of both accuracy and probability elicitation time compared to the other two methods.

A probability scale can be a horizontal or vertical line with several anchors [46]. Fig. 8 shows a probability scale with 7 numerical and verbal anchors [48]. However, there are several variants of probability scales which would help to facilitate individual probability entry. Witteman et al. compared 3 probability scales: (i) probability scale with numerical and verbal anchors, (ii) probability scale with only numerical anchors, and (iii) probability scale with only verbal anchors [49]. They compared 3 probability scales based on a study with general practitioners in the domain of medical decision making. They concluded that all 3 probability scales are equally suitable to facilitate individual probability entry. However, they recommended the probability scale with numerical and verbal anchors to facilitate individual probability entry as it provides numerical anchors for experts who prefer numbers and verbal anchors for experts who prefer words. Furthermore, Witteman et al. compared 2 different probability scales: (i) probability scale with numerical and verbal anchors, (ii) probability scale with only numerical anchors [50]. They compared 2 probability scales based on a study with arts and mathematics students. They concluded that the probability scale with numerical and verbal anchors is more comfortable to use compared to the probability scale with only numerical anchors.

There are real-world applications of the probability scale with numerical and verbal anchors in the elicitation of probabilities to construct the quantitative part of BN models [19,44]. Van der Gaag et al. used the probability scale with numerical and verbal anchors for a case study in oesophageal cancer [19]. This study was conducted with two experts in gastrointestinal oncology. The experts found that this method is easier to use than any other method they used before. Van der Gaag et al. also highlighted that the large number of probabilities are elicited in a reasonable time using this method. Furthermore, Hanninen et al. used the probability scale with numerical and verbal anchors for the construction of quantitative part of collision and grounding BN model [44]. This study was conducted with 8 experts who possessed maritime working experience between 3 and 30 years. These studies show that the probability scale with numerical and verbal anchors can be used for facilitating individual probability entry involving experts with different background.

We choose probability scales for our application as they are better in terms of accuracy and probability elicitation time compared to other methods. In particular, we would employ the probability scale with numerical and verbal anchors to facilitate individual probability entry in our application as they are effective and practicable based on previous studies. We would utilise the probability scale with 7 numerical and verbal anchors to facilitate individual probability entry with a variation. In our application, the experts could mark the suitable probability among 7 anchors in the scale directly or express fine-grained probabilities using the probability scale with numerical and verbal anchors as a supporting aid to visualise the probability range. This is convenient when the experts would like to express fine-grained probabilities based

Table 5
Parameter Elicitation for the Problem Variable (Y): Example.

Major cause for sensor (S_1) sends incorrect water level measurements (Y)	
v_{XL}	***"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack** given that the physical access-control for sensor (S_1) is strong, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written?"*
v_{X1}	***"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak,** data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written, **and no other unmodelled causal factors are present?"***
v_{X2}	***"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the** physical access-control for sensor (S_1) is strong, **data integrity verification is not performed for sensor (S_1) data,** sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written, **and no other unmodelled causal factors are present?"***
d_{U1}	***"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is accidental technical failure given that the** physical access-control for sensor (S1) is strong, data integrity verification is performed for sensor (S1) data, **sensor (S_1) is not always physically maintained,** maintenance procedure for sensor (S_1) is well-written, **and no other unmodelled causal factors are present?"***
d_{U2}	***"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is accidental technical failure given that the** physical access-control for sensor (S_1) is strong, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, **maintenance procedure for sensor (S_1) is not well-written, and no other unmodelled causal factors are present?"***

Table 6
Application of the DeMorgan Model: CPT Example.

	X_2	U_1	U_2	Y	
				Intentional Attack	Accidental Technical Failure
True	**True**	**True**	**True**	0.09	0.91
True	**True**	**True**	**False**	0.04	0.96
True	**True**	**False**	**True**	0.50 (v_{X1})	0.50
True	**True**	**False**	**False**	0.29	0.71
True	**False**	**True**	**True**	0.10	0.90
True	**False**	**True**	**False**	0.05	0.95
True	**False**	**False**	**True**	0.68	0.32
True	**False**	**False**	**False**	0.34	0.66
False	**True**	**True**	**True**	0.15	0.85 (d_{U1})
False	**True**	**True**	**False**	0.01	0.99
False	**True**	**False**	**True**	0.15 (v_{XL})	0.85
False	**True**	**False**	**False**	0.50	0.50 (d_{U2})
False	**False**	**True**	**True**	0.05	0.95
False	**False**	**True**	**False**	**0.03**	0.97
False	**False**	**False**	**True**	0.25 (v_{X2})	0.75
False	**False**	**False**	**False**	0.18	0.82

on historical data which is realistic for accidental technical failures in our application.

As a part of the probability elicitation process, in addition to the case outline, we also need to provide information related to the type of floodgate (example – criticality rating: very high) and context (example – threat level: substantial). This guideline would help to avoid very diverse responses over participants as they have substantive information based on the system knowledge. This is evident from our application of the proposed approach [16]. Furthermore, it is also important to select appropriate group of experts to elicit probabilities considering the type of floodgate and needed expertise. For instance, in our application of the proposed approach, we relied on experts who have experience working with safety and/or security of ICS in the water management sector in the Netherlands as we dealt with a type of floodgate in the Netherlands [16].

Finally, focus group workshop is one of the approaches that can be used to facilitate the probability elicitation process in addition to questionnaire [16]. The use of focus group workshops can also help to facilitate discussion among the participants once we gather the responses from each of them on the reasoning behind the varied probabilities which they provided for some variables (if any) [16]. These mechanisms would supplement the probability scales with numerical and verbal anchors and allow us to elicit reliable probabilities.

