Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27870-cd

Handling Uncertainty in Maritime Incident Assessment: An Approach to Safety–Security Classification

Frank Sill Torres, Babette Münch, Melina Bischoff, Daniel Hofmann, Jan Stockbrügger

German Aerospace Center, Institute for the Protection of Maritime Infrastructures, Germany.
E-mail: (Frank.SillTorres, Babette.Muench, melina.bischoff, daniel.hofmann, jan.stockbruegger)@dlr.de

Distinguishing whether a maritime incident stems from safety-related, i. e. accidental, or security-related, , i. e. deliberate, causes is a central challenge, particularly in early phases when available information is incomplete, ambiguous, or contradictory. Although both domains may involve similar observable hazards, they differ in underlying mechanisms, institutional responsibilities, and required response measures. Decision makers must therefore evaluate high-impact situations under considerable epistemic uncertainty. This paper proposes a structured decision-support framework based on Credal Networks, which extend Bayesian Networks by representing probabilities as intervals rather than precise point estimates. The approach is designed to be adaptable to specific maritime contexts. It includes a methodology for identifying and structuring observable indicators using a Human–Technology–Environment categorization, followed by the derivation of causal relationships and the estimation of corresponding credal sets. A representative use case involving a technically impaired vessel near critical infrastructure demonstrates the applicability of the method. The results confirm its feasibility and underline the value of credal networks for uncertainty-aware early-phase maritime incident classification.

Keywords: Maritime Security, Maritime Safety, Credal Networks, Decission Support, Critical Infrastructures

1. Introduction

The maritime domain is characterized by complex operational environments, dense traffic flows, and the presence of critical infrastructure such as submarine cables, offshore energy installations, and port facilities. In this setting, incidents may originate from unintentional safety-related causes, such as technical failures, human error, or adverse environmental conditions, or from deliberate security-related actions, including sabotage or other hostile interference. Distinguishing between these two categories at an early stage is a fundamental challenge for maritime authorities and infrastructure operators.

Although safety and security share certain observable hazards, like vessel malfunctions, abnormal maneuvers, or communication failures, their underlying mechanisms, escalation dynamics, and response requirements differ substantially. Safety incidents typically demand technical mitigation and rescue coordination, whereas security-related events may require law-enforcement involvement, intelligence assessment, or protective measures for critical infrastructure Larsson (2024). Misclassification can therefore lead to inappropriate or delayed response actions, with potentially severe operational, economic, and geopolitical consequences.

Early-phase assessment is particularly difficult because available information is often incomplete, ambiguous, or even contradictory. Sensor data may be unreliable, weather conditions may obscure observations, and communication with involved actors may be limited. Moreover, indicators such as switched-off AIS (Automatic Identification System), unexpected course deviations, or the presence of non-official vessels can be interpreted in multiple ways. Decision makers must therefore evaluate high-impact scenarios under substantial epistemic uncertainty, while still providing timely recommendations.

Traditional probabilistic decision-support approaches, such as Bayesian networks, offer a structured framework for modeling dependencies between indicators and hypotheses. However, they require precise probability specifications, which may not be justifiable in early incident phases when data are sparse or expert assessments di-

vergeMauá and Cozman (2020). In such situations, point probabilities can create an illusion of precision and obscure the extent of uncertainty influencing the classification.

To address this limitation, this paper proposes a structured decision-support framework based on credal networks. Credal networks generalize Bayesian networks by allowing sets or intervals of probabilities instead of single values, thereby enabling robust inference under imprecise or conflicting evidence **??**. By explicitly modeling epistemic uncertainty, the approach not only estimates the likelihood of safety- versus security-driven causes but also reveals where critical information gaps might affect the assessment.

The remainder of this paper is organized as follows. Section 2 provides preliminary information on the subject of this work. Section 3 introduces the proposed methodology in detail, while Section 4 discusses an exemplary use case. Finally, Section 5 concludes this work.

2. Preliminaries

This section outlines the necessary background and technical foundations.

2.1. *Maritime Safety and Security*

In the maritime context, the terms safety and security are often used together, but refer to different types of risks, responsibilities and authorities. Both concepts serve to protect people, the environment and maritime infrastructure, but are assigned to different stakeholder groups, decision-making processes and operational responsibilities. Accordingly, safety- and security-related incidents are handled in practice by different authorities and organizations.

