Taylor & Francis
Taylor & Francis Group

Journal of Applied Non-Classical Logics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tncl20

Epistemic space of degradation processes

Liu Yang & Antoine Rauzy

To cite this article: Liu Yang & Antoine Rauzy (2021) Epistemic space of degradation processes, Journal of Applied Non-Classical Logics, 31:1, 1-25, DOI: 10.1080/11663081.2020.1850047

To link to this article: https://doi.org/10.1080/11663081.2020.1850047

Published online: 26 Nov 2020.

JOURNAL OF APPLIED NON-CLASSICAL LOGICS
2021, VOL. 31, NO. 1, 1–25
https://doi.org/10.1080/11663081.2020.1850047

Taylor & Francis
Taylor & Francis Group

Epistemic space of degradation processes

Liu Yang and Antoine Rauzy

Department of Mechanical and Industrial Engineering (MTP), Norwegian University of Science and Technology (NTNU), Trondheim, Norway

ABSTRACT

In this article, we present a new approach of modelling epistemic uncertainties in degradation processes. This approach is established in the framework of finite degradation structures (FDSs), which is recently proposed by the authors and can be seen as a formal extension of the fault tree analysis into multistate systems. When epistemic uncertainties are added to the states of the system, it implicitly increases the number of states and make even the Boolean systems become multistate. In the existing approaches, the addition of epistemically uncertain states as well as the new valuation mappings of the operations for those states should be done manually by the analysts depending on the type of system and its components. This manual addition may be time-consuming, error-prone and lack of generality, especially when systems get large and complex. Instead of manually remodelling the system, we propose in this article to automatic transform the model built on FDSs into epistemic space to take into account epistemic uncertainties. The proposed automatic transformations are mathematically defined and explained. As results, the uncertainty-embedded (critical) scenarios and probabilistic indicators like the belief and the plausibility in the Dempter–Shafer theory can be obtained. Illustrative examples with experimental results are also provided.

ARTICLE HISTORY
Received 1 July 2019
Accepted 12 October 2020

KEYWORDS
Epistemic uncertainty; degradation process; finite degradation structures; multistate systems; Dempter–Shafer theory

1. Introduction

Since 1960s, Boolean logics have been widely applied in reliability and safety analysis, i.e. as the mathematical basis of combinatorial models like fault trees, event trees and reliability block diagrams. In fault tree analysis (FTA), components are assumed to be either working or failed and they are modelled by Boolean variables taking values in $\{0, 1\}$, where 0 stands for working and 1 stands for failed. A fault tree is made up of events and logic gates, where events are Boolean variables and logic gates are AND gate, OR gate, XOR gate, …, which are used to describe the failure mechanism of the system under study (see Ruijters & Stoelinga, 2015). Fault tree models are therefore Boolean functions, based on which the probability of top event and the minimal cutsets (i.e. prime implicants) (Rauzy, 2001) can be calculated to support the required reliability and safety analysis.

CONTACT Liu Yang zf_yangliu@126.com

However, when the states of component are not Boolean, i.e. that it may experience a series of degradation states before ultimately being failed, the classical FTA becomes inapplicable. Many researches have been dedicated to solve this situation. The first is to use the so-called state/transition models (i.e. finite state automata), such as Markov chains, Petri nets and guarded transition systems (Rauzy, 2008). Although these models are able to capture multistate features, their computational complexity of calculating risk indicators (i.e. using stochastic simulations) increases dramatically when systems get large (Rauzy, 2018). The second solution is to add more truth values between 0 and 1, for instance, the fuzzy sets (Zadeh, 1965, 1999) and theories like the so-called multistate systems (Ushakov, 2012), universal generating functions (Levitin, 2005), multi-valued logics (Zaitseva & Levashenko, 2017) and multi-valued decision diagrams (Nakahara et al., 2017; Zhai et al., 2015). These approaches are well designed for probabilistic calculations, however, the notion of minimal cutsets in traditional FTA has not been fully concluded, since they only compare the minimality between the working state with other non-working states while not provide a formal way to define the 'minimality' between degradation states and failed states.