5. Application of the methodology

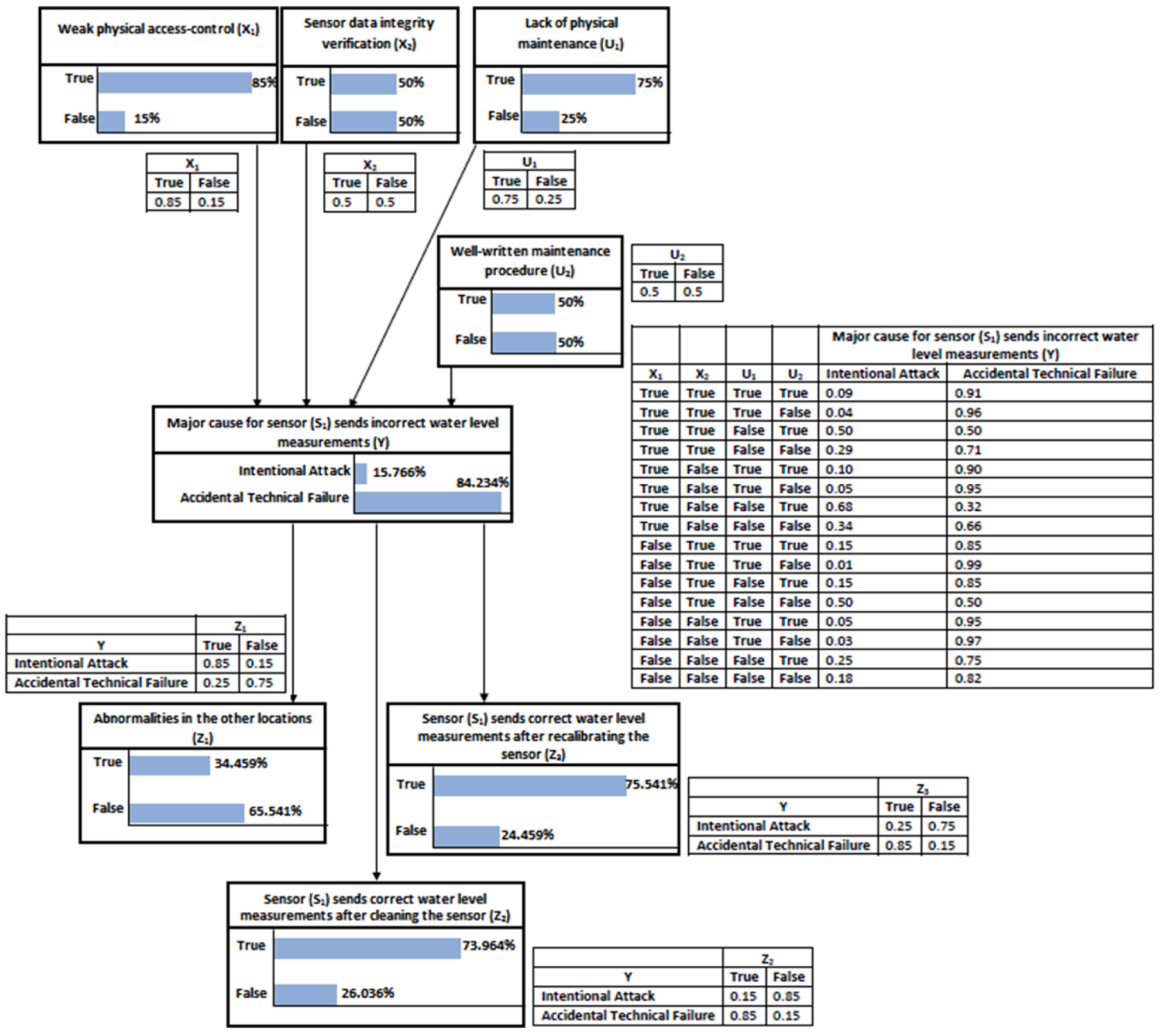
In this section, we use an illustrative case of a floodgate in the Netherlands to explain how we effectively construct CPTs of BN models for distinguishing attacks and technical failures.

We considered the upper and middle layer of our framework for the application of our methodology. It is important to reduce the number of conditional probabilities to elicit for the problem variable as a considerable number of contributory factors (upper layer), corresponding to intentional attack and accidental technical failure, typically interact with the problem variable (middle layer), which in turn increases the CPT size of the problem variable exponentially. On the other hand, the conditional probabilities for observations (or test results) (lower layer) would be easy to elicit directly as there is only one problem variable (middle layer) in our framework, which makes the CPT size of an observation (or test result) variable to 4 (2^{1+1}). We shall consider the BN model with the upper and middle layer of our framework depicted in Fig. 7 for the application of our methodology. We considered the problem "Sensor (S_1) sends incorrect water level measurements" as it could develop more complex situations in the case of floodgate. In case the floodgate closes when it should not be based on the incorrect water level measurements sent by the sensor (S_1), it would lead to severe economic damage, for instance, by delaying cargo ships. On the other hand, in case the floodgate opens when it should not be due to incorrect water level measurements sent by the sensor (S_1), it would lead to flooding.

The normal text (i.e., text without bold formatting) in Table 5 denotes the explicitly mentioned causal factors that are absent (Example: data integrity verification is performed for the sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written). This makes the probability elicitation process simple as they do not affect the corresponding probability based on our structural assumptions. The experts could directly read the remaining text (i.e., text with bold formatting) (Example: "What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak and no other unmodelled causal factors are present?") and mark the answer which could also reduce probability elicitation time.

We considered 4 contributory factors to the major causes (intentional attack or accidental technical failure) of the observed problem: (i) Weak physical access-control (X_1), (ii) Sensor data integrity verification (X_2), (iii) Lack of physical maintenance (U_1), and (iv) Well-written maintenance procedure (U_2) as shown in Fig. 7 to depict each type of causal interaction. The type of causal interaction between individual parent X_1 and the child Y is cause. The type of causal interaction between individual parent X_2 and the child Y is barrier. The type of causal interaction between individual parent U_1 and the child Y is inhibitor. The type of causal interaction between individual parent U_2 and the child Y is requirement. In this example, we need to elicit only 5 (4 + 1) parameters instead of 32 (2^{4+1}) to completely define CPT for the problem variable. The 5 parameters which we need to elicit are: $v_{X_L}, v_{X_1}, v_{X_2}, d_{U_1}, d_{U_2}$.