Maritime safety describes the protection against unintentional hazards resulting from technical defects, human error, organizational weaknesses or environmental influences. It is characterized by the absence of a deliberate intention to cause harm. The assessment of such events focuses on technical reliability, organizational framework conditions and external influencing factors such as environmental conditions or local traffic density in the sea area.

Maritime security refers to deliberate, targeted actions aimed at damaging, disrupting or exploiting maritime systems. Security incidents are characterized by an intentional component and can involve both state and non-state actors. The analysis focuses in particular on behavioral patterns, anomalies, target reference and the ability of an actor to consciously plan and adapt measures.

In practice, however, the safety and security dimensions are not strictly separate. In particular, grey zone or hybrid events can have both intentional and unintentional causes Larsson (2024). A systematic classification of such incidents can be achieved by combining technical characteristics, human or behavioral actions, and environmental factors, and this provides the basis for deriving suitable indicators.

2.2. *Probabilistic Networks*

Probabilistic networks are graphical models for representing and analyzing uncertain systems. In safety and security contexts, they provide a structured framework for modeling dependencies among hazards, threats, and system components. By combining prior knowledge with observed evidence, they support quantitative risk and threat assessment and enable the continuous updating of risk estimates as new information becomes available.

Bayesian Networks (BNs) are a prominent class of probabilistic networks and are widely applied across various domains Ramírez Agudelo et al. (2021); Tecklenburg et al. (2022). In safety and security applications, they are used to aggregate risks associated with individual subsystems or components into an overall system-level risk evaluation.

Formally, a Bayesian network consists of a directed acyclic graph (DAG) whose nodes represent random variables in the set $\mathbf{X} = X_1, \ldots, X_n$, together with a joint probability distribution $\mathcal{P}(\mathbf{X})$ over these variables Mauá and Cozman (2020). The nodes of the DAG correspond to partial risks or system states, while directed edges encode conditional dependencies among them. Each variable X_i is associated with a conditional probability table (CPT) that specifies $P(X_i \mid Pa(X_i))$,

where $Pa(X_i)$ denotes the set of parent nodes of X_i Zinke et al. (2020).

The joint probability distribution over all variables can be factorized according to the network structure as shown in Eq. 1. In particular, the probability of each node X_i is defined conditionally on its parent nodes.

$$P(X_i, \ldots, X_n) = \prod_{i=1}^{n} P\big(X_i \mid Pa(X_i)\big) \quad (1)$$

Credal Networks (CNs) extend BNs by relaxing the assumption that all probabilities are precisely known Mauá and Cozman (2020); Corani, Antonucci, and Zaffalon (Corani et al.). Instead of assigning a single conditional probability distribution to each node, a CN specifies a set of plausible probability distributions, typically represented as intervals or convex sets. This allows the explicit modeling of epistemic uncertainty arising from incomplete data, imprecise expert knowledge, or conflicting information.

Formally, each CPT is replaced by a *credal set* $\mathcal{K}(X_i)$, i. e. a closed and convex set of probability distributions for a random variable X_i. Furthermore,the set comprising its extreme points is denoted by $ext[\mathcal{K}(X_i)]$. As a consequence, inference does not yield a single posterior probability but lower and upper probability bounds. Lower and upper probabilities $\underline{P}$ and $\overline{P}$ obtainable for a variable X_i are respectively defined by Eqs. 2 and 3.

$$\underline{P}(X_i) = \min_{P(X_i)\in \mathrm{ext}[(\mathcal{K}X_i]} P(X_i), \quad (2)$$

$$\overline{P}(X_i) = \max_{P(X_i)\in \mathrm{ext}[(\mathcal{K}X_i]} P(X_i), \quad (3)$$

In safety and security contexts, CNs are particularly useful when reliable statistical data are scarce or when conservative risk estimates are required. By propagating probability bounds rather than point estimates, they provide a more robust basis for decision-making under severe uncertainty.

3. Methodology

This section discusses the proposed methodology and details its individual elements.

Ongoing maritime scenarios are often ambiguous in their interpretation, such that safety and security incidents cannot be reliably distinguished based on individual observable indicators alone. Instead, the distinction must be derived from the combined effect of multiple contributing factors.

Accordingly, the primary objective of the proposed methodology is to provide an expert-driven probabilistic framework for distinguishing between safety and security incidents in ongoing maritime situations. Given the diversity of operational environments in the maritime domain, a single generic solution applicable to all scenarios is not feasible. For instance, situations occurring in offshore wind farms differ substantially from those in port areas. The methodology is therefore designed to enable the development of environment-specific models tailored to the characteristics of each scenario.

