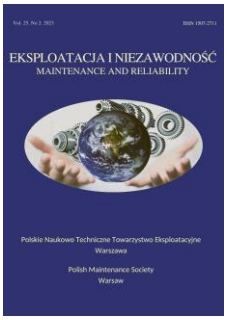

Eksploatacja i Niezawodnosc – Maintenance and Reliability
Volume 28 (2026), Issue 3
journal homepage: http://www.ein.org.pl

Article citation info:
Wang S, Zhou X-D, Song H-Y, Xu Y-L, Cui L, DBN-MC approach for electronic safety & arming device PSA under CCF and epistemic uncertainty, Eksploatacja i Niezawodnosc – Maintenance and Reliability 2026: 28(3) http://doi.org/10.17531/ein/218674

DBN-MC approach for electronic safety & arming device PSA under CCF and epistemic uncertainty

Indexed by: Web of Science Group

Shuo Wang[a], XiaoDong Zhou[a,*], HongYang Song[a], YanLi Xu[a], Liang Cui[a]

[a] National Demonstration Center of Experimental Teaching for Ammunition Support and Safety Evaluation Education, Army Engineering University of PLA, China

Highlights

- Proposes a DBN–MC PSA framework for ESADs under multi-source CCF and epistemic uncertainty.
- Propagates epistemic uncertainty in CCF parameters via outer-loop Monte Carlo sampling.
- Produces time-dependent unintended-arming probability trajectories with percentile uncertainty bands.
- Computes intervention-based importance measures using RAW and normalized RRW.
- Quantifies robustness of importance rankings across epistemic scenarios.

Abstract

Electronic safety and arming devices (ESADs) require extremely low unintended-arming probabilities, making success-run demonstration testing impractical. This paper proposes a DBN–MC dynamic PSA framework that encodes sequential enabling constraints and multi-source common-cause failures (CCFs) via local CPTs, and propagates epistemic uncertainty in data-scarce CCF parameters through outer-loop Monte Carlo sampling. In a case study, the mission-end unintended-arming probability is 1.896×10^{-7} with a 90% uncertainty interval of $[5.421\times10^{-9}, 6.948\times10^{-7}]$, providing time-dependent risk trajectories with percentile uncertainty band. Decision support is further enabled by intervention-based importance measures—RAW for worst-case amplification and normalized RRW for improvement potential—and by robustness diagnostics that summarize ranking variability across epistemic scenarios. The results show CCF mechanisms dominate worst-case amplification, while improvement priorities are distributed and scenario dependent, supporting uncertainty-informed ESAD design screening and prioritization.

Keywords
Monte Carlo, electronic safety and arming device, dynamic Bayesian network, probabilistic safety assessment, common-cause failure, epistemic uncertainty

1. Introduction

Electronic safety and arming devices (ESADs) must satisfy extremely stringent safety requirements. GJB 373B-2019 requires the probability of unintended arming before the initiation of the arming process to be below 1×10^{-6}, making ESADs typical high-reliability systems. Using traditional pass–fail testing, meeting this target would require approximately 2.3×10^{6} samples under 90% confidence with zero failures according to the success-run theorem [1], which is often infeasible in practice.

Probabilistic safety assessment (PSA) provides a feasible alternative for quantifying safety and supporting design decisions [2–4]. Classical PSA methods such as fault tree analysis (FTA) and event tree analysis (ETA) are widely used [5,6] and ESAD safety is often evaluated by FTA following the "Fuze Typical Fault Tree Manual" [7]. However, ESAD failure processes are inherently time-dependent and governed by

(*) Corresponding author.
E-mail addresses: S. Wang (ORCID: 0009-0008-3749-0716) 1392780361@qq.com, X-D. Zhou (ORCID: 0009-0008-6912-7700) fadsjkl@163.com, H-Y. Song (ORCID: 0009-0008-7675-3363) glock_17@163.com, Y-L. Xu (ORCID: 0000-0002-0843-2962) jessiexyl@163.com, L. Cui (ORCID: 0009-0002-0338-7944) 543353754@qq.com

sequential arming logic, which is difficult to capture with purely static models [8]. Markov chain models have therefore been adopted to evaluate dynamic schemes and compare logic designs [9–11]. Yet, Markov formulations can become cumbersome to construct and maintain due to global state enumeration when dependency structures and correlated failure mechanisms are introduced.

Common-cause failures (CCFs) are particularly important for modern ESADs, yet they are not consistently treated in existing ESAD-oriented PSA studies. Empirical studies report that CCFs contribute more than 30% of failures in critical avionics systems [12]. For ESADs, which increasingly adopt fully electronic architectures, CCF mechanisms may significantly affect redundant safety components. Existing ESAD-oriented PSA studies often consider simplified CCF settings and show that risk can increase markedly once CCFs are included [13,14]. These observations underscore the need for ESAD PSA models that can incorporate CCF mechanisms in a structured and extendable manner.

The challenge is compounded by data scarcity. While independent failure probabilities can often be obtained from standards such as GJB-299C, key CCF parameters (e.g., the β-factor) frequently lack empirical support and are therefore specified as fixed values or ranges based on expert judgment [8,15] or obtained via scoring methods such as those in IEC-61508 [16], inevitably introducing epistemic uncertainty due to subjectivity in parameter selection [17]. More broadly, recent studies have emphasized uncertainty-aware, data-efficient reliability analysis under limited degradation information. For example, He et al. [18] integrate a physics-informed neural network with a Wiener-process-based degradation model to improve degradation modeling and reliability prediction under sparse data, while Wang et al. [19] employ neural-network-supported monotonic stochastic processes to quantify and propagate multiple sources of uncertainty in reliability assessment. However, ESAD probabilistic safety assessment is system-oriented and rare-event driven: safety depends not only on individual component behavior but also on cross-channel interactions, component–environment and human–system interactions (e.g., mis-operation), external disturbances, and other low-probability stochastic events, for which representative degradation datasets are often unavailable. Inspired by these uncertainty-aware efforts, our DBN–MC framework propagates epistemic uncertainty in CCF parameters through DBN inference into risk metrics and importance measures, thereby supporting decision-making for ESAD-type time-ordered redundant systems.

Bayesian networks (BNs) provide a causal graphical representation with conditional probability tables (CPTs) for uncertainty modeling [20,21]. Since Bobbio et al. proposed mapping fault trees into BNs [22], BN-based reliability modeling has attracted increasing attention [23,24]. However, BNs are static. Dynamic Bayesian networks (DBNs) extend BNs by explicitly modeling temporal dependence between time slices, making them suitable for PSA settings where sequential enabling constraints and dependent mechanisms must be represented [25–27], a practical remaining challenge is to integrate epistemic uncertainty in data-scarce CCF parameters into dynamic inference in a tractable and decision-relevant manner.

To address data scarcity in CCF parameters and the resulting epistemic uncertainty, we develop a DBN–MC framework that propagates epistemic uncertainty through dynamic inference. The framework outputs time-dependent unintended-arming probability trajectories with percentile uncertainty bands. For decision support, we compute intervention-based importance indices (RAW and normalized RRW). Importantly, we further evaluate whether the resulting importance priorities are stable under epistemic uncertainty by summarizing ranking robustness across epistemic scenarios using rank-frequency and normalized entropy.

To differentiate this study from recent and representative DBN/DTBN/CTBN-based dynamic PSA and reliability approaches that explicitly incorporate CCF modeling. For clarity, Table 1 compares representative studies along four dimensions: (i) CCF representation, (ii) handling of epistemic uncertainty (point / bounds-only / propagated), (iii) state-space handling, and (iv) importance analysis (measures and ranking-robustness assessment). Abbreviations used in Table 1 include: dynamic Bayesian network (DBN); discrete-time Bayesian network (DTBN); continuous-time Bayesian network (CTBN); continuous-time dynamic Bayesian network (CTDBN); common-cause failure (CCF); conditional probability table (CPT); phased-mission system (PMS); dynamic fault tree

(DFT); best–worst method (BWM); hesitant fuzzy set (HFS); efficient decomposition and aggregation (EDA); and Fussell–Vesely (FV).

As summarized in Table 1, recent DBN/DTBN/CTBN-based dynamic PSA/reliability studies that incorporate CCFs predominantly adopt point CCF parameters or provide bounds-only risk results (e.g., via interval assumptions or conservative endpoint selection), rather than propagating epistemic uncertainty through the dynamic model to obtain time-dependent risk distributions (e.g., percentile bands). Moreover, when importance analysis is reported, it is typically computed at a single nominal parameterization (i.e., point importance), and importance-ranking robustness under epistemic uncertainty is not assessed.

In contrast, our incremental contribution is a decision-oriented uncertainty-to-importance workflow: we propagate epistemic uncertainty through the DBN to generate time-dependent risk trajectories with percentile bands, compute intervention-based RAW and normalized RRW under each epistemic scenario, and then quantify ranking robustness using rank-frequency and normalized entropy. This enables preliminary-design screening that distinguishes robust priorities that persist across epistemic scenarios from scenario-dependent priorities driven by epistemic assumptions, thereby improving the interpretability of importance-based recommendations under data scarcity.

Table 1. Comparison of recent DBN/DTBN/CTBN-based dynamic PSA/reliability studies incorporating CCFs: epistemic-uncertainty handling, state-space handling, and importance analysis (measures and ranking robustness).