The values for these 5 parameters could be elicited from experts by providing the appropriate elicitation questions based on the DeMorgan model and the probability scale with numerical and verbal anchors, which could help experts answer in terms of probabilities to elicitation questions as shown in Table 5. The normal text in Table 5 makes the



X1	X2	U1	U2	Major cause for sensor (S1) sends incorrect water level measurements (Y): Intentional Attack	Accidental Technical Failure
True	True	True	True	0.09	0.91
True	True	True	False	0.04	0.96
True	True	False	True	0.50	0.50
True	True	False	False	0.29	0.71
True	False	True	True	0.10	0.90
True	False	True	False	0.05	0.95
True	False	False	True	0.68	0.32
True	False	False	False	0.34	0.66
False	True	True	True	0.15	0.85
False	True	True	False	0.01	0.99
False	True	False	True	0.15	0.85
False	True	False	False	0.50	0.50
False	False	True	True	0.05	0.95
False	False	True	False	0.03	0.97
False	False	False	True	0.25	0.75
False	False	False	False	0.18	0.82

Fig. 9. BN Model with CPTs Example.

probability elicitation process simple as they do not affect the corresponding probability based on our structural assumptions. The experts could directly read the remaining text and mark the answer for each question in Table 5 which could also reduce probability elicitation time. Suppose the expert marks the answer for v_{X_L} as 0.15, v_{X_1} as 0.50, v_{X_2} as 0.25, d_{U_1} as 0.85, d_{U_2} as 0.50. These probabilities are examples to demonstrate the application of the methodology.

Once we elicit all the required parameters, we could use (1) to completely define CPT for our example BN model. For instance, we could use (1) to calculate: $P(Y|X_1',X_2',U_1,U_2') = (1 - (1 - 0.15)(1 - 0.25))(1 - 0.85)(1 - 0.50) = 0.03$. The number with bold formatting in Table 6 denotes this probability. The completed CPT for the problem variable (Y) is shown in Table 6.

Once we complete the CPT for the problem variable, we could define the a priori probabilities for each contributory factor and observation (or test result) by eliciting corresponding probabilities directly from the experts as they are not complicated. An example BN model with corresponding CPTs for each variable is shown in Fig. 9.

Once the problem ("Sensor (S_1) sends incorrect water level measurements") is observed in the floodgate, the evidence (True/False) contributory factors and observations (or test results) could be set by the operator (or end-user) to determine the major cause for the observed problem. Once the evidence for contributory factors and observations (or test results) is set, the posterior probability of the problem variable would be computed accordingly. Based on the computed posterior probability, the appropriate response strategy could be put in place for the most likely major cause (intentional attack/accidental technical failure) for the observed problem ("Sensor (S_1) sends incorrect water level measurements") thereby minimising negative consequences.

In the example shown in Fig. 10, we provided the evidence for the contributory factors "Weak physical access-control (X_1) = True", "Sensor data integrity verification (X_2) = False", "Lack of physical maintenance (U_1) = False", "Well-written maintenance procedure (U_2) = True", and observation (or test result) "Abnormalities in other locations (Z_1) = True", "Sensor (S_1) sends correct water level measurements after recalibrating the sensor (Z_3) = False". On the other hand, we did not provide the evidence for the problem "Major cause for sensor (S_1) sends incorrect water level measurements (Y)" and observation (or test result) "Sensor (S_1) sends correct water level measurements after cleaning the sensor (Z_2)". The BN computes the posterior (updated) probabilities of the other nodes (Y, and Z_2) based on the provided evidence. The BN in Fig. 10 determines that the major cause for the observed problem "Sensor (S_1) sends incorrect water level measurements" is most likely due to intentional attack as the corresponding posterior probability (0.97306) is higher compared to the posterior probability of accidental technical failure (0.02694).

6. Discussion

An example parameter elicitation for the problem variable (Y) without reduced number of conditional probabilities is provided in Table 7). This example helps to highlight key challenges especially in

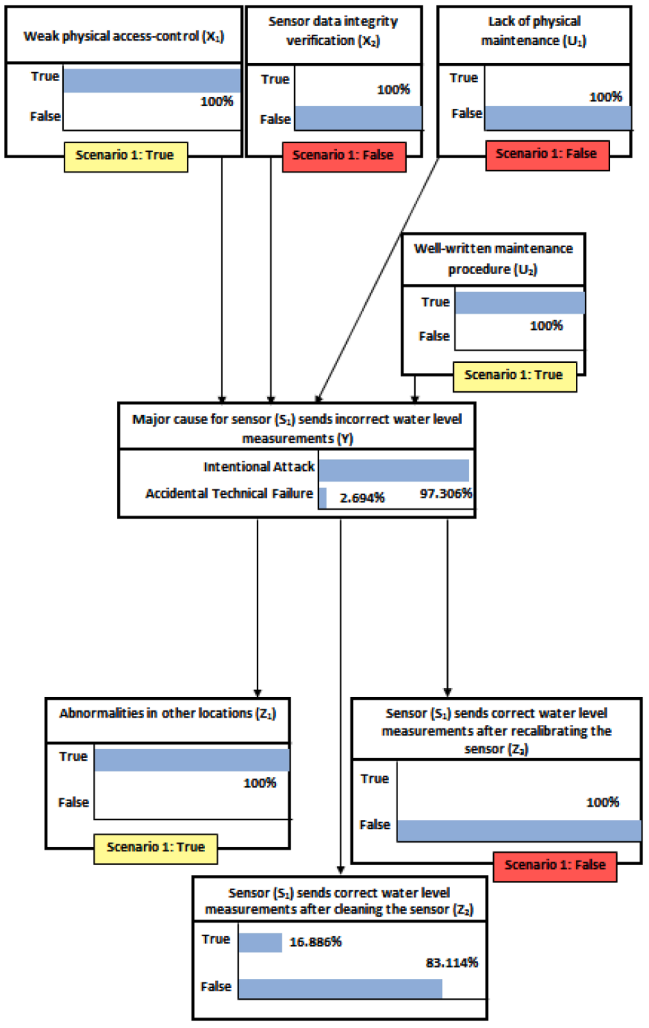


Fig. 10. BN with Updated Probabilities Based on the Evidence.

terms of number of conditional probabilities to elicit in addition to complexity of questions that experts need to answer in both cases (i.e., during parameter elicitation with and without reduced number of conditional probabilities). In the case of without number of reduced conditional probabilities, we need to elicit 16 parameters from experts for the problem variable (Y) as shown in Table 7. However, in the case of parameter elicitation with reduced number of conditional probabilities, we need to elicit only 5 parameters from experts for the problem variable (Y) as shown in Table 5. This reduces the burden of probability elicitation, which in turn can also ensure the accuracy of elicited parameters.