As discussed in Section 2, Credal Networks (CNs) are a well-established and widely applied approach for modeling situations characterized by significant uncertainty in expert knowledge and available information. Accordingly, the proposed methodology focuses on the design of such CNs for applications in the maritime domain.

The proposed methodology employs the Human–Technical–Environmental (HTE) categorization Selin and Selin (2023). The human component captures behavioral anomalies as well as the willingness of involved actors to communicate and cooperate. The technical component considers damage patterns, system malfunctions, and their potential impact on maritime infrastructure. The environmental component addresses external physical and atmospheric influences within the operational area, acknowledging that adverse weather conditions or natural anomalies can contribute to accidents or technical failures. This division into three components enables a structured weighting of the various influencing factors and supports the translation of causal relationships into a more coherent probabilistic assessment.

This proposed methodology consists of following steps.

Context definition: This initial step defines the overall setting in which the method will be applied. It includes specifying the location, identifying relevant infrastructure, assessing environmental conditions, determining the types of actors involved (e. g., vessels and/or aerial drones), and considering technical aspects such as available surveillance and communication systems, as well as the applicable regulatory framework.

Identification of observable indicators: This step focuses on identifying measurable quantities, features, or observations that will be available for scenario analysis. These indicators are grouped into the following categories:

- **Human**, such as *NoResponseToRadio*, indicating that involved actors are not communicating, or *AbnormalMovement*, indicating unexpected vessel movement.
- **Technical**, such as *NearbyInfrastructure*, indicating that relevant or critical infrastructure is located close to the event site, or *SystemIntegrityFailure*, indicating that integrity checks of the surveillance system have reported an error.
- **Environmental**, such as *HighWaves*, indicating rough sea conditions near the event site, or *UndisclosedDepths*, indicating the presence of known but poorly charted depths in the surrounding area.

Definition of intermediate causal factors: In this approach, intermediate causal factors translate observable indicators into higher-level situational states that ultimately determine whether a safety or security incident occurs. This final outcome is driven by the intermediate factors *Human*, *Technical*, and *Environmental*. These factors, in turn, receive causal input from additional intermediate variables that are directly connected to the observable indicators.

For example, the factor *Technical* receives information from the intermediate factors *SecondaryDamages* and *TechnicalAnomalies*. These are linked to the observable nodes *NearbyInfrastructure* and *InfrastructureDestroyed*, and *RadioDisfunction* and *SystemIntegrityFailure*, respectively.

The definition of the intermediate causal factors is closely tied to the design of the network architecture, which naturally emerges from the underlying causal relationships.

Elicitation of conditional probability tables (CPTs): The CPTs of all nodes are parameterized in a two-step process. First, the network is treated as a Bayesian Network (BN), and the CPTs are elicited using expert-driven methods[a] Fenton and Neil (2018); Weber et al. (2012). Expert assessments are based on the verbal–numerical scale proposed by Renooij et al. Renooij and van der Gaag (2002), which establishes a mapping between qualitative judgments and quantitative probability values $p \in (0, 1)$, with *Almost impossible* $\rightarrow p = 0$, *Improbable* $\rightarrow p = 0.15$, *Uncertain* $\rightarrow p = 0.25$, *fifty-fifty* $\rightarrow p = 0.5$, *Expected* $\rightarrow p = 0.75$, *Probable* $\rightarrow p = 0.85$, *Almost certain* $\rightarrow p = 1$. While more fine-grained verbal–numerical scales, such as the one proposed by Walley Walley (1996), could also be employed, the quantification of probabilities in the context of security events is inherently challenging. Using overly detailed scales therefore bears the risk of assigning seemingly precise values without a sufficiently reliable basis.

During this step, a confidence level is assigned to each node and recorded as an uncertainty factor $u \in (0, 0.3)$. This factor ranges from *very low uncertainty* ($u = 0.05$), *low uncertainty* ($u = 0.1$), *high uncertainty* ($u = 0.2$), to *very high uncertainty* ($u = 0.3$).The resulting uncertainty values are then averaged across all expert assessments.

In the following step, the BN is transformed by determining the respective ranges for each CPT considering the uncertainty using following procedure.