Refs.	CCF representation	Epistemic-uncertainty handling	State-space handling	Importance analysis (measures; ranking robustness)
[28]	Explicit CCF mode/states in DTBN (independent vs. CCF).	Point (fixed parameters)	Standard DTBN state space (no reduction)	Not reported; Robustness: N/A
[29]	β-factor in CTBN CPT; step/impulse functions	Bounds-only (uses upper endpoint; not propagation)	Standard CTBN state space (no reduction)	Measures: Birnbaum; Robustness: No
[30]	β-factor in CTBN CPT; DFT→CTBN	Bounds-only (BWM+HFS for β; interval theory yields risk bounds)	Structured CTBN from DFT; no reduction	Not reported; Robustness: N/A
[31]	CCF in PMS-DTBN (added events/nodes)	Not emphasized (focus on efficiency; not explicit epistemic propagation)	EDA decomposition/aggregation reduces DTBN size	Not reported; Robustness: N/A
[32]	β-factor in CTDBN; step/impulse	Point (fixed parameters)	Standard CTDBN state space (no reduction)	Measures: Prob. importance; FV; RRW; differential (point); Robustness: No
[33]	Explicit CCF states in DTBN	Bounds-only (interval analysis yields risk bounds)	Standard DTBN state space (no reduction)	Not reported; Robustness: N/A
[34]	Explicit CCF states in DBN (imperfect coverage)	Bounds-only (sensitivity/ interval assumptions yield bounds at a time point)	Standard DBN state space (no reduction)	Measures: qualitative sensitivity only (no quantitative importance); Robustness: No
[35]	GO-FLOW→DTBN with CCF	Point (fixed parameters)	Standard DTBN state space (no reduction)	Measures: contribution share to total unreliability (point); Robustness: No
[36]	Explicit CCF process/states in DBN redundancy	Point (fixed parameters)	Standard DBN state space (no reduction)	Not reported; Robustness: N/A
This work	Explicit CCF mechanism nodes in DBN	Propagated (outer-loop MC on epistemic factors; dynamic risk percentiles)	Exact forward propagation (no reduction)	Measures: RAW + normalized RRW (per epistemic scenario); Robustness: Yes (rank-frequency + normalized

2. System description and problem definition

2.1. System overview and safety objective

An ESAD with three sequentially armed safety components is considered. The modeling assumptions are as follows:

(1) Absorbing-state assumption: Each Safety component is modeled as a two-state variable, Unarmed and Armed. Once a component transitions to Armed, it remains in that state for the remainder of the mission horizon.

(2) Preliminary-design (a priori) assessment assumption: The model targets the preliminary design phase, where operational evidence is limited. Model parameters therefore reflect design-time knowledge. The analysis is intended for a priori risk screening and design prioritization, rather than post-deployment statistical estimation.

(3) CCF mechanism assumption: Dependencies among safety components are represented using CCF mechanism nodes that capture latent common-cause triggers capable of simultaneously affecting multiple safety components within a time step. Given the preliminary-design context, a conservative forcing semantics is adopted: if a relevant CCF mechanism occurs at time *t*, the affected safety components are forced into the Armed state within the same time step. Each CCF mechanism is also treated as absorbing over the mission horizon.

ESAD unintended-arming failure is synonymous with unintended arming defined as the simultaneous armed state of Safety 1-Safety 3:

$$F(t) \triangleq \{S_1(t) = \text{Armed}, S_2(t) = \text{Armed}, S_3(t) = \text{Armed}\} \quad (1)$$

The ESAD unintended-arming failure probability at time *t* is:

$$P_F(t) \triangleq P\big(F(t)\big) \quad (2)$$

The schematic of the ESAD is shown in Figure 1.

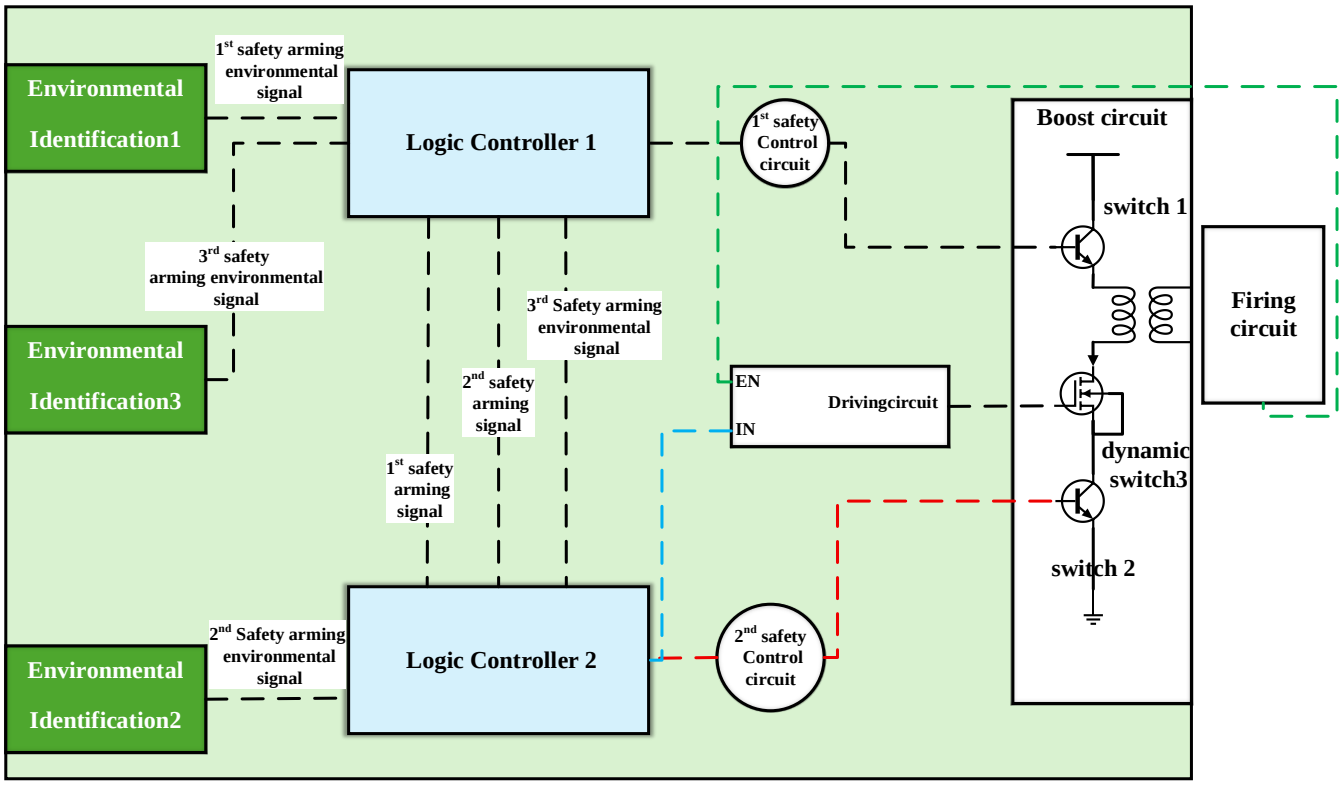

Figure 1. Schematic of the ESAD.

Level 1: Environmental Identification 1 detects a predefined signal and transmits it to Logic Controller 1. Upon validation, Logic Controller 1 commands Switch 1 to close.

Level 2: After confirming the Safety 1 has been armed and then receiving a signal from Environmental Identification 2, Logic Controller 2 outputs a control signal to arm the Safety 2, thereby forming a closed source–drain loop for the dynamic energy switch.

Level 3: This stage requires confirmation of preceding states and collaborative evaluation of a third environmental signal. Logic Controller 2 generates alternating control signals that interact with feedback voltages, driving periodic operation of the dynamic switch and ultimately placing the system in standby mode.

2.2. Sequential logic and dynamic feedback

The intended arming logic of the ESAD is sequential. A downstream Safety component is allowed to arm only after the required upstream component has already entered the Armed state. In this study, unintended arming is driven by independent component mechanisms and by CCF mechanisms.

When no CCF occurs, the enabling condition directly governs the Unarmed-to-Armed transition. Safety 2 is permitted to transition from Unarmed to Armed only if Safety 1 is Armed. Safety 3 is permitted to transition from Unarmed to Armed only if Safety 2 is Armed. If the enabling condition is not satisfied, the downstream component cannot arm in that time step and remains Unarmed. If the enabling condition is satisfied, the downstream component may arm according to its independent per-step probability.

This sequential dependence creates dynamic feedback. The inferred probability that an upstream component is Armed changes over time, and this changing belief continuously modulates the effective arming behavior of downstream components through the enabling rule.

2.3. Multi-source common cause failures and modeling needs

For ESADs, CCF risks stem from shared intrinsic factors, functional coupling, and common external stresses, which can lead to correlated, near-simultaneous unintended arming across multiple safety components.

Data supporting the associated CCF parameters are often scarce, and the underlying mechanisms are complex, making precise quantification difficult. As a result, epistemic uncertainty becomes a key driver of assessment uncertainty.

An uncertainty-informed PSA should therefore report not only a point estimate of failure probability, but also uncertainty ranges and the stability of importance rankings across plausible epistemic scenarios.

3. Theoretical foundation

3.1. DBN process model

A DBN represents the probabilistic evolution of system variables over time by extending a BN with temporal dependencies [37]. A DBN consists of an initial network defining the prior distribution at t=0 and a transition network defining state transitions between consecutive time slices under a first-order Markov assumption [38]:

$$P(X_t|X_{0:t\text{-}1}) = P(X_t|X_{t-1}) \tag{3}$$

Over the mission horizon, the joint distribution factorizes as

$$P(X_{0:T}) = P(X_0)\prod_{t=1}^{T} P(X_t|X_{t-1}) \tag{4}$$

This factorization is the basis for forward propagation: starting from $P(X_0)$, the model iteratively predicts the distribution at the next time step [39].