Moreover, in the case of parameter elicitation without reduced number of conditional probabilities based on our structural assumptions, experts need to think about multiple conditions which influence the major cause as shown in Appendix (Table 7). For instance, experts need to answer questions when all the conditions which influence the major cause are "True": *"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is well-written?"* This in turn makes it merely impossible for experts to provide reliable probabilities. However, experts need to think about only a condition which influence the major cause, in the case of parameter elicitation with reduced number of conditional probabilities as shown in Table 5. This can also ensure the accuracy of elicited

Table 7
Parameter Elicitation for the Problem Variable (Y) without Reduced Number of Conditional Probabilities: Example.

	Major cause for sensor (S_1) sends incorrect water level measurements (Y)
1	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is well-written?"
2	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is not well-written?"
3	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written?"
4	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is not well-written?"
5	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is not performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is well-written?"
6	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is not performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is not well-written?"
7	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is not performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written?"
8	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is weak, data integrity verification is not performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is not well-written?"
9	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is well-written?"
10	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is not well-written?"
11	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written?"
12	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is not well-written?"
13	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is not performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is well-written?"
14	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is not performed for sensor (S_1) data, sensor (S_1) is not always physically maintained, maintenance procedure for sensor (S_1) is not well-written?"
15	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is

(*continued on next page*)

Table 7 (*continued*)

Major cause for sensor (S_1) sends incorrect water level measurements (Y)	
	not performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is well-written?"
16	"What is the probability that the major cause for the observed problem (sensor (S_1) sends incorrect water level measurements) is intentional attack given that the physical access-control for sensor (S_1) is strong, data integrity verification is not performed for sensor (S_1) data, sensor (S_1) is always physically maintained, maintenance procedure for sensor (S_1) is not well-written?"

parameters. Furthermore, Zhang et al. also highlighted that reducing the number of conditional probabilities to elicit reduces the uncertainty and bias and improves elicitation accuracy [57]. Finally, Zagorecki et al. conducted an empirical study to elicit probabilities under Noisy-OR assumptions in addition to elicit complete probabilities directly from human experts [57]. Like DeMorgan structural assumptions, the elicitation of probabilities under Noisy-OR assumptions reduce the number of parameters that need to be elicited from exponential to linear in the number of parents to define a full CPT for the child variable. Based on the empirical study, Zagorecki et al. concluded that the elicitation of probabilities under Noisy-OR assumptions yield better accuracy than the elicitation of complete probabilities directly from human experts [58].

To determine the most critical variables, sensitivity analysis is performed with Y (Major cause for sensor (S_1) sends incorrect water level measurements) selected as the target node. The sensitivity levels are shown in Fig. 11. According to the results of the tornado diagram which shows 10 most critical events leading to Y due to intentional attack, "Lack of physical maintenance", "Well written maintenance procedure", "Weak physical access control" were identified as the top three most effective variables. Based on the tornado diagram, "Lack of physical maintenance" is identified as the most influential variable in the occurrence of the studied scenario. This in turn would help to focus on most critical variables during elicitation.

Performance-based weighting is one of the systematic approaches that can help to guarantee the accuracy of elicited parameters [51]. In this approach, each expert is weighted on their performance in answering calibration (or seed) questions. These are a set of questions from the experts' field that have observed true values and also closely related to the variables of interest [52]. The overall weight for each expert can be obtained by multiplying two separate scores, which include statistical accuracy (or calibration) score and information score [53]. Accuracy score assesses how close an expert's estimate to the truth value. Furthermore, information score assesses the amount of entropy in what the expert says or in the expert's performance. This overall weight for each expert can then be used to combine multiple expert judgements. Eggstaff et al. highlighted that the performance-based weighting significantly outperforms equally weighting expert judgement [54]. There are various applications of performance-based weighting [51,55,56]. This can supplement the proposed framework to ensure the accuracy of elicited parameters.

7. Conclusions and future work directions

Limited availability of data is one of the key challenges to construct BN models in domains like cyber security which results in modellers depending on expert knowledge. However, BNs are not suitable for knowledge elicitation involving domain experts. In our previous work, we developed a systematic method using fishbone diagrams for knowledge elicitation involving domain experts to construct the DAGs of BN models for distinguishing attacks and technical failures. Noticeably, the systematic method for knowledge elicitation involving domain experts

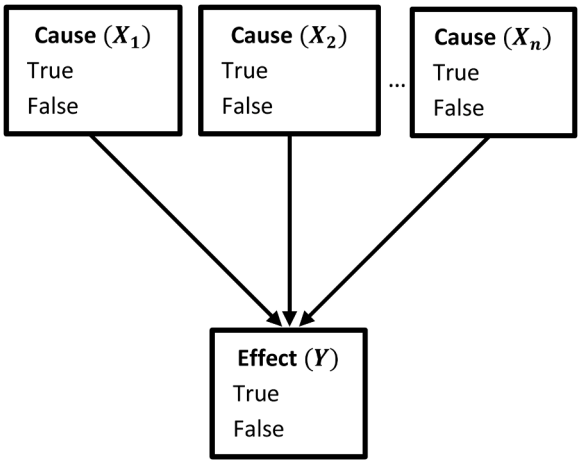


Fig. 1A. Noisy-OR Model: Structure.