Let X_i be a discrete node with state space $\mathcal{X}i = x_1, \ldots, x_m$ and parent set $Pa(X_i)$. For a fixed parent configuration $\pi \in \mathcal{X}Pa(X_i)$, denote the

[a]The methodology also allows for data-driven parameterization; however, this is beyond the scope of the present work.

corresponding row of the original CPT by

$$p_k(\pi) := P(X_i = x_k \mid Pa(X_i) = \pi), \quad k = 1, \ldots, m, \tag{4}$$

with the normalization condition

$$\sum_{k=1}^{m} p_k(\pi) = 1. \tag{5}$$

for each state x_i, the corresponding interval of unnormalized weights is defined as

$$w_i(\pi) \in \Big[\, p_i(\pi)\big(1 - \tfrac{u}{2}\big),\ p_i(\pi)\big(1 + \tfrac{u}{2}\big)\Big]. \tag{6}$$

The uncertainty parameter u is halved to ensure that the interval is applied symmetrically around the nominal probability $p_i(\pi)$, so that the total relative width of the interval equals u.

The corresponding *credal set* $\mathcal{K}(\pi)$ for a fixed parent configuration π is defined as

$$\mathcal{K}(\pi) = \Bigg\{ q \in \Delta^{m-1} \;\Big|\; \exists\, w \in \mathbb{R}^m_{\geq 0} : w_i \in \big[p_i(\pi)(1 - \tfrac{u}{2}),\, p_i(\pi)(1 + \tfrac{u}{2})\big], \quad q_i = \frac{w_i}{\sum_{j=1}^{m} w_j},\ i = 1, \ldots, m \Bigg\}. \tag{7}$$

where $\Delta^{m-1} = \{q \in \mathbb{R}^m_{\geq 0} : \sum_{i=1}^{m} q_i = 1\}$ is the probability simplex.

In the case of binary nodes $X_i \in \{0, 1\}$, this simplifies to

$$\mathcal{K}_{bin}(\pi) = \Big\{ q \in \Delta^1 \;\Big|\; q_1 \in \big[p_1(\pi)(1 - \tfrac{u}{2}),\, p_1(\pi)(1 + \tfrac{u}{2})\big], q_0 = 1 - q_1 \Big\}. \tag{8}$$

4. Representative use case

The selected use case focuses on a vessel potentially in distress within an Exclusive Economic Zone (EEZ) and in close proximity to critical infrastructure (CRITIS). A disabled vessel may drift due to wind and currents or deploy its anchor as an emergency measure. Both situations pose a potential threat to nearby infrastructure, particularly submarine communication or power cables. From a safety and security perspective, such incidents require rapid risk assessment and coordinated response measures to prevent accidental damage and to evaluate the possibility of intentional interference.

For validation purposes, the following four real-world incidents have been selected.

Scenario 1 – C-Lion1: In November 2024, the C-Lion1 submarine data cable between Finland and Germany was damaged. The exact cause remained under investigation; authorities considered external impacts such as fishing equipment or anchor drag, while political discussions also raised concerns about possible hybrid threats Mukherjee (2024).

Scenario 2 – Estlink-2: On 25 December 2024, the Estlink-2 power cable and nearby telecommunications cables in the Gulf of Finland were severed. Finnish authorities suspected that a tanker had dragged its anchor across the seabed, leading to investigations and temporary restrictions imposed on the vessel and its crew News (2024).

Scenario 3 – LVRTC cable: In January 2025, a submarine data cable between Sweden and Latvia, operated by Latvia's State Radio and Television Centre (LVRTC), was damaged in the Baltic Sea. Although initial suspicion pointed to deliberate sabotage, investigations later attributed the incident to anchor drag and poor seamanship under adverse weather conditions Sytas and Ahlander (2025).

Scenario 4 – TPECS: In January 2025, the vessel Shunxing-39 was suspected of damaging a segment of the Trans-Pacific Express Cable System (TPECS), an undersea fiber-optic cable linking Taiwan to the U.S. West Coast. The damage was reportedly caused by anchor dragging north of Taiwan News (2025).

4.1. *Credal Network Design*

The generation of the CN started with the definition of the context. The incident side is placed in open waters in an EEZ. Thus, ship traffic control and surveillance is provided by maritime authorities. Also, AIS must be turned on in case of vessels with over 300 gross tonnage on international voyage and over 500 gross tonnage on national voyage, and all passenger ships. Furthermore, CRITIS like data cables, pipelines, offshore wind farms

and offshore HVDC converter platforms, are located nearby.