3.2. Node-level cpts and forward propagation

Each node $Y(t)$ is governed by a conditional probability table (CPT) given its parents:

$$P\big(Y(t)|Pa(Y(t))\big) \tag{5}$$

Forward propagation is performed by marginalizing over parent configurations:

$$P(Y(t)=y) = \sum_{\pi\in\Omega_{Pa(Y)}} P(Y(t)=y|\pi)\,P(\pi) \tag{6}$$

In the case study, parent sets are small and discrete, so exact enumeration of π provides stable and reproducible propagation.

3.3. Two-state absorbing components and enabling/forcing logic

Absorbing behavior for a two-state component is encoded directly in its CPT:

$$P(\mathrm{S}(t)=Armed|\mathrm{S}(t-1)=Armed,\cdot)=1 \tag{7}$$

When a component is Unarmed at t-1, it can transition to Armed at t through its independent mechanism when enabling conditions are satisfied and no forcing mechanism applies:

$$\begin{aligned} &P(\mathrm{S}(t)=Armed)\big|\mathrm{S}(t-1)\\ &\quad =Unarmed,\ enabled,\ no\ forcing=q \end{aligned} \tag{8}$$

CCF "forcing" is implemented by assigning probability 1 to Armed when the relevant CCF is in Occurred state in that step.

3.4. Epistemic uncertainty propagation by Monte Carlo

Epistemic uncertainty in data-scarce parameters is represented by a multiplicative factor:

$$q = q_0 U \tag{9}$$

Each Monte Carlo draw defines an epistemic scenario $s \in \{1,\ldots,S\}$. An epistemic scenario corresponds to one joint instantiation of all epistemically uncertain parameters. For scenario s, parameters are instantiated as:

$$q^{(s)} = q_0 U^{(s)} \tag{10}$$

The DBN is propagated under each scenario to obtain $P_F^{(s)}(t)$. The mean trajectory is estimated by:

$$E[P_F(t)] \approx \frac{1}{S}\sum_{s=1}^{S} P_F{}^{(s)}(t) \tag{11}$$

and uncertainty intervals are obtained from empirical quantiles across scenarios.

3.5. Intervention-based importance measures

1) Risk achievement worth

The RAW indicator aims to quantify the contribution of a specific failure event to the overall risk of the system. Its essence is to measure the intensity of the negative impact on system reliability when the event transitions from a state of certain probability of occurrence to a state of absolute occurrence. Its mathematical expression is:

$$RAW_i = \frac{P_F(T;q_i \leftarrow 1)}{P_F(T;q_i \leftarrow q_i{}^0)} \tag{12}$$

The larger the RAW value, the greater the "contribution" of the component failure to the system risk, indicating stronger conditional amplification of system failure probability under the imposed intervention [40].

2) Normalized risk reduction worth

Risk Reduction Worth is used to quantify the potential risk reduction when a basic event is perfectly improved (i.e., entirely prevented) under the adopted intervention [41]. In this work we use a normalized Risk Reduction Worth so that the metric directly represents the fractional reduction of the system failure probability and is bounded in [0,1], its mathematical expression is:

$$RRW_i = \frac{P_F(T;q_i \leftarrow q_i{}^0) - P_F(T;q_i \leftarrow 0)}{P_F(T;q_i \leftarrow q_i{}^0)} \tag{13}$$

A larger RRW value indicates that improving the reliability of the corresponding event yields a greater fractional reduction in system failure probability.

3.6. Ranking robustness under epistemic uncertainty

This paper achieves robustness analysis of importance ranking through the following systematic process: First, in the outer Monte Carlo loop, repeated sampling is conducted from the joint distribution of epistemic uncertainty parameters, with each sample yielding a complete set of parameter realization values $\theta(s)$. These parameter samples represent the possible values of parameters under different scenarios.

Next, for each parameter sample $\theta(s)$, the inner DBN dynamic inference process is executed to calculate the RAW and RRW values of each failure event in that scenario. Based on the magnitude of the importance values, a ranking sequence of failure events for the current scenario is generated.

$$RANK^{(s)} = [rank_1^{(s)},\ rank_2^{(s)},\ \ldots,\ rank_N^{(s)}] \tag{14}$$

After completing all S sampling iterations, a sample set of rankings is obtained. By statistically analyzing the frequency of each failure event appearing in different ranks, a probability distribution matrix of the importance ranking is constructed.

$$P(rank_i = j) = \frac{1}{S}\sum_{s=1}^{S} I\left(rank_i^{(s)} = j\right) \tag{15}$$

Concentrated rank probabilities indicate robust prioritization; dispersed probabilities indicate scenario sensitivity.

To complement the rank-frequency matrices, we report a normalized Shannon entropy computed from each event's rank distribution. Let $p_{e,r}$ denote the empirical probability that event e attains rank r across epistemic scenarios, and let n be the number of basic events. The normalized entropy is:

$$H_e = -\frac{1}{log_2 n}\sum_{r=1}^{n} p_{e,r}\, log_2\, p_{e,r} \tag{16}$$

Where $H_e \in [0,1]$. Smaller H_e indicates a more concentrated ranking, whereas larger H_e indicates greater dispersion.

4. Case study

4.1. DBN modeling

Based on the system description in Section II, a DBN model is constructed. The mission time is 500 h, discretized with Δt = 10 h (T = 50 steps). The initial condition sets S_1–S_3 to *Unarmed* and all CCF mechanisms to *Not Occurred* at t=0, consistent with $P(X_0)$ in (4). Since this study targets the preliminary design stage, CCFs are introduced as mechanism variables for a priori risk screening, rather than component-level failure modes inferred from field data. Each CCF node represents a class of latent common-cause triggers used for a priori risk screening and design prioritization rather than event attribution from field

data that can simultaneously affect multiple safety channels including CCF_{123}, CCF_{23}, CCF_{12} and CCF_{13}. The instantiated network topology used in the case study is shown in Figure 2.

CCF_{123} affects S_1, S_2, and S_3;

CCF_{12}: affects S_1 and S_2;

CCF_{13}: affects S_1 and S_3;

CCF_{23}: affects S_2 and S_3.

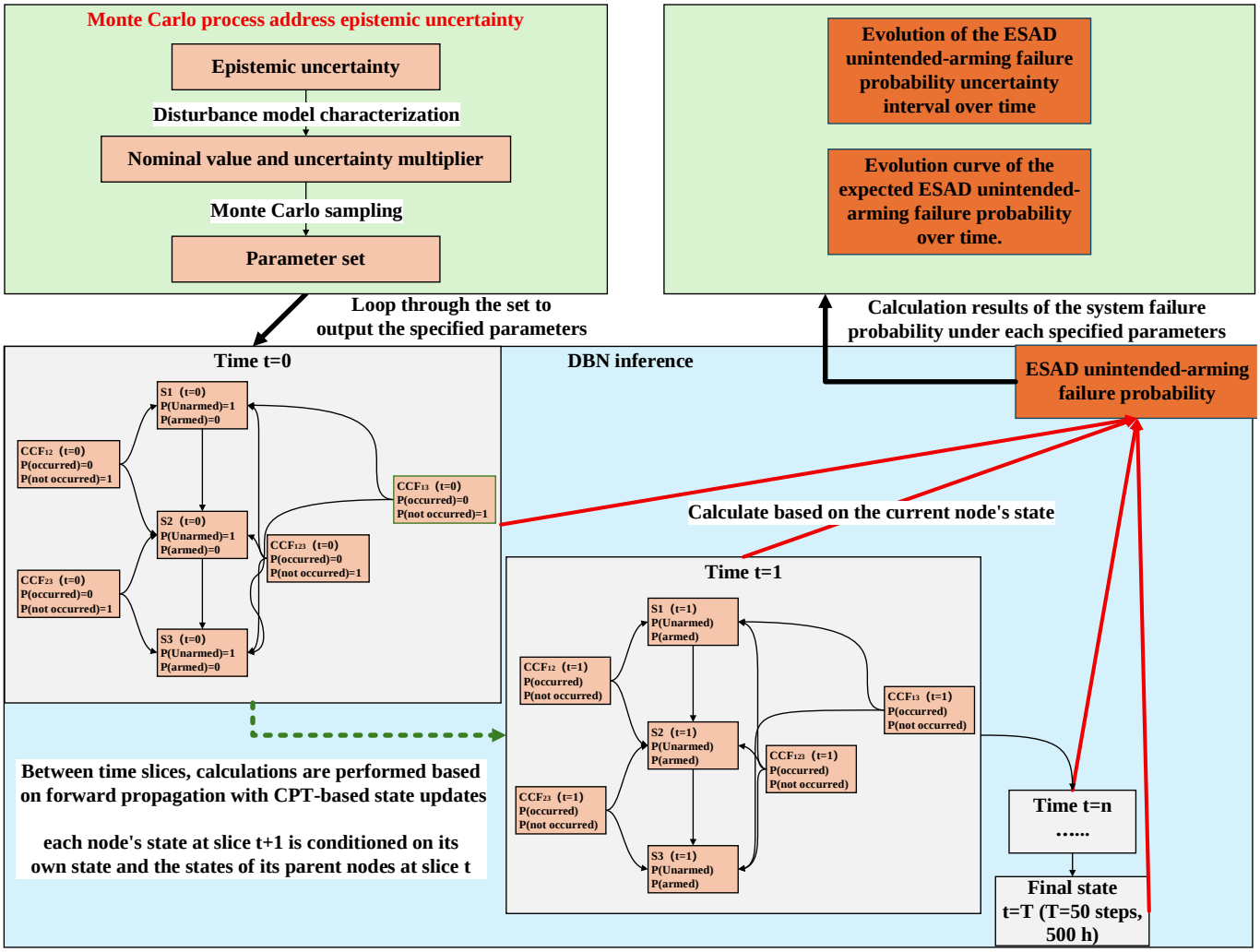

Figure 2. Schematic diagram of the systematic inference process and topological structure.