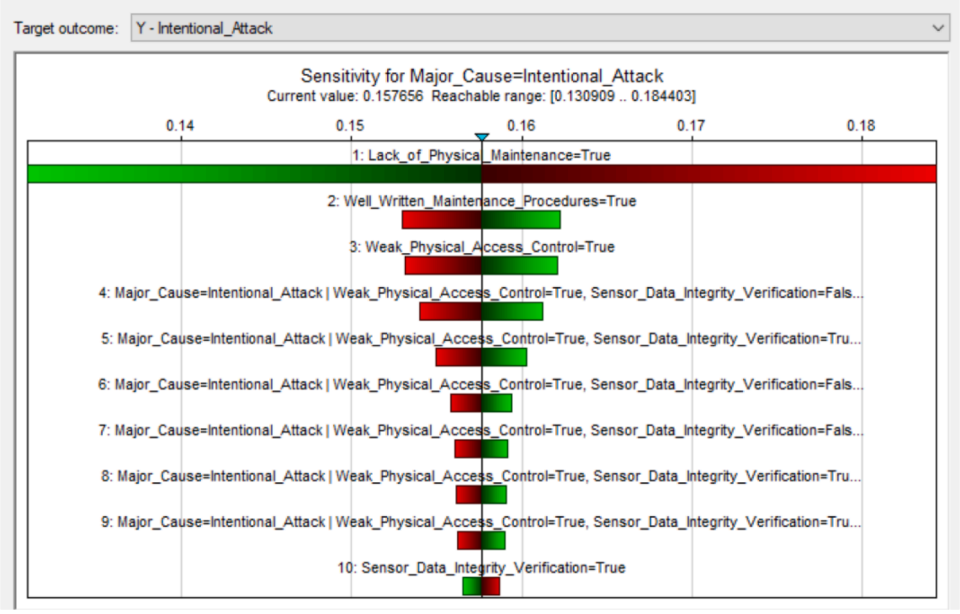


Fig. 11. Tornado Diagram Obtained from Sensitivity Analysis for Major Cause for Sensor (S_1) Sends Incorrect Water Level Measurements.

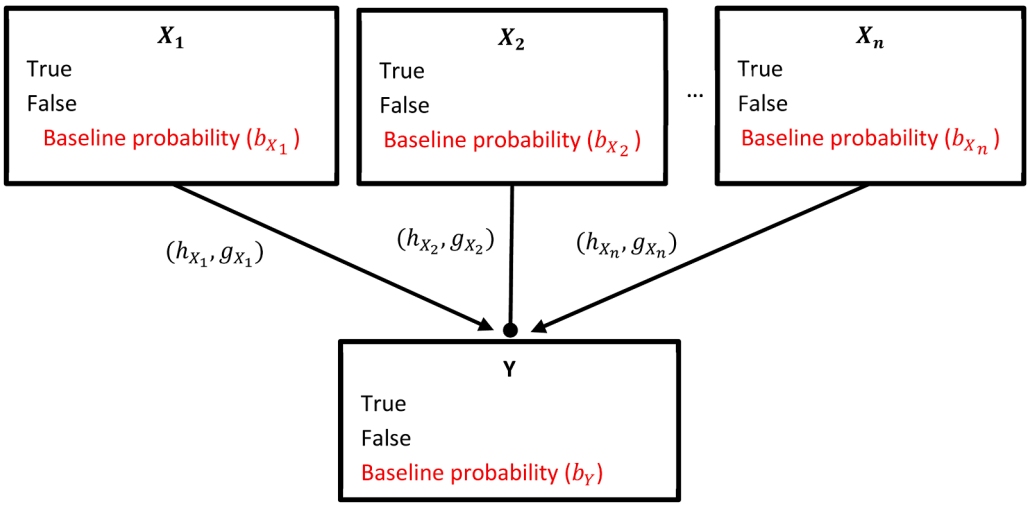


Fig. 2A. CAST Parameters.

to construct the CPTs of such BN models is missing in our previous work.

In this paper, we utilised (a) DeMorgan models to reduce the number of conditional probabilities to elicit and (b) probability scales with numerical and verbal anchors to facilitate individual probability entry. We thereby reduce the burden of probability elicitation, which is critical for BN models that rely on expert knowledge. The proposed approach can ensure the reliability of elicited probabilities by reducing the workload of experts in probability elicitation, especially DeMorgan models can reduce the number of parameters that need to be elicited from exponential to linear in the number of parents to define a full CPT for the child variable. The proposed approach also completes a holistic framework to distinguish between attacks and technical failures by proposing a systematic method for probability elicitation involving domain experts.

Furthermore, we demonstrated the proposed approach with an example problem of incorrect sensor measurements in the water management domain. Our holistic framework is directly applicable to different domains for knowledge elicitation involving domain experts to construct BN models for distinguishing attacks and technical failures. The constructed BN models could be used by operators/end-users in different domains to determine the major cause (intentional attack or accidental technical failure) of an abnormal behaviour in a component of the ICS and initiate appropriate response strategies to minimise negative consequences.

In the future, we aim to evaluate our proposed framework by constructing BN models for observable problems in the water management domain involving domain experts. Furthermore, there is a need to compare the performance of BN model constructed with and without the use of DeMorgan model in the future and determine the accuracy of the proposed approach involving DeMorgan model in the future. However, this is currently almost impossible due to the lack of empirical data and the following challenges corresponding to expert knowledge: (i) limited experts on safety and/or security of ICS in the water management sector, (ii) limited time availability of experts [16]. In addition, we aim at addressing the limitation that the DeMorgan model is suitable for binary variables only. In order to be able to reduce the number of conditional probabilities to elicit involving parents and/or child with more than two states, it is important to extend the DeMorgan model for multi-valued variables in the future.

CRediT authorship contribution statement

Sabarathinam Chockalingam: Conceptualization, Methodology, Validation, Writing – original draft. **Wolter Pieters:** Writing – review & editing, Supervision. **André M.H. Teixeira:** Writing – review & editing, Supervision. **Pieter van Gelder:** Writing – review & editing, Supervision.

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.

Data availability

No data was used for the research described in the article.

Acknowledgements

The authors wish to thank Dr. Nima Khakzad for his comments on an early draft. This research received funding from the Netherlands Organization for Scientific Research (NWO) in the framework of the Cyber Security research program under the project "Secure Our Safety: Building Cyber Security for Flood Management (SOS4Flood)".