Next, the observable indicators were identified based on the HTE approach discussed in the previous section. With respect to the human factor, affected actors may exhibit conspicuous behavior through atypical movement patterns, represented by the indicator *AbnormalMovement*. A lack of willingness to communicate or cooperate may be reflected by the deactivation of the AIS or by radio silence, captured by the indicators *AISoff* and *NoResponseToRadio*. The involvement of additional actors can be inferred from the presence of unidentified vessels or actors that are not part of maritime authorities in the vicinity of the incident, represented by the indicators *UnidentifiedActorsNearby* and *NonOfficialsNearby*. If these actors are also associated with known critical states with respect to the EEZ state (indicator *CriticalStates*) or past incidents (indicator *PastIncidents*), the likelihood of classifying the situation as security-relevant is further increased.

For the technical component, the focus is on indicators that can be observed in ongoing situations and do not require forensic analysis. The indicator *RadioDisfunction* captures known disturbances of radio communication in the vicinity of the incident, while *SystemIntegrityFailure* reflects reported malfunctions of the deployed surveillance systems. Potential effects on nearby infrastructure are considered in terms of secondary damage. The indicator *NearbyInfrastructure* reflects the presence of relevant or critical infrastructure that may be affected, whereas *InfrastructureDestroyed* records reported damage or destruction of such infrastructures.

For the environmental component, adverse weather conditions are represented by the indicators *HighWaves*, set to true for wave heights exceeding 2.5 m; *HighWind*, set to true for wind speeds above 25 m/s; and *ExtremeWeather*, which reflects the presence of official weather warnings Sill Torres et al. (2020). Natural hazards and geographical characteristics are captured by the indicators *NaturalDisaster*, based on official warning information, and *UndisclosedDepths*, described in Section 3.

Based on the identified observable indicators, intermediate causal factors were defined. As a result, the node *Human* (state 1: *critical/complicated*) receives input from the nodes *AffectedActors* (state 1: *suspicious*) and *OtherActors* (state 1: *suspicious*). The node *Technology* (state 1: *critical/complicated*) depends on *SecondaryDamages* (state 1: *present*) and *TechnicalAnomalies* (state 1: *present*). Finally, the node *Environment* (state 1: *critical/complicated*) receives input from *WeatherConditions* (state 1: *critical/complicated*) and *NaturalAnomalies* (state 1: *pronounced*). The resulting network structure is shown in Fig. 1.

The CPTs were specified based on expert elicitation. The resulting credal sets, including the quantified uncertainty assessments provided by the experts, are presented in the Appendix.

4.2. *Results and Discussion*

The networks were implemented in Python using the *pyAgrum* framework. Inference was performed with the *LazyPropagation* engine for BNs and *CNMonteCarloSampling* for CNs. For each scenario, the corresponding evidence was defined based on a literature review. The resulting evidence configurations are provided in the Appendix.

Table 1 and Fig. 2 present the posterior probabilities and probability intervals of the node *IncidentType* obtained for both the CN and the BN across the selected scenarios.

For all scenarios, the BN results lie within the corresponding CN probability intervals, as expected. The credal approach thus provides a more comprehensive assessment by explicitly quantifying epistemic uncertainty and offering a range of plausible outcomes rather than a single point estimate.

Table 1. Posterior probabilities and intervals for the outcome *security event*.

	CN_{min}	CN_{max}	BN
Scenario 1	0.71	0.94	0.85
Scenario 2	0.67	0.91	0.80
Scenario 3	0.60	0.81	0.72
Scenario 4	0.69	0.89	0.81