Persistence is encoded through inter-slice arcs, whereas forcing/enabling is encoded by selecting appropriate parent sets in the CPTs. These CPTs are constructed directly from the DBN construction framework:

Absorbing Safety dynamics and absorbing CCF dynamics are encoded by (7).

Sequential enabling is implemented by conditioning the independent transition of $S_2(t)$ on $S_1(t)$ and of $S_3(t)$ on $S_2(t)$, consistent with the "enabled" condition in (8).

CCF forcing is implemented by setting the conditional arming probability of a Safety component to 1 whenever any affecting CCF is Occurred at the current step. This construction ensures that the model is evaluated by repeated application of the DBN propagation rules in (3)-(6).

Since this is an a priori assessment in preliminary design, CCF parameters represent design knowledge (standards/ analogy/ expert judgment) rather than data-driven estimates; epistemic uncertainty is therefore explicitly modeled to quantify decision-relevant bounds.

For the independent failure probability parameters of the components, the calculation logic references literature [13], with values primarily based on authoritative standards. Specifically, the baseline independent failure probability for components S_1, S_2, and S_3 are derived from the reliability data of components provided by GJB-299C, which is based on extensive testing and field statistical results, thus possessing

high credibility. Given the low epistemic uncertainty of these foundational failure probability data, they are set as fixed values in the model.

Table 2. Common cause failure factor table for logical subsystems, sensors, or final elements (1oo2 system).

Engineering judgment score	β	
	Logical subsystems	sensors, final elements
≥120	0.5%	1%
70-120	1%	2%
45-75	2%	5%
＜45	5%	10%

Table 3. Common cause failure factor table for logical subsystems, sensors, or final elements (MooN system).

MooN		N			
		2	3	4	5
M	1	β	0.5β	0.3β	0.2β
	2	-	1.5β	0.6β	0.4β
	3	-	-	1.75β	0.8β

Epistemic uncertainty is introduced only for the CCF parameters through the multiplicative model in (9)-(10), i.e., $q_{ccf,r} = q_{ccf,r,0}U_r$. This choice reflects the preliminary-design setting considered here, where available evidence is typically limited to order-of-magnitude guidance and does not support identifying a unique, highly structured prior shape. IEC 61508 β-factor tables already imply substantial dispersion: for 1oo2 architectures β ranges from 0.5% to 10%, and for MooN systems βis further scaled by coefficients from 0.2 to 1.75. When such subsystem-level guidance is mapped to a per-step, mechanism-level occurrence probability in a discretized DBN—where the result depends on architectural interpretation, cause grouping, and the discretization interval Δt; therefore, additional variability is plausible. We therefore assign log-uniform multipliers $U_r \in [10^{-2}, 10^{2}]$, which encodes order-of-magnitude uncertainty without favoring any particular magnitude a priori. To maintain physical plausibility and decision relevance at the chosen time-step granularity, we impose plausibility constraints on each per-step CCF probability. Specifically, we apply two sanity bounds: each q_{ccfr} is kept below the smallest independent per-step arming probability of the affected safety component, and for each affected pair q_{ccfr} is kept no smaller than the product of the two corresponding independent per-step probabilities, so that CCF effects remain physically plausible and non-negligible at the chosen time step. Section V further evaluates sensitivity to the prior family (log-uniform vs. truncated log-normal) and to admissible-range contraction. The adopted nominal parameters and uncertainty settings are summarized in Table 4 and 5. System nodes and their dependencies are listed in Table 6. The CPTs for each node are presented in Table 7–10.

Table 4. Per-step parameters (Δt=10h).

Parameter	Value
q_{S1}	2.7×10^{-5}
q_{S2}	3.316×10^{-5}
q_{S3}	3.012×10^{-5}
$q_{ccf123,0}$	2.0×10^{-10}
$q_{ccf12,0}$	5.0×10^{-8}
$q_{ccf13,0}$	5.0×10^{-8}
$q_{ccf23,0}$	5.0×10^{-8}

Table 5. Parameter uncertainty settings.

Parameter	Distribution	Range
U_{123}	Log-uniform	$[10^{-2}, 10^{2}]$
U_{12}	Log-uniform	$[10^{-2}, 10^{2}]$
U_{23}	Log-uniform	$[10^{-2}, 10^{2}]$
U_{13}	Log-uniform	$[10^{-2}, 10^{2}]$

Table 6. System nodes and their dependencies.

Node Code	Parent Node	State Space
$S_1(t)$	$S_1(t\text{-}1)$ $CCF_{123}(t)$, $CCF_{12}(t)$, $CCF_{13}(t)$	['*Unarmed*', '*Armed*']
$S_2(t)$	$S_2(t\text{-}1)$, $S_1(t)$, $CCF_{123}(t)$, $CCF_{12}(t)$, $CCF_{23}(t)$	['*Unarmed*', '*Armed*']
$S_3(t)$	$S_3(t\text{-}1)$, $S_2(t)$, $CCF_{123}(t)$, $CCF_{13}(t)$, $CCF_{23}(t)$	['Unarmed', '*Armed*']
$CCF_{123}(t)$	$CCF_{123}(t\text{-}1)$	['*Not Occurred*', '*Occurred*']
$CCF_{12}(t)$	$CCF_{12}(t\text{-}1)$	['*Not Occurred*', '*Occurred*']
$CCF_{13}(t)$	$CCF_{13}(t\text{-}1)$	['Not Occurred', '*Occurred*']
$CCF_{23}(t)$	$CCF_{23}(t\text{-}1)$	['*Not Occurred*', '*Occurred*']

Table 7. Conditional probability table for node S_1.

$S_1(t\text{-}1)$	$CCF_{123}(t)$	$CCF_{12}(t)$	$CCF_{13}(t)$	$P(S_1(t) = Armed)$	$P(S_1(t) = Unarmed)$
-	Occurred	-	-	1.0	0.0
-	-	Occurred	-	1.0	0.0
-	-	-	Occurred	1.0	0.0
Armed	Not Occurred	Not Occurred	Not Occurred	1.0	0.0
Unarmed	Not Occurred	Not Occurred	Not Occurred	q_{S1}	1-q_{S1}

Table 8. Conditional probability table for node S_2.

$S_2(t\text{-}1)$	$S_1(t)$	$CCF_{123}(t)$	$CCF_{12}(t)$	$CCF_{23}(t)$	$P(S_2(t) = Armed)$	$P(S_2(t) = Unarmed)$
-	-	Occurred	-	-	1.0	0.0
-	-	-	Occurred	-	1.0	0.0
-	-	-	-	Occurred	1.0	0.0
Armed	*Armed*	Not Occurred	Not Occurred	Not Occurred	1.0	0.0
Unarmed	*Armed*	Not Occurred	Not Occurred	Not Occurred	q_{S2}	$1\text{-}q_{S2}$
Armed	*Unarmed*	Not Occurred	Not Occurred	Not Occurred	1.0	0.0
Unarmed	*Unarmed*	Not Occurred	Not Occurred	Not Occurred	0.0	1.0

Table 9. Conditional probability table for node S_3.

$S_3(t\text{-}1)$	$S_2(t)$	$CCF_{123}(t)$	$CCF_{13}(t)$	$CCF_{23}(t)$	$P(S_3(t) = Armed)$	$P(S_3(t) = Unarmed)$
-	-	Occurred	-	-	1.0	0.0
-	-	-	Occurred	-	1.0	0.0
-	-	-	-	Occurred	1.0	0.0
Armed	*Armed*	Not Occurred	Not Occurred	Not Occurred	1.0	0.0
Unarmed	*Armed*	Not Occurred	Not Occurred	Not Occurred	q_{S3}	$1\text{-}q_{S3}$
Armed	*Unarmed*	Not Occurred	Not Occurred	Not Occurred	1.0	0.0
Unarmed	*Unarmed*	Not Occurred	Not Occurred	Not Occurred	0.0	1.0

Table 10. Conditional probability table for node CCF_{123}/CCF_{12}/ CCF_{23}/ CCF_{13}.

CCF Type	$CCF(t\text{-}1)$	$P(CCF(t) = Occurred)$	$P(CCF(t) = Not\ Occurred)$
CCF_{123}	Not Occurred	q_{ccf123}	$1\text{-}q_{ccf123}$
	Occurred	1.0	0.0
CCF_{12}	Not Occurred	q_{ccf12}	$1\text{-}q_{ccf12}$
	Occurred	1.0	0.0
CCF_{13}	Not Occurred	q_{ccf13}	$1\text{-}q_{ccf13}$
	Occurred	1.0	0.0
CCF_{23}	Not Occurred	q_{ccf23}	$1\text{-}q_{ccf23}$
	Occurred	1.0	0.0

4.2. Failure probability computation workflow

For each scenario s, uncertain parameters are instantiated by (10) and the DBN is propagated from t=1 to T using (4)-(6). At each time t, the failure event is evaluated by (1) and the failure probability by (2). The mean trajectory and uncertainty bands are computed using (11). The overall computation flow used in the case study is summarized in Figure 3.

4.3. Convergence analysis

Convergence of the ESAD unintended-arming failure probability $P_F(T)$ with respect to scenario count S is reported in Table 11. The results stabilize for S≥3000, and S=5000 is adopted in the subsequent analyses. The reported 90% uncertainty interval corresponds to the 5^{th}-95^{th} percentiles of $P_F(T)$ over the epistemic scenarios.

Table 11. Results of Different Sampling Counts.