Appendix

Noisy-OR Model

The noisy-OR model is applicable when there are several parents (causes) and a common child (effect) as shown in Fig. 1A. In general, the CPT size of a binary variable with n binary parents is 2^{n+1}. However, only n parameters are sufficient to completely define CPT using the noisy-OR model.

In the noisy-OR model, each cause variable (X_i) has the values x_i and x_i' for the presence and absence of the cause respectively. Furthermore, the effect variable (Y) has values y for the effect being present and y' for the effect being absent. The noisy-OR model assumes that the properties of exception independence and accountability holds true [38]. The property of exception independence states that presence of any single cause is enough

to produce the effect and that the hidden processes that may inhibit the occurrence of the effect are mutually independent [35]. In case all the modelled causes of the effect are false, the property of accountability requires that the effect be presumed false, i.e., $P(y'|x_1',x_2',\ldots, x_n') = 1$.

In the noisy-OR model, the effect can be caused by any cause similar to a logical-OR. However, the relationship is not deterministic – each of the causes X_i alone can cause the effect with probability p_i, which is known as link probability [36].

$$p_i = P(y|only\ X_i\ is\ present) = P\left(y|x_1^{'},\ x_2^{'},\ldots,\ x_i,\ldots,\ x_n^{'}\right)$$

Where x_1',x_2',…, x_i,…, x_n'represents the absence of the other causes except X_i.

The probability of any combination of active causes can be calculated as:

$$P(y|X) = 1 - \prod_{x_i \in X}(1 - p_i)$$

Where X represents all active causes.

Causal strength (CAST) logic

CAST logic is applicable when there are several parents and a common child as shown in Fig. 2A [39]. CAST logic assumes all the variables in the model are binary. CAST logic is only applied in the international policy and crisis analysis domain [41]. The interaction between a parent and the common child can be either promoting or inhibiting. The promoting influence is depicted by an arrowhead, whereas the negative influence is illustrated by a filled circle as shown in Fig. 2A.

The parameters which need to be elicited to completely define CPTs using CAST logic are: (i) causal strengths (g_{Xi},h_{Xi}) for each arc, and (ii) baseline probability (b) for each variable. The values of causal strengths (g_{Xi},h_{Xi}) are not probabilities and can take any arbitrary values from the range $[-1, 1]$. The value of causal strength (h_{Xi}) indicates the change in belief of Y relative to the baseline probability of Y (b_Y) under the assumption that X_i is in "True" state. For instance, h_{X_1} indicates how much the presence of X_1 would change our belief of Y. On the other hand, the value of causal strength (g_{Xi}) indicates the change in belief of Y relative to the baseline probability of effect (b_Y) under the assumption that X_i is in "False" state. For instance, g_{X_1} indicates how much the absence of X_1 would change our belief of Y.

Once we elicit the above-mentioned parameters, we could apply CAST algorithm for every combination of parent states to completely define the CPT of child variable. CAST algorithm consists of four steps: (i) aggregate positive causal strengths, (ii) aggregate negative causal strengths, (iii) combine the positive and negative causal strengths, and (iv) derive conditional probabilities.

In the first step, the positive causal strengths are aggregated using (1A):

$$S_+ = 1 - \prod_i (1 - s_{X_i}) \tag{1A}$$

Where s_{X_i} can be g_{X_i} or h_{X_i} depending on the state of the parent.

In the second step, the negative causal strengths are aggregated using (2A):

$$S_- = 1 - \prod_i (1 - |s_{X_i}|) \tag{2A}$$

Where s_{X_i} can be g_{X_i} or h_{X_i} depending on the state of the parent.

In the third step, the positive and negative causal strengths are combined. The overall influence (O) of all parents is determined using (3A) if $S_+ >=S_-$ and using (4A) if $S_- < S_+$:

$$O = 1 - \frac{1 - S_+}{1 - S_-} \tag{3A}$$

$$|O| = 1 - \frac{1 - S_-}{1 - S_+} \tag{4A}$$

In the final step, the conditional probabilities are derived using (5A) if $O_j \geq 0$ and using (6A) if $O_j < 0$:

$$P\left(Y|X_j\right) = b_Y + (1 - b_Y)\ O_j \tag{5A}$$

$$P\left(Y|X_j\right) = b_Y - b_Y|O_j| \tag{6A}$$

Where O_j denotes the overall influence of j^{th} combination of parent states X_j.

Requirements elicitation – discussion guide

Q1. When the operator notices an abnormal behaviour in a component of the ICS, how do they respond to it?
Q2. Do you have a mechanism for the operator to determine whether an abnormal behaviour in a component of the ICS is due to attacks or technical failures?
Q3. Does the same department deal with the attacks and technical failures? If not, how?
Q4. Which functionalities do you think are important in a system which helps to distinguish between attacks and technical failures?
Q5. Are there any cyber-attacks reported in your infrastructure?
Q6. Are there any technical failures reported in your infrastructure?
Q7. Do you have a repository of technical failure reports?
Q8. If so, whether this repository of technical failure reports is available for research or not?
Q9. What do you think are the alternate data sources available for research?
Q10. What are the challenges you foresee in the alternate data sources you proposed?

Q11. In addition to risk factors and symptoms based on tests, what are other elements that you would take into account when you diagnose an (intentional) attack on a component?
Q12. In addition to risk factors and symptoms based on tests, what are other elements that you would take into account when you diagnose (accidental) technical failure?
Q13. Is it possible to evaluate the developed method in the real water management infrastructure? If so, are there any challenges?
Q14. Whether do we have access to system architectures of any real water management infrastructure or not?