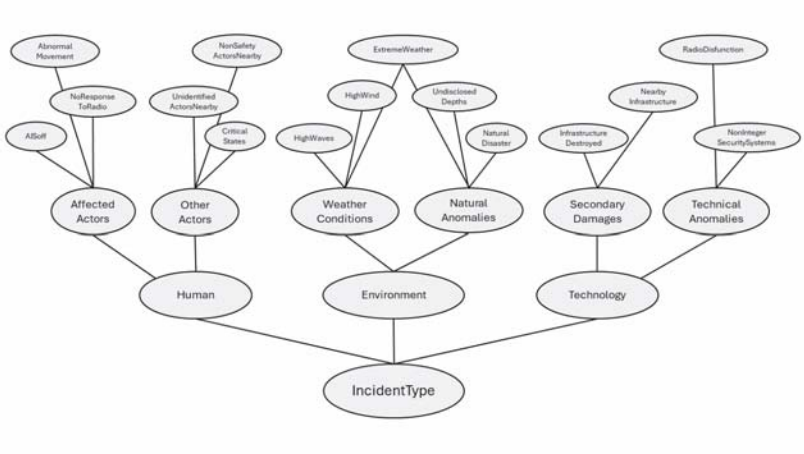

Fig. 1. Credal Network architecture of exemplary use case

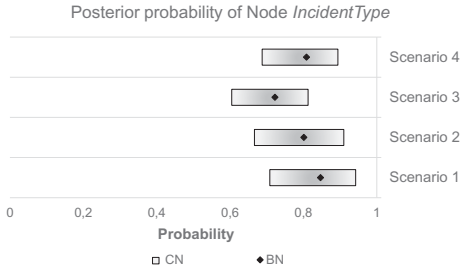

Fig. 2. Posterior probabilities and intervals for the outcome *security event* for the CN and BN

5. Conclusion

This work addressed the challenge of distinguishing between accidental and deliberate maritime incidents under conditions of early-phase uncertainty. It introduced a decision-support framework based on Credal Networks, enabling probabilistic reasoning while explicitly accounting for epistemic uncertainty. A representative use case demonstrated the feasibility and practical relevance of the proposed approach.

References

Corani, G., A. Antonucci, and M. Zaffalon. Bayesian networks with imprecise probabilities: Theory and application to classification. In *Data Mining*.

Fenton, N. and M. Neil (2018). *Risk Assessment and Decision Analysis with Bayesian Networks* (2 ed.). CRC Press.

Larsson, O. L. (2024). Sea blindness in grey zone preparations. *Def. Stud. 24*(3), 399–420.

Mauá, D. D. and F. G. Cozman (2020). Thirty years of credal networks: Specification, algorithms and complexity. *Int. J. Appr. Reasoning 115*, 45–73.

Mukherjee, S. (2024, Nov). One of two damaged baltic sea cables back online, arelion says.

News, T. (2025, January). Taiwan seeks south korean help investigating chinese ship suspected of cutting undersea cable. accessed 2026-02-06.

News, Y. (2024, Dec). Maps reveal the path of the eagle s on christmas day. accessed 2026-02-06.

Ramírez Agudelo, O. H., C. Köpke, Y. Guillouet, J. Schäfer-Frey, E. Engler, J. Mielniczek, and F. Sill Torres (2021). Expert-driven probabilistic assessment of safety and security of offshore wind farms. *Energies 14*(17), 5465.

Renooij, S. and L. C. van der Gaag (2002). From qualitative to quantitative probabilistic networks. In A. Darwiche and N. Friedman (Eds.), *Un. in AI*, pp. 422–429.

Selin, H. and N. E. Selin (2023). The human–technical–environmental systems framework for sustainability analysis. *Sus. Science 18*, 791–808.

Sill Torres, F., N. Kulev, B. Skobiej, M. Meyer,

O. Eichhorn, and J. Schäfer-Frey (2020). Indicator-based safety and security assessment of offshore wind farms. In *Resilience Week*, pp. 26–33.

Sytas, A. and J. Ahlander (2025). Sweden opens sabotage probe into baltic undersea cable damage. accessed 2026-02-06.

Tecklenburg, B., A. Gabriel, and F. Sill Torres (2022). A scenario based threat assessment using bayesian networks for a high voltage direct current converter platform. In *ESREL*.

Walley, P. (1996). Measures of uncertainty in expert systems. *AI 83*, 1–58.

Weber, P., O. Medina-Oliva, C. Simon, and B. Iung (2012). Overview on bayesian networks applications for dependability, risk analysis and maintenance areas. *Eng. Appl. of AI 25*(4), 671–682.

Zinke, R., J. Melnychuk, F. Köhler, and U. Krause (2020). Quantitative risk assessment of emissions from external floating roof tanks during normal operation and in case of damages using bayesian networks. *RESS 197*, 106826.