Samples S	Mean $P_F(T)$	90% uncertainty interval
1000	1.921×10^{-7}	$[4.090\times10^{-9},6.989\times10^{-7}]$
1500	1.880×10^{-7}	$[4.213\times10^{-9},6.981\times10^{-7}]$
2000	1.865×10^{-7}	$[4.527\times10^{-9},6.445\times10^{-7}]$
3000	1.875×10^{-7}	$[5.171\times10^{-9},6.833\times10^{-7}]$
4000	1.872×10^{-7}	$[4.979\times10^{-9},6.946\times10^{-7}]$
5000	1.896×10^{-7}	$[5.421\times10^{-9},6.948\times10^{-7}]$

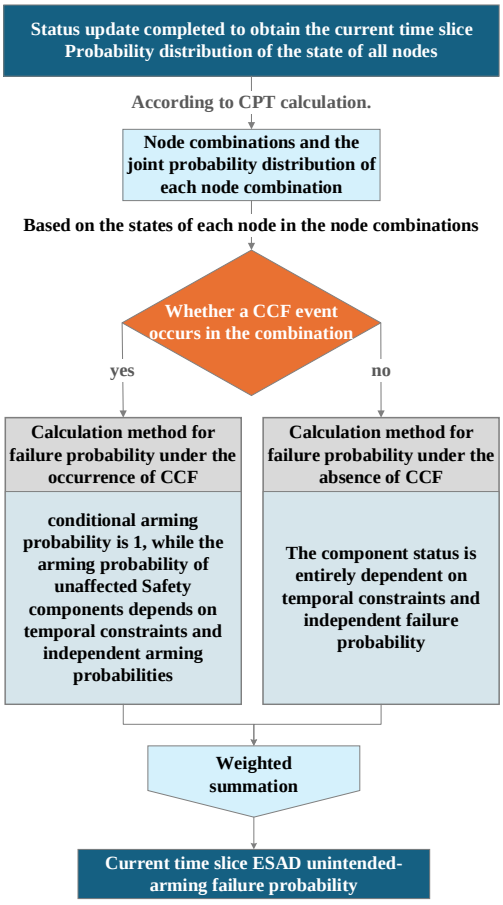

Figure 3. Schematic diagram of the ESAD unintended-arming failure probability calculation process.

4.4. ESAD unintended-arming failure probability and baseline comparison

To contextualize the proposed DBN–MC results, a deterministic baseline is obtained using FTA, which solves the top-event probability via minimal cut sets. For the deterministic FTA input, the expected value of the log-uniform multiplier U is used for CCF parameters:

$$E[U] = \frac{\text{b-a}}{ln(\frac{b}{a})},\ \text{a} = 10^{-2}, \text{b} = 10^{2},\ \text{yielding}\ E[U] \approx 10.857.$$

Accordingly, the deterministic CCF inputs are set as:

$q_{CCF_{r,det}} = E[U]q_{CCF_{r,0}}$ The DBN–MC results are reported in terms of the mean trajectory and percentile bounds over epistemic scenarios. The ESAD unintended-arming failure probability evolution over time calculated by DBN-MC method is shown in Figure 4 and the unintended-arming failure probability is summarized in Table 12.

To numerically verify the correctness of DBN forward propagation for the discretized model, an equivalent discrete-time Markov formulation was implemented under the same discretization Δt and mission length T. the Markov method represents the system as a discrete-time Markov chain with a finite state space. Let $\pi(t)$ denote the row vector of state probabilities at step t, and let P denote the one-step transition probability matrix. The propagation is:

$$\pi(t) = \pi(t-1)P, t = 1, \dots, T \tag{17}$$

Hence

$$\pi(T) = \pi(0)P^{T} \tag{18}$$

The ESAD unintended-arming failure probability is obtained by summing the probabilities of all states that satisfy the failure event definition $F(T)$ in (1):

$$P_F{}^{Markov}(T) = \sum_{x \in F} \pi_x(T) \tag{19}$$

where F is the set of failure states in which S_1, S_2, S_3 are all in the Armed state. The transition matrix P is constructed using the same per-step parameters and the same enabling/forcing rules as those encoded in the DBN CPTs, ensuring consistency between Markov and DBN formulations.

The resulting Markov failure-probability trajectory matches the DBN inference result (see Table 12) to within numerical error, with the maximum absolute discrepancy below 10^{-15}, providing a numerical cross-check of the DBN propagation implementation computed via (4)–(6). In addition, the DBN representation (as used in the proposed DBN–MC framework) provides a modular and maintainable modeling template: system dynamics are specified locally through parent sets and conditional probability tables (CPTs), which naturally encode sequential enabling logic and correlated mechanisms without explicitly constructing a global transition matrix. Consequently, extensions or logic/dependency changes can often be implemented by adding or revising a small number of nodes and local CPT entries, reducing re-modeling effort compared with rebuilding and validating a full-state transition matrix. Moreover, the Monte Carlo component enables straightforward uncertainty propagation via repeated sampling and DBN inference, while keeping the logical structure unchanged.

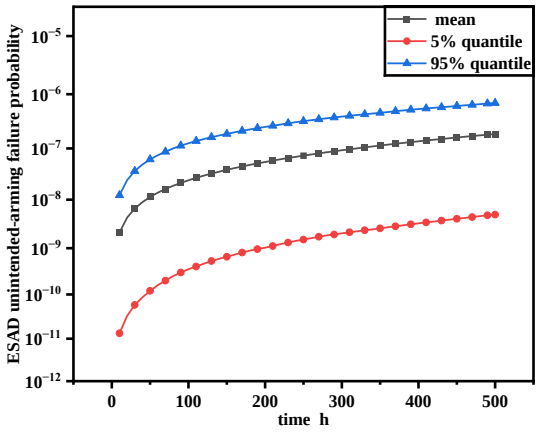

Figure 4. ESAD unintended-arming failure probability evolution over time calculated by DBN-MC method.

Table 12. Comparison of ESAD Unintended-Arming Failure Probability at t=500 h (T=50) by different Assessment Method.

Assessment Method	ESAD unintended-arming failure probability
FTA	2.322×10^{-7}
Markov	1.896×10^{-7}
DBN–MC mean	1.896×10^{-7}
DBN–MC 90% uncertainty interval	[5.421×10^{-9}, 6.948×10^{-7}]

The wide spread of the uncertainty interval indicates that epistemic uncertainty in the data-scarce CCF parameters dominates the width of the uncertainty bounds for the ESAD unintended-arming failure probability.

Although the case study considers an ESAD with three sequentially armed safety components, the proposed DBN–MC workflow generalizes directly to additional cascaded stages by appending stage nodes and specifying the corresponding local CPTs. Other configurations can be accommodated through localized updates to parent sets and mechanism nodes, while the

uncertainty-propagation procedure (Monte Carlo sampling + DBN inference) remains unchanged.

4.5. Importance analysis under epistemic uncertainty conditions

Importance measures were evaluated for all seven basic-event parameters q_{ccf123}, q_{ccf12}, q_{ccf13}, q_{ccf23}, q_{S1}, q_{S2}, q_{S3} using parameter-intervention ("clamping") analysis. Specifically, RAW and RRW were computed according to (12) and (13) , respectively, by re-evaluating the ESAD unintended-arming failure probability under the two interventions $q_i \leftarrow 1$ and $q_i \leftarrow 0$. The resulting distributions across Monte Carlo scenarios were summarized by the mean and the 5%/95% quantiles, as reported in Table 13.

A strong dominance of q_{ccf123} was observed in RAW. Its RAW mean was on the order of 10^7 far exceeding other events. A second tier was formed by the remaining CCFs affecting two safety channels parameters, while the independent safety arming parameters were substantially smaller. This hierarchy was consistent with the model structure encoded in the CPTs: under the RAW intervention $q_i \leftarrow 1$, the occurrence of the corresponding CCF mechanism was forced, and the affected safety components were driven to the Armed state with probability one through the forcing rules in the CPT specification tables. In contrast, independent arming events were constrained by sequential enabling constraints and therefore produced limited amplification even under forced-occurrence intervention. As a result, RAW acted primarily as a structural indicator of worst-case escalation pathways dominated by CCF forcing mechanisms.

RRW q_{ccf123} reflected a more distributed improvement potential. Although remained influential on average, multiple other parameters—including independent safety arming events—exhibited RRW means of comparable magnitude. The broad RRW percentile ranges in Table 13. indicated scenario dependence: in some epistemic realizations, eliminating a particular mechanism yielded limited benefit because the residual risk was dominated by other pathways; in other realizations, the same intervention produced substantial fractional reduction. Because RRW was defined using the "perfect improvement" intervention $q_i \leftarrow 0$ in (13), it was interpreted as an upper bound on achievable benefit. Practical design changes would typically reduce probabilities by finite factors rather than to 0, and the corresponding reductions in system risk would be smaller.

Table 13. DBN-MC importance calculation results table.