Constraints (Cs) and requirements (Rs)

Based on the responses which we received from the experts to those questions, the following set of constraints and high-level requirements is extracted by manually analysing the interview notes and summarising the essence of the responses:

C1. When the operators notice an abnormal behaviour in a component of the ICS, they presume that this is due to a technical failure and initiate corresponding response procedures. The response strategy initiated towards a technical failure is not effective in case of an attack.
C2. There is a lack of real data regarding cyber-attacks as they claim that there are no/limited cyber-attacks on their infrastructures. Furthermore, this is not shareable due to the sensitivity of data.
C3. Technical failures occur in their infrastructures which are documented as technical failure reports. However, they are also not shareable due to the sensitivity of data.
C4. The automation department deals with the technical failures, whereas the security department deals with cyber-attacks in the water management infrastructure. There are experts who have expertise in dealing with both technical failures and cyber-attacks.
C5. Experts are limited in this domain with limited time availability.
C6. The real water management infrastructure like a floodgate is not available for the evaluation of the developed method due to availability and criticality issues.
C7. There are system architectures with specific components which are not shareable due to the sensitivity issues. However, there is a possibility to arrange a visit to a water management infrastructure which could help to understand the system architecture on a high-level. Furthermore, the system architecture needs to be anonymised when publishing it.
C8. There is a need for decision support that would help operators to distinguish between intentional attacks and accidental technical failures as it provides input to the decision-makers to choose appropriate response strategy. However, the selection of these response strategies also depends on cost-benefit and feasibility.
R1. An effective and practical alternative to data-driven approaches for developing decision support to distinguish between attacks and technical failures is required.
R2. Decision support should help operators to distinguish between attacks and technical failures by taking into account real-time system information.
R3. The method for developing decision support should facilitate to involve experts from the department that deals with technical failures and the department that deals with cyber-attacks including experts who have expertise in dealing with both technical failures and cyber-attacks.
R4. The workload of experts during the knowledge elicitation process for developing decision support to distinguish between attacks and technical failures should be limited.
R5. The reliability of knowledge elicited for developing decision support to distinguish between attacks and technical failures should be ensured.
R6. The developed decision support should be scalable to different problems in the real environment.

References

[1] Effendi A, Davis R. ICS and IT: managing cyber security across the enterprise. In: Proceedings of the SPE middle east intelligent oil and gas conference and exhibition. Society of Petroleum Engineers; 2015.
[2] Zhivich M, Cunningham RK. The real cost of software errors. IEEE Secur Priv 2009; 7(2):87–90.
[3] Knowles W, Prince D, Hutchison D, Disso JFP, Jones K. A survey of cyber security management in industrial control systems. Int J Crit Infrastruct Prot 2015;9:52–80.
[4] RISI. "German Steel Mill Cyber Attack." http://www.risidata.com/database/detail/german-steel-mill-cyber-attack.
[5] Nikovski D. Constructing Bayesian networks for medical diagnosis from incomplete and partially correct statistics. IEEE Trans Knowl Data Eng 2000;12(4):509–16.
[6] Nakatsu RT. Reasoning with diagrams: decision-making and problem-solving with diagrams. Wiley; 2009.
[7] Cai B, Liu Y, Xie M. A dynamic-Bayesian-network-based fault diagnosis methodology considering transient and intermittent faults. IEEE Trans Autom Sci Eng 2016;14(1):276–85.
[8] Cai B, Liu H, Xie M. A real-time fault diagnosis methodology of complex systems using object-oriented Bayesian networks. Mech Syst Sig Process 2016;80:31–44.
[9] Cai B, Xie M, Liu Y, Liu Y, Feng Q. Availability-based engineering resilience metric and its corresponding evaluation methodology. Reliab Eng Syst Saf 2018;172: 216–24.
[10] Cai B, et al. Remaining useful life estimation of structure systems under the influence of multiple causes: subsea pipelines as a case study. IEEE Trans Ind Electron 2019;67(7):5737–47.
[11] Ben-Gal I. Bayesian networks. Encyclopedia of statistics in quality and reliability. Ltd: John Wiley & Sons; 2008.
[12] Darwiche A. Bayesian networks. Found Artif Intell 2008;3:467–509.
[13] Cai B, et al. Application of Bayesian networks in reliability evaluation. IEEE Trans Ind Inf 2018;15(4):2146–57.
[14] Chockalingam S, Pieters W, Teixeira A, Khakzad N, van Gelder P. Combining Bayesian networks and fishbone diagrams to distinguish between intentional attacks and accidental technical failures. Graphical models for security, 11086. Springer; 2019. p. 31–50. https://doi.org/10.1007/978-3-030-15465-3_3.
[15] Chockalingam S, Pieters W, Teixeira A, van Gelder P. Bayesian network models in cyber security: a systematic review. In: Proceedings of the Nordic conference on secure IT systems. Springer; 2017. p. 105–22.
[16] Chockalingam S, Pieters W, Teixeira A, van Gelder P. Bayesian network model to distinguish between intentional attacks and accidental technical failures: a case study of floodgates. cybersecur 2021;4(1):1–19.
[17] Zhang G, Thai VV. Expert elicitation and Bayesian Network modeling for shipping accidents: a literature review. Saf Sci 2016;87:53–62.
[18] Maaskant PP, Druzdzel MJ. An independence of causal interactions model for opposing influences. In: Proceedings of the 4th European workshop on probabilistic graphical models; 2008. p. 185–92.
[19] van der Gaag LC, Renooij S, Witteman C, Aleman BM, Taal BG. Probabilities for a probabilistic network: a case study in oesophageal cancer. Artif Intell Med 2002;25 (2):123–48.
[20] van der Gaag LC, Renooij S, Witteman CL, Aleman BM, Taal BG. How to elicit many probabilities. In: Proceedings of the 15th conference on Uncertainty in artificial intelligence. Morgan Kaufmann Publishers Inc.; 1999. p. 647–54.
[21] Seixas FL, Zadrozny B, Laks J, Conci A, Saade DCM. A Bayesian network decision model for supporting the diagnosis of dementia, Alzheimer′ s disease and mild cognitive impairment. Comput Biol Med 2014;51:140–58.
[22] Huang Y, McMurran R, Dhadyalla G, Jones RP. Probability based vehicle fault diagnosis: Bayesian network method. J Intell Manuf 2008;19(3):301–11.
[23] Hevner A, Chatterjee S. Design science research in information systems. Design research in information systems. Springer; 2010. p. 9–22.
[24] Johannesson P, Perjons E. An introduction to design science. Springer; 2014.
[25] March ST, Smith GF. Design and natural science research on information technology. Decis Support Syst 1995;15(4):251–66.