In order to realise the formal and complete extension of FTA into multistate systems, we have proposed a unified combinatorial modelling framework, called finite degradation structures (FDSs) (Rauzy & Yang, 2019b). In FDSs, the state space of an object (i.e. component/subsystem/system) is modelled by a partially ordered set, more exactly a meet-semi-lattice. The partial orders in such meet-semi-lattice are interpreted as degradation orders, by which the states are ordered according to their degradation levels in the state space of the object. Thanks to this ordering relationship, the notion of minimal cutsets can be fully extended into multistate systems, i.e. that the minimality of cutsets are defined by the minimality of their degradation levels. The cutsets analysis in FDSs is therefore named as scenarios analysis since not only failure scenarios (i.e. cutsets) but also degradation scenarios as well as the working scenarios can be analysed. In FDSs, the notion of minimal cut/path sets is replaced by the notion of minimal and maximal scenarios. Moreover, to support the calculation of probabilistic risk indicators, we allow to equip the meet-semi-lattices with probability measures so that the indicators calculated in FTA, such as probability of failure and importance measures, can be calculated in a similar way in FDSs.

The modelling of epistemic space of degradation process can be seen as a typical application of FDSs. Generally, reliability and safety models are built under the condition that the knowledge about the current state of system is complete. However, such condition may not be fulfilled in all situations, i.e. that there may be some discrepancies between the diagnostic made on the state of system and its actual state. These discrepancies will implicitly increase the number of states (i.e. by introducing uncertain states) that are needed to be studied in the system and eventually make even the Boolean systems become multistate. This is exactly where FDSs can come into play.

Another highlighted advantage of applying FDSs to model epistemic uncertainties is that each time when needs to add uncertainties, the model can be automatically transformed into epistemic space rather than being manually reconstructed. This automatic transformation is more efficient, more generic and less error prone than the manual work especially when the number of states in the state space increases.

Technically, this automatic transformation is made up of two parts: the transformation of FDSs and the transformations of operations on FDSs. For the former, the degradation orders can be automatically transformed while the probability measure should be reassigned as belief functions (see the Dempster–Shafer theory in Dempster, 2008; Shafer, 1976 and the subsequent theories like Salicone, 2007). For the operations on FDSs, we propose four transformations regarding different places where uncertainties are added. The assessment of the transformed model follows the same procedure as the original one. Calculation algorithms can be found in our papers (Rauzy & Yang, 2019a; Yang & Rauzy, 2019). As results, uncertainty-embedded (critical) scenarios and probabilistic indicators such as belief and plausibility can be calculated from the transformed model.

The rest of the article proceeds as follows. Section 2 presents a case study of the attack of a storage farm and identifies the epistemic uncertainties focused in this article. Section 3 gives a quick view of the modelling framework of FDSs. Section 4 shows the proposed automatic transformations. Section 5 presents two examples of how to reinterpret models built on FDSs. Section 6 identifies the accessible resulted indicators and shows the calculation results of two examples in Section 5. Finally, Section 7 concludes the article.

2. Illustrative case study

2.1. System description

This case study is extracted from Misuri et al. (2018). The objective is to analyse the security problem of the storage farm if an attack (which is uncertain) happens.

The outline of the storage farm is shown in Figure 1.

For the sake of simplicity, the fault tree model of this case study is written by the following Boolean equations:

$$\begin{aligned}
Attack(OR) &:= \vee(AG, AW)\\
Attack(XOR) &:= \sqcup_{XOR}(AG, AW)\\
AG &:= \wedge(UIG, Exp)\\
AW &:= \wedge(UIW, Exp)\\
UIG &:= \wedge(\wedge(FSL, CCTV), SF)\\
UIW &:= \wedge(\wedge(CCTV, SF), Doc)\\
Exp &:= \wedge(IED, Reg)\\
FSL &:= \wedge(\vee(MG, FF), Pat)\\
Doc &:= \wedge(Pat, DB)
\end{aligned} \tag{1}$$

The acronyms in the above equations can be found in Table 1. The two top events $Attack(OR)$ and $Attack(XOR)$ represent the two different points of view of the success of the attack with respect to the attack via ground *AG* and the attack via water *AW*. The operators $\vee$, $\wedge$ and $\sqcup_{XOR}$ stand for the disjunction, the conjunction and the exclusive-OR operation. The valuations of $\wedge(u, v)$, $\vee(u, v)$ and $\sqcup_{XOR}(u, v)$ are given in Table 2.