Parameter Name	RAW mean	RAW 5%	RAW 95%	RRW mean	RRW5%	RRW 95%
q_{S1}	2.276×10^{2}	5.634	7.21×10^{2}	2.542×10^{-1}	2.713×10^{-3}	8.920×10^{-1}
q_{S2}	2.667×10^{2}	4.292	1.109×10^{3}	2.119×10^{-1}	1.982×10^{-3}	9.163×10^{-1}
q_{S3}	2.745×10^{2}	5.254	1.136×10^{3}	1.972×10^{-1}	2.392×10^{-3}	8.547×10^{-1}
q_{ccf123}	4.614×10^{7}	1.306×10^{6}	2.088×10^{8}	3.832×10^{-1}	2.181×10^{-3}	9.691×10^{-1}
q_{ccf12}	6.982×10^{4}	2.075×10^{3}	3.145×10^{5}	1.761×10^{-1}	3.198×10^{-4}	8.354×10^{-1}
q_{ccf13}	7.683×10^{4}	2.285×10^{3}	3.468×10^{5}	1.897×10^{-1}	2.840×10^{-4}	8.986×10^{-1}
q_{ccf23}	6.269×10^{4}	1.863×10^{3}	2.828×10^{5}	2.320×10^{-1}	4.442×10^{-4}	8.876×10^{-1}

4.6. Robustness of importance rankings

Ranking robustness was quantified using (14). The ranking probability distributions of RAW and RRW were visualized as heatmaps in Figure 5. where the upper panel reports the probability that each event attains each rank across epistemic scenarios, and the lower panel reports the pairwise dominance confidence $P(A>B)$ computed across scenarios. Under the baseline epistemic setting (log-uniform multipliers on $X=\log_{10}(U_r)\in[-2,2]$. RAW rankings were found to be highly robust across epistemic scenarios. q_{ccf123} was ranked first in 100% of scenarios, and pairwise comparisons confirmed that q_{ccf123} exceeded every other event in RAW with probability 100%. The subsequent ranks were also stable: q_{ccf13} was ranked second in 97% of scenarios and q_{ccf12} was ranked third in 93.5% of scenarios, while q_{ccf23} was ranked fourth in 96.5% of scenarios. Independent safety arming events did not appear in ranks 1–4 and were confined to ranks 5–7. This concentration indicated that worst-case amplification, as measured by RAW, was dominated by the full-set CCF mechanism and that the ordering of leading CCF contributors was largely invariant to the sampled epistemic uncertainty. This observation is also

reflected in the low normalized Shannon entropy of the rank distribution for RAW data under the baseline uncertainty width, calculated using (16) shown in Table 13. This behavior reflects the fact that RAW is dominated by mechanism-level contrasts rather than by the specific epistemic multiplier, leading to highly concentrated rank distributions and near-zero entropy for some parameters. In contrast, RRW rankings were less robust, indicating that improvement potential was distributed and sensitive to which pathway dominated under each epistemic realization. q_{ccf123} attained rank 1 in 39% of scenarios but also appeared in lower ranks, indicating that in a substantial fraction of scenarios, perfecting q_{ccf123} was not the single most effective improvement action. Independent Safety events frequently appeared among the top ranks: q_{S1} ranked 1–2 in 41.5% of scenarios, q_{S2} ranked 1–2 in 28.5% of scenarios, and q_{S3} ranked 1–2 in 24% of scenarios. Pairwise dominance probabilities were consistent with this dispersion: the dominance of q_{ccf123} over q_{S2} and q_{S3} was near 60%, while dominance over q_{S1} was close to 52.5%, and non-negligible fractions of scenarios favored other parameters including q_{S1}, q_{S2}, and q_{ccf23}. The same conclusion is captured by the normalized Shannon entropy shown in table, which was substantially higher for RRW under the same baseline uncertainty width. Consequently, unlike RAW, RRW did not yield a universally dominant improvement target. The results indicated that improvement prioritization should be performed under uncertainty-informed criteria, rather than relying on a single deterministic ranking. Finally, because RRW is defined using a "perfect improvement" intervention, it should be interpreted as an upper bound on achievable benefit. Practical redesign actions would correspond to reducing probability by finite factors, which would yield smaller but more realistic gains; nevertheless, the RRW rankings and robustness analysis provide a principled basis for screening and prioritizing candidate improvement actions under epistemic uncertainty.

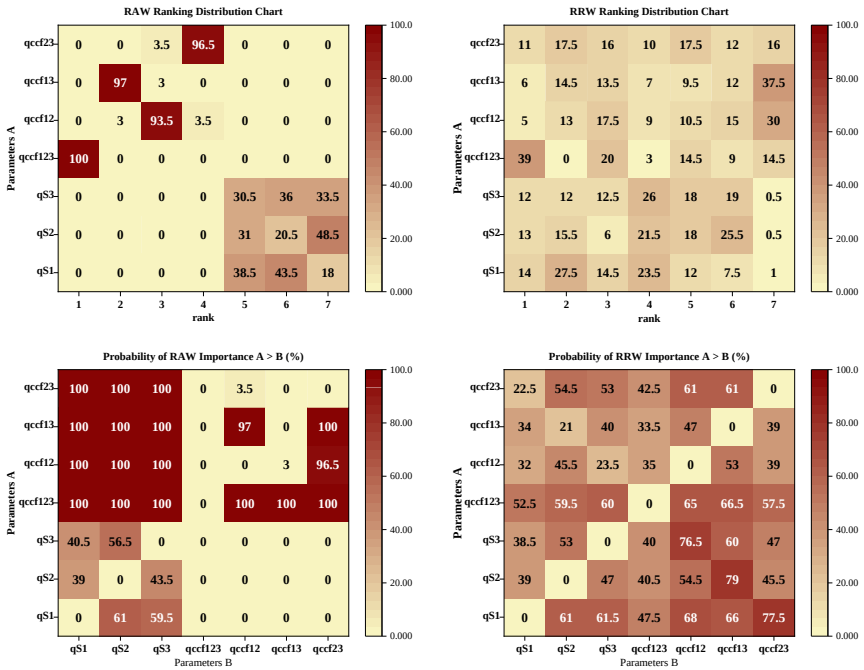

Figure 5. Heatmap of the probability distribution of importance rankings under the baseline epistemic setting.

To avoid redundancy, the robustness discussion above focuses on the baseline configuration shown in Figure 5 The robustness of ranking outcomes under additional sensitivity settings is summarized using rank-frequency heatmaps in Figure 8 and the entropy metrics in Table 14. Across these settings, the dominant contributors and the overall ordering remain stable, indicating that the ranking conclusions are not artifacts of specific modeling assumptions.

5. Sensitivity analyses

5.1. Absorbing-state representation of arming stages

In the proposed DBN-MC approach, each arming stage is

represented as an absorbing state: once an arming stage is reached, it remains active in all subsequent time slices. This choice is a deliberate approximation aligned with the PSA objective considered here—namely, quantifying whether an unintended-arming condition occurs at least once within the mission time and screening for dominant design drivers under limited evidence—rather than representing reset, recovery, or operator interventions. For preliminary design screening, the absorbing-state approximation yields a parsimonious state-space structure and avoids introducing additional transition parameters that are difficult to justify empirically at an early stage.

The validity of this assumption may be limited when transient faults or intermittent disturbances can induce temporary arming indications that later clear, implying reversible arming paths. If such mechanisms are relevant, the DBN–MC can be extended by relaxing the absorbing rows of the CPTs and allowing recovery transitions Sk $1\rightarrow0$. This extension preserves the two-slice DBN factorization but introduces additional transition parameters that should be supported by evidence or conservatively treated under epistemic uncertainty.

5.2. Sensitivity to delayed CCF forcing

The baseline model adopts an instantaneous CCF-forcing assumption, which is conservative in that a realized CCF is assumed to drive the affected arming-stage transition in the same time slice. To examine the conservatism of this assumption, we introduce a discrete forcing delay $\delta\in\{0,1,2\}$ time slices. Operationally, a CCF realization at time t is assumed to exert its forcing effect on the corresponding arming-stage transition at time $t+\delta$.

Figure 6 compares the unintended-arming failure probability trajectories $P_F(t)$ under δ=0,1,2. As expected, nonzero delays mainly introduce a modest lag at early times because the CCF influence has not yet propagated to the final unintended-arming condition. As t increases, the trajectories converge, and the mission-end failure probability $P_F(T)$ changes only slightly with δ. The mean mission-end probabilities and 90% uncertainty intervals are:

For δ=0: $P_F(T)=1.896\times10^{-7}$,

90% uncertainty interval: $[5.421\times10^{-9},6.948\times10^{-7}]$;

For δ=1: $P_F(T)=1.849\times10^{-7}$,

90% uncertainty interval: $[5.257\times10^{-9},6.799\times10^{-7}]$;

For δ=2: $P_F(T)=1.803\times10^{-7}$,

90% uncertainty interval: $[5.104\times10^{-9},6.657\times10^{-7}]$;

These delay-induced differences are small relative to the epistemic spread, indicating that the overall risk quantification is robust to modest forcing delays. Ranking robustness under δ=0,1,2 is summarized in Figure 8; the ordering remains stable relative to the baseline, supporting that the key conclusion regarding CCF dominance is not an artifact of the instantaneous-forcing assumption.

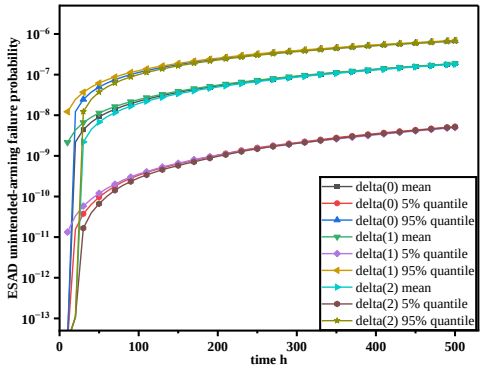

Figure 6. Unintended-arming failure probability $P_F(t)$ under forcing-delay sensitivity (δ=0,1,2). Mean and 5th–95th uncertainty envelope.