[26] Endi M, Elhalwagy Y. Three-layer plc/scada system architecture in process automation and data monitoring. In: Proceedings of the computer and automation engineering (ICCAE). 2. IEEE; 2010. p. 774–9. 2010 the 2nd international conference on.
[27] Skopik F, Smith P. Smart grid security: innovative solutions for a modernized grid. Syngress; 2015.
[28] Doggett AM. Root cause analysis: a framework for tool selection. Qual Manag J 2005;12(4):34.
[29] Ilie G, Ciocoiu CN. Application of fishbone diagram to determine the risk of an event with multiple causes. Manag Res Pract 2010;2(1):1–20.
[30] K. Ishikawa, Guide to quality control (no. TS156. I3713 1994). 1982.
[31] Desai MS, Johnson RA. Using a fishbone diagram to develop change management strategies to achieve first-year student persistence. SAM Adv Manag J 2013;78(2):51.
[32] White AA, et al. Cause-and-effect analysis of risk management files to assess patient care in the emergency department. Acad Emerg Med 2004;11(10):1035–41.
[33] Zhang NL, Poole D. Exploiting causal independence in Bayesian network inference. J Artif Intell Res 1996;5:301–28.
[34] Fallet-Fidry G, Weber P, Simon C, Iung B, Duval C. Evidential network-based extension of Leaky Noisy-OR structure for supporting risks analyses. Fault Detect Superv Saf Techn Process 2012;8(1):672–7.
[35] Bolt JH, van der Gaag LC. An empirical study of the use of the noisy-OR model in a real-life Bayesian network. In: Proceedings of the international conference on information processing and management of uncertainty in knowledge-based systems. Springer; 2010. p. 11–20.
[36] Anand V, Downs SM. Probabilistic asthma case finding: a noisy or reformulation. In: Proceedings of the AMIA Annual symposium proceedings. 2008. American Medical Informatics Association; 2008. p. 6–10.
[37] Diez FJ. Parameter adjustment in Bayes networks. The generalized noisy OR–gate. Uncertainty in artificial intelligence, 1993. Elsevier; 1993. p. 99–105.
[38] Woudenberg SP, Van Der Gaag LC. Using the noisy-or model can be harmful… but it often is not. In: Proceedings of the European conference on symbolic and quantitative approaches to reasoning and uncertainty. Springer; 2011. p. 122–33.
[39] Rosen JA, Smith WL. Influence net modeling with causal strengths: an evolutionary approach. In: Proceedings of the command and control research and technology symposium. Citeseer; 1996. p. 25–8.
[40] P. Maaskant, "A causal model for qualitative reasoning," MSc Thesis, Delft University of Technology, 2006.
[41] Zagorecki A. Local probability distributions in bayesian networks: knowledge elicitation and inference. University of Pittsburgh; 2010.
[42] Kraaijeveld P. Genierate: an interactive generator of diagnostic bayesian network models. Citeseer; 2005.
[43] M. Henrion, "Practical issues in constructing a bayes' Belief Network," arXiv preprint arXiv:1304.2725, 2013.
[44] Hänninen M, et al. Expert elicitation of a navigation service implementation effects on ship groundings and collisions in the Gulf of Finland. In: Proceedings of the institution of mechanical engineers, part o: journal of risk and reliability. 228; 2014. p. 19–28.
[45] Wang H, Druzdzel MJ. User interface tools for navigation in conditional probability tables and elicitation of probabilities in Bayesian networks. In: Proceedings of the 16th conference on Uncertainty in artificial intelligence. Morgan Kaufmann Publishers Inc.; 2000. p. 617–25.
[46] Renooij S. Probability elicitation for belief networks: issues to consider. Knowl Eng Rev 2001;16(3):255–69.
[47] Wang H, Dash D, Druzdzel MJ. A method for evaluating elicitation schemes for probabilistic models. IEEE Trans Syst Man Cybern Part B (Cybern) 2002;32(1):38–43.
[48] Renooij S, Witteman CLM. Talking probabilities: communicating probabilistic information with words and numbers. Utrecht University: Information and Computing Sciences; 1999.
[49] Witteman CL, Renooij S, Koele P. Medicine in words and numbers: a cross-sectional survey comparing probability assessment scales. BMC Med Inf Decis Making 2007;7(1):13.
[50] Witteman C, Renooij S. Evaluation of a verbal–numerical probability scale. Int J Approx Reason 2003;33(2):117–31.
[51] Aspinall WP, Cooke RM, Havelaar AH, Hoffmann S, Hald T. Evaluation of a performance-based expert elicitation: WHO global attribution of foodborne diseases. PLoS One 2016;11(3):e0149817.
[52] Colson AR, Cooke RM. Expert elicitation: using the classical model to validate experts' judgments. Rev Environ Econ Policy 2020.
[53] Hanea A, Nane G. Calibrating experts' probabilistic assessments for improved probabilistic predictions. Saf Sci 2019;118:763–71.
[54] Eggstaff JW, Mazzuchi TA, Sarkani S. The effect of the number of seed variables on the performance of Cooke′ s classical model. Reliab Eng Syst Saf 2014;121:72–82.
[55] Jaiswal K, Aspinall W, Perkins D, Wald D, Porter K. Use of expert judgment elicitation to estimate seismic vulnerability of selected building types. In: Proceedings of the 15th world conference on earthquake engineering; 2012. 24-28 Sep 2012.
[56] Naseri M, Fuqing Y, Barabady J. Performance-based aggregation of expert opinions for reliability prediction of Arctic offshore facilities. In: Proceedings of the IEEE international conference on industrial engineering and engineering management (IEEM). IEEE; 2015. p. 1062–6.
[57] Zhang G, Thai VV. Expert elicitation and Bayesian Network modeling for shipping accidents: a literature review. Saf Sci 2016;87:53–62.
[58] Zagorecki A, Druzdzel MJ. An empirical study of probability elicitation under noisy-OR assumption. In: Proceedings of the flairs conference; 2004. p. 880–6.