Appendix A

This appendix presents the *credal sets* $\mathcal{K}$ determined for the use case in Section 4. Since all variables are binary with state space $\{0, 1\}$, each *credal set* is given as a vector of probability intervals $\left[\underline{P}(X = 1), \overline{P}(X = 1)\right]$, listed in lexicographic order of the parent configurations. Furthermore, the experts uncertainty u is added.

IncidentType (parents: Human, Environment, Technology): $\mathcal{K}$ = ([0,0]; [0.795,0.684]; [0.150,0.130]; [0.666,0.574]; [0.312,0.268]; [0.968,0.833]; [0.473,0.407]; [0.860,0.740]), $u = 0.15$

Human (parents: AffectedActors, OtherActors): $\mathcal{K}$ = ([0, 0]; [0.872, 0.768]; [0.872, 0.768]; [1.000, 0.937]), $u = 0.13$

Environment (parents: WeatherConditions, NaturalAnomalies): $\mathcal{K}$ = ([0, 0]; [0.787, 0.693]; [0.850, 0.750]; [1.000, 0.937]), $u = 0.13$

Technology (parents: SecondaryDamages, TechnicalAnomalies): $\mathcal{K}$ = ([0, 0]; [0.881, 0.758]; [0.538, 0.463]; [1.000, 0.925]), $u = 0.15$

AffectedActors (parents: NoResponseToRadio, AISoff, AbnormalMovement): $\mathcal{K}$ = ([0, 0]; [0.425, 0.375]; [0.595, 0.525]; [0.904, 0.796]; [0.553, 0.487]; [0.914, 0.806]; [0.872, 0.768]; [1.000, 0.937]), $u = 0.13$

OtherActors (parents: UnidentifiedActorsNearby, NonOfficialsNearby, PastIncidents, CriticalStates): $\mathcal{K}$ = ([0, 0]; [0.544, 0.456]; [0.337, 0.283]; [0.892, 0.748]; [0.544, 0.456]; [0.849, 0.711]; [0.751, 0.629]; [0.925, 0.775]; [0.609, 0.511]; [0.740, 0.620]; [0.870, 0.730]; [0.925, 0.775]; [0.849, 0.711]; [0.925, 0.775]; [0.925, 0.775]; [1.000, 0.912]), $u = 0.18$

WeatherConditions (parents: HighWaves, HighWind, ExtremeWeather): $\mathcal{K}$ = ([0, 0]; [0.675, 0.565]; [0.609, 0.511]; [0.870, 0.730]; [0.892, 0.748]; [0.892, 0.748]; [0.892, 0.748]; [1.000, 0.912]), $u = 0.18$

NaturalAnomalies (parents: ExtremeWeather, NaturalDisaster, UndisclosedDepths): $\mathcal{K}$ = ([0, 0]; [0.825, 0.675]; [0.781, 0.639]; [0.935, 0.765]; [0.759, 0.621]; [0.935, 0.765]; [0.935, 0.765]; [1.000, 0.900]), $u = 0.2$

SecondaryDamages (parents: NearbyInfrastructure, InfrastructureDestroyed): $\mathcal{K}$ = ([0, 0]; [0.409, 0.352]; [0.914, 0.786]; [1.000, 0.888]), $u = 0.15$

TechnicalAnomalies (parents: RadioDisfunction, SystemIntegrityFailure): $\mathcal{K}$ = ([0,0]; [0.473, 0.407]; [0.666, 0.574]; [1.000, 0.888]), $u = 0.13$

Appendix B

This appendix presents the extracted evidence for each of the 4 scenarios:

The variables are ordered as follows: E_1 = AISoff, E_2 = NoResponseToRadio, E_3 = AbnormalMovement, E_4 = UnidentifiedActorsNearby, E_5 = NonOfficialsNearby, E_6 = PastIncidents, E_7 = CriticalStates, E_8 = HighWaves, E_9 = HighWind, E_{10} = ExtremeWeather, E_{11} = NaturalDisaster, E_{12} = UndisclosedDepths, E_{13} = NearbyInfrastructure, E_{14} = InfrastructureDestroyed, E_{15} = RadioDisfunction, E_{16} = SystemIntegrityFailure.

Each scenario is encoded as a vector $(E_1, \ldots, E_{16})$ according to the defined variable order. The value 0.5 denotes *no hard evidence*.

Scenario 1: (1, 0.5, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0.5).

Scenario 2: (0, 0.5, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0.5).

Scenario 3: (0.5, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0.5).

Scenario 4: (1, 0.5, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0.5)