5.3. Sensitivity to prior shape of epistemic multipliers

In the preliminary-design setting considered here, available evidence is typically limited to broad order-of-magnitude guidance, and does not support identifying a unique, highly structured prior shape. Introducing additional shape parameters (e.g., skewness, multi-modality, or mechanism-specific tail specifications) would therefore amount to over-parameterizing epistemic belief with assumptions that are difficult to justify or reproduce at this stage. Therefore, we assess prior-shape sensitivity by varying the distributional form of X while keeping the same admissible bounds and the same nominal center, so that differences reflect belief concentration rather than a systematic shift of the CCF scale. We adopt truncated log-normal priors $X_r \sim N(0,\sigma_{10}^2)$truncated to the same bounds $[10^{-2},10^{2}]$ using two a priori dispersion settings to represent different epistemic states: $\sigma_{10}=1.216$ (quantile-matched dispersion) and$\sigma_{10}=0.949$ (more nominal-centered concentration). This set spans a weakly-informative baseline and a nominal-centered

belief within the same physically constrained range, without introducing additional shape parameters that cannot be supported at this design stage. Figure 7 shows that the mean trajectories and 5th–95th percentile bands of the P_F(t) under these priors exhibit substantial overlap and preserve the same temporal trend. Consistently, the RAW/RRW rank-frequency heatmaps in Figure 8 show no qualitative change in the dominant contributors or the overall ordering under the prior-shape switch. Hence, within the adopted admissible range and under the same nominal centering, the main risk and importance conclusions are robust to reasonable variations in prior shape.

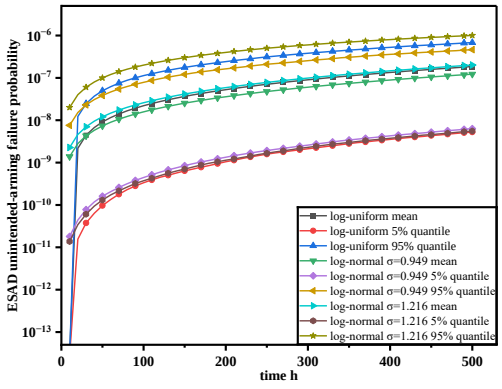

Figure 7. Prior-shape sensitivity of unintended-arming failure probability $P_F(t)$.

5.4. Sensitivity to epistemic-range contraction

To illustrate the effect of epistemic convergence due to accumulating evidence, we hypothetically contract the admissible uncertainty range of the CCF multipliers while keeping the nominal CCF parameter values fixed. Specifically, we narrow the baseline range from $X=\log_{10}(U_r)\in[-2,2]$ to a contracted range $X=\log_{10}(U_r)\in[-0.5,0.5]$ The contraction reduces the dispersion of ranking outcomes for both importance indices, consistent with increased concentration of epistemic belief. The comparative rank-frequency heatmaps for RAW and RRW under the contracted range are included in Figure 8. Quantitatively, Table 14 reports the corresponding normalized Shannon-entropy coefficients, showing decreased entropy under the contracted range and a noticeably stronger reduction for RRW. RAW rankings remain highly concentrated, consistent with the structural dominance of q_{ccf123} in the forced-occurrence analysis, whereas RRW becomes more concentrated toward leading improvement candidates, indicating improved consistency of improvement prioritization as epistemic uncertainty narrows. Residual dispersion is not fully eliminated because RRW depends on which risk-contributing mechanism dominates under each realization, even within a narrower range.

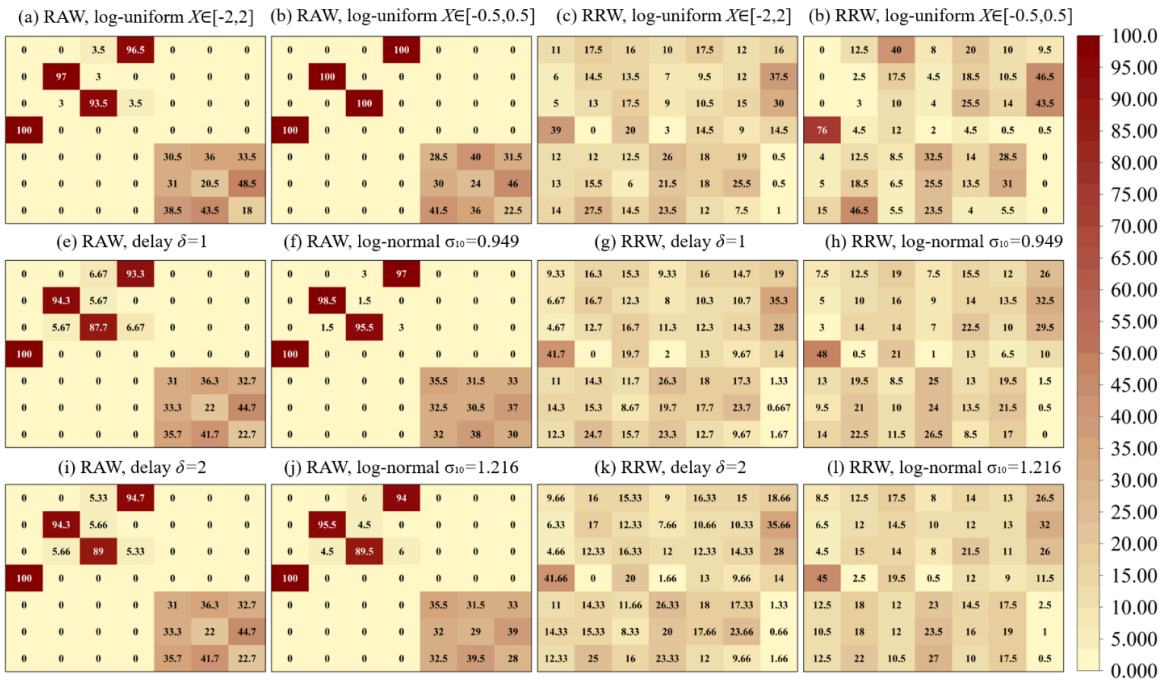

Figure 8. Robustness of RAW/RRW ranking heatmaps across sensitivity settings.

Rank-frequency heatmaps (probability that each event attains each rank across epistemic scenarios) for RAW (left two columns) and RRW (right two columns) under multiple sensitivity configurations. The figure includes: (i) the baseline log-uniform admissible range $X=\log_{10}(U_r)\in[-2,2]$ and an evidence-converged contracted range $X\in[-0.5,0.5]$ (ii) forcing-delay sensitivity with $\delta=1$ and $\delta=2$ time-slice delays; and (iii) prior-shape sensitivity using truncated log-normal multipliers with $\sigma_{10}=0.949$ and $\sigma_{10}=1.216$, all enforcing identical bounds when applicable. The ordering of dominant contributors remains stable across sensitivity settings, indicating robust importance conclusions.

Table 14. Normalized Shannon-entropy coefficients (H_e) of importance-ranking dispersion under two epistemic-uncertainty magnitudes (log-uniform multipliers).

Parameter Name	Log-uniform[-2,2]		Log-uniform [-0.5,0.5]	
	H_e^{RAW}	H_e^{RRW}	H_e^{RAW}	H_e^{RRW}
q_{S1}	0.53	0.90	0.55	0.73
q_{S2}	0.53	0.89	0.55	0.83
q_{S3}	0.56	0.91	0.56	0.82
q_{ccf123}	0.00	0.81	0	0.45
q_{ccf12}	0.15	0.93	0	0.75
q_{ccf13}	0.07	0.90	0	0.74
q_{ccf23}	0.08	0.99	0	0.82

6. Conclusion

This paper proposes a DBN–MC-based dynamic PSA framework for ESAD architectures with sequential enabling constraints and multi-source CCF mechanisms under data-scarce epistemic uncertainty. By encoding absorbing Safety/CCF dynamics together with enabling/forcing logic via local CPTs and propagating epistemic uncertainty through outer-loop Monte Carlo sampling, the framework produces unintended-arming probability trajectories with percentile uncertainty bands for a priori design-stage assessment. A numerical cross-check against an equivalent discrete-time Markov model shows consistent forward-propagation results. In the case study, the unintended-arming probability remains on the order of 10^{-7} while its uncertainty interval spans multiple orders of magnitude, indicating that epistemic uncertainty in CCF parameters dominates the percentile bounds. Intervention-based importance analysis provides two complementary decision views: RAW identifies structurally dominant escalation mechanisms with robust dominance across epistemic scenarios, whereas normalized RRW quantifies improvement potential and is scenario dependent under different epistemic realizations. These results support an uncertainty-informed two-level ESAD strategy: (i) protect against structurally dominant CCF paths guided by RAW, and (ii) prioritize design improvements using RRW under the remaining epistemic uncertainty. A practical limitation is the exponential state-space growth associated with exact DBN inference for larger architectures. Future work will investigate scalability enhancements via state aggregation/compression and approximate inference methods that exploit conditional independencies.

References

1. O'Connor P D T, Kleyner A. Practical Reliability Engineering. 5th ed. Chichester (UK): John Wiley & Sons; 2012. doi:10.1002/9781119961260.
2. Zhang Y, Chen J. Dual-loop integration framework for model-based system design and reliability analysis using Bayesian networks. Results in Engineering 2025; 27: 106018. doi:10.1016/j.rineng.2025.106018.
3. Uludağ Y, Evin E, Gürbüz N G. Integration of systems design and risk management through model-based systems development. Systems Engineering 2023; 26(1): 48–70. doi:10.1002/sys.21643.
4. Kuelper N, Jeyaraj A K, Liscouët-Hanke S, Thielecke F. Integration of a model-based systems engineering framework with safety assessment for early design phases: A case study for hydrogen-based aircraft fuel system architecting. Results in Engineering 2025; 25: 104249. doi:10.1016/j.rineng.2025.104249.
5. Zhou Z, Zhang Q. Model event/fault trees with dynamic uncertain causality graph for better probabilistic safety assessment. IEEE Transactions on Reliability 2017; 66(1): 178–188. doi:10.1109/TR.2017.2647845.
6. Tan J, Chen X, Bu Y, Wang F, Wang J, Huang X, Hu Z, Liu L, Lin C, Meng C, Lin J, Xie SJ, Xu J, Jing R, Zhao Y. Incorporating FFTA based safety assessment of lithium-ion battery energy storage systems in multi-objective optimization for integrated energy systems. Applied Energy 2024; 367: 123472. doi:10.1016/j.apenergy.2024.123472.

7. Bai X, Liu F, Hao Y, Pan J. Security system safety research for fully electronic initiators. Journal of Ordnance Equipment Engineering 2024; 45(11): 59–67. doi:10.11809/bqzbgcxb2024.11.008.
8. Chen D, Xu J Y, Yao C Y, Pan H Y, Hu Y L. Continuous-time T-S dynamic fault tree analysis method. Journal of Mechanical Engineering 2021; 56(10): 231–244. doi:10.3901/JME.2021.10.231.
9. Dang R. Electronic safety and arming system [master's thesis]. Nanjing (China): School of Mechanical Engineering, Nanjing University of Science and Technology 1991. doi:10.7666/d.Y170516.
10. He G. Analysis on the arming logic of fuze electronic safety and arming. Transactions of Beijing Institute of Technology 2008; 28(12): 1083–1087.
11. Wang P, Li H, Yu H, Zhang C. Failure probability calculation of a recoverable loitering munition fuze electronic safety system. Journal of Detection & Control 2025; 47(1): 57–63. doi:10.20225/j.issn.1008-1194.20250107.
12. Dagal I. Probabilistic fault tree analysis and dynamic redundancy optimization for next-generation avionic flight control systems. Reliability Engineering & System Safety 2026; 266: 111841. doi:10.1016/j.ress.2025.111841.
13. Wang Y, Ma Q. Electronic safety and arming system failure probability calculation methods. Journal of Detection and Control 2023; 45(1): 1–10.
14. Huang Z, Huang X. Control logic design of electronic safety system and failure probability calculation. Journal of Ordnance Equipment Engineering 2024; 45(8): 140–145. doi:10.11809/bqzbgcxb2024.08.019.
15. Zhao X, Malasse O, Buchheit G. Verification of safety integrity level of high demand system based on stochastic Petri nets and Monte Carlo simulation. Reliability Engineering & System Safety 2019; 184: 258–265. doi:10.1016/j.ress.2018.02.004.
16. International Electrotechnical Commission. IEC 61508-6:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3. Geneva (Switzerland): IEC; 2010.
17. Zhang H Y, Li S X, Zhang H W, Tian H R. β factor estimation method based on D-S evidence theory. Railway Standard Design 2023; 67(9): 170–175. doi:10.13238/j.issn.1004-2954.202204010007.
18. He Z, Wang S, Shi J, Liu D, Duan X, Shang Y. Physics-informed neural network supported wiener process for degradation modeling and reliability prediction. Reliability Engineering & System Safety 2025; 258: 110906. doi:10.1016/j.ress.2025.110906.
19. Wang E, Wu X, Liu D, Wang S, Shang Y. Artificial neural network supported monotonic stochastic processes for reliability analysis considering multi-uncertainties. Eksploatacja i Niezawodność – Maintenance and Reliability 2025; 27(3): 197051. doi:10.17531/ein/197051.
20. Jiang J, Wang Y, Li Z. A cognitive reliability model research for complex digital human-computer interface of industrial system. Safety Science 2018; 108: 196–202. doi:10.1016/j.ssci.2017.07.016.
21. Xin J, Wang D, Guo R. Research on satellite-ground operation model and reliability of navigation satellite system. Systems Engineering—Theory & Practice 2020; 40(2): 520–528. doi:10.12011/1000-6788-2018-0850-09.
22. Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering & System Safety 2001; 71: 249–260. doi:10.1016/S0951-8320(00)00077-6.
23. Nima K, Faisa K, Paul A. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety Science 2013; 57: 108–117. doi:10.1016/j.ssci.2013.01.022.
24. Nima K, Faisa K, Paul A. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliability Engineering & System Safety 2011; 96(8): 925–932. doi:10.1016/j.ress.2011.03.012.
25. Daniel S. Stochastic modeling of deterioration processes through dynamic Bayesian networks. Journal of Engineering Mechanics 2009; 135(10): 1089–1099. doi:10.1061/(ASCE)EM.1943-7889.0000024.
26. Berrouane M T, Khan F, Amyotte P. Bayesian stochastic Petri nets (BSPN)—A new modelling tool for dynamic safety and reliability analysis. Reliability Engineering & System Safety 2020; 193: 106587. doi:10.1016/j.ress.2019.106587.
27. Nie Z, Chang Y, Liu X Q, Chen G M. A DBN-Go approach for success probability prediction of drilling riser emergency disconnect in deep water. Ocean Engineering 2019; 180: 49–59. doi:10.1016/j.oceaneng.2019.04.005.
28. Guo Y, Zhong M, Gao C, Wang H D, Liang X, Yi H. A discrete-time Bayesian network approach for reliability analysis of dynamic systems with common cause failures. Reliability Engineering & System Safety 2021; 216: 108028. doi:10.1016/j.ress.2021.108028.

29. Yu Y, Shuai B, Huang W. Resilience evaluation of train control on-board system considering common cause failure: Based on a beta-factor and continuous-time Bayesian network model. Reliability Engineering & System Safety 2024; 246: 110088. doi:10.1016/j.ress.2024.110088.
30. Zhang R, Song S. Bayesian network approach for dynamic fault tree with common cause failures and interval uncertainty parameters. Eksploatacja i Niezawodność – Maintenance and Reliability 2024; 26(4): 190379. doi:10.17531/ein/190379.
31. Bai L, Shen J, Qiu Y, Zhang Y. Reliability analysis of phased-mission system with common cause failure based on discrete-time Bayesian network. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 2025. doi:10.1177/1748006X251380917.
32. Yao C Y, Han D D, Chen D N, Liu Y M. A novel continuous-time dynamic Bayesian network reliability analysis method considering common cause failure. Chinese Journal of Scientific Instrument 2022; 43: 174–184. doi:10.19650/j.cnki.cjsi.J2209135.
33. Song Y, Mi J, Cheng Y, Bai L, Wang X. Application of discrete-time Bayesian network on reliability analysis of uncertain system with common cause failure. Quality and Reliability Engineering International 2019; 35(4): 1025–1045. doi:10.1002/qre.2443.
34. Liu Z, Liu Y, Cai B, Zhang D, Zheng C. Dynamic Bayesian network modeling of reliability of subsea blowout preventer stack in presence of common cause failures. Journal of Loss Prevention in the Process Industries 2015; 38: 58–66. doi:10.1016/j.jlp.2015.09.001.
35. Fan D, Wang Z, Liu L, Ren Y. A modified GO-FLOW methodology with common cause failure based on discrete time Bayesian network. Nuclear Engineering and Design 2016; 180: 49–59. doi:10.1016/j.nucengdes.2016.06.010.
36. Li Z Q, Xu T X, An J, Fu L Y, Gu J Y. Common cause failure modeling for redundant system based on dynamic Bayesian network. Chinese Journal of Scientific Instrument 2018; 39(3): 190–198. doi:10.19650/j.cnki.cjsi.J1702575.
37. Neapolitan RE. Learning Bayesian Networks. Upper Saddle River (NJ): Prentice Hall; 2003.
38. Khakzad N, Reniers G, Abbassi R, Khan F. Vulnerability analysis of process plants subject to domino effects. Reliability Engineering & System Safety 2016; 154: 127–136. doi:10.1016/j.ress.2016.06.004.
39. Murphy K P. Dynamic Bayesian Networks: Representation, Inference and Learning [PhD dissertation]. Berkeley (CA): University of California, Berkeley; 2002.
40. Wang H, Wu Y, Liu P. Study on the effect of probability truncation limit on probabilistic safety assessment RAW for importance measures. Nuclear Science and Engineering 2006; 4: 363–367. doi:10.3321/j.issn:0258-0918.2006.04.014.
41. Xu Z, Song Z. Discussion on relationship between risk reduction factor and average failure probability on demand. Automation in Petro-Chemical Industry 2021; 57(6): 47–49. doi:10.3969/j.issn.1007-7324.2021.06.012.

Nomenclature

t	Discrete time index, t=0,1,…,T
Δt	Discretization time step
T	Mission-end index (number of time steps)
X_t	Set of all DBN variables at time t
$S_k(t)$	k_{th} safety component state at time t
$CCF_r(t)$	State of CCF mechanism r at time t
$P(\cdot)$	Probability operator
$P_F(t)$	ESAD unintended-arming failure probability at time t
$P_F(T)$	Mission-end unintended-arming probability
q_{Sk}	Per-step independent transition probability S_k: Unarmed→Armed
q_{CCFr}	Per-step occurrence probability of CCF mechanism r
U_r	Epistemic multiplier applied to CCF parameter
X_r	Log-scale epistemic variable $X_r=\log_{10}(U_r)$
σ_{10}	Standard deviation of the log-normal prior for X_r on the $\log_{10}$ scale
δ	Discrete forcing delay (time slices) for CCF-to-arming influence; effect applied at $t+\delta$
S	Number of epistemic scenarios
s	Epistemic scenario index
$\theta(s)$	Realization of the full uncertain-parameter set in scenario s
i	Basic-event/parameter index
q_i	Generic per-step probability parameter indexed by i
q_i^0	Baseline (nominal) value of parameter q_i
π	Configuration of a node's parent variables
RAW_i	Risk Achievement Worth of parameter i
RRW_i	Normalized Risk Reduction Worth of parameter i
$Rank_i(s)$	Rank position of event i in scenario s
$p_{i,r}$	Empirical probability that event i attains rank r across scenarios

n	Number of ranked basic events/parameters
H_e	Normalized Shannon entropy of rank distribution