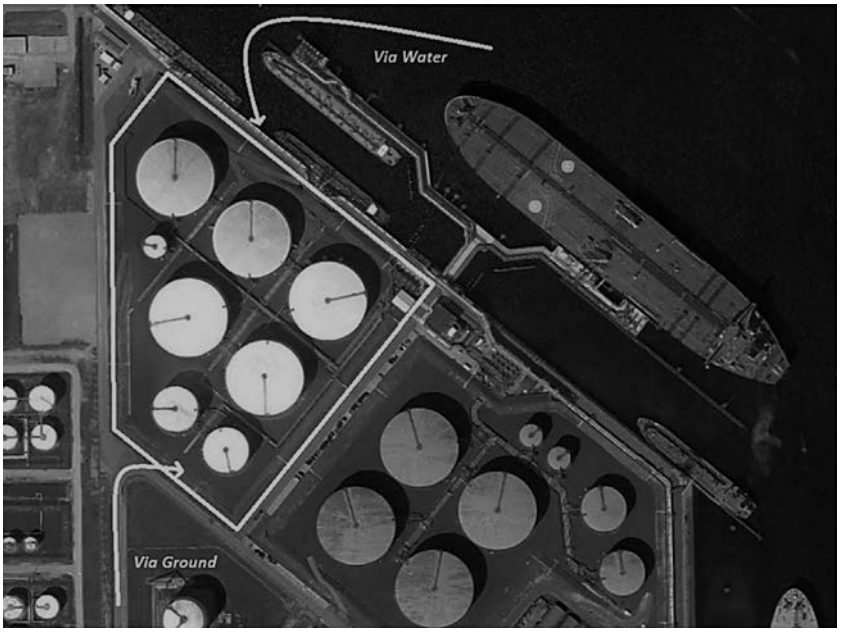

Figure 1. Case study in Misuri et al. (2018), where the premises of the storage farm are outlined in white; the two intrusion paths considered, 'Via Ground' and 'Via Water' are reported as white arrows.

Table 1. Definitions of acronyms.

AG	Attact via Ground	AW	Attact via Water
UIG	Undetected Intrusion from Ground	UIW	Undetected Intrusion from Water
Exp	Explosion	FSL	First Security Layer
FF	First Fence	SF	Second Fence
Pat	Patrol	MG	Main Gate
Doc	Docking	DB	Docking Barriers
IED	Improvised Explosive Device	Reg	Regress

Table 2. The valuation of $\wedge(u, v)$, $\vee(u, v)$ and $\sqcup_{XOR}(u, v)$.

		$\wedge$				$\vee$				$\sqcup_{XOR}$	
v		W	F	v		W	F	v		W	F
u	W	W	W	u	W	W	F	u	W	W	F
	F	W	F		F	F	F		F	F	W

2.2. Incomplete knowledge on states

In reliability and safety analysis, uncertainties can be categorised into aleatory uncertainty and epistemic uncertainty (Helton & Burmaster, 1996; Parry, 1996). The aleatory aspect of uncertainty is addressed when the occurrence of an event or a phenomenon is modelled as a random variable in a stochastic manner. Therefore, aleatory uncertainty can be mathematically modelled using probability theory. The epistemic uncertainty is caused by the incomplete information and the lack of knowledge. Although probabilistic measure is also used to quantify epistemic uncertainty, it is

interpreted – different from the probability of random variables – as a kind of subjective probability or belief that measures the analysts' confidence on a phenomenon.

In this article, we focus on the epistemic uncertainty caused by the incomplete knowledge on the states of objects (i.e. components/subsystems/system).

Given a multistate component C, let the finite set $\Theta = \{x_1, \ldots, x_n\} (n \geq 1)$ be its state space and v be its state variable. Denote the valuation domain of v by $\mathrm{dom}(v)$.

- If the states of C are certain, then $\mathrm{dom}(v) = \Theta$;
- If the states of C are epistemically uncertain, then $\mathrm{dom}(v) = 2^{\Theta} \backslash \{\emptyset\} = \Omega$.

2^{Θ} is the power set of Θ. Ω is called the epistemic space of Θ which contains all the epistemically possible values of v (Bjerring, 2014). The empty set ø is excluded from Ω since v should take at least one value in Θ according to the closed-world assumption.

Take the Boolean component as example. The state space Θ is $\{W, F\}$, where W stands for working and F stands for failed. According to the above definition, its epistemic space Ω is $2^{\{W,F\}} \backslash \{\emptyset\} = \{\{W\}, \{F\}, \{W, F\}\}$. Each element in Ω can be understood as follows:

- $\{W\}$ means that it is known that the component is working;
- $\{F\}$ means that it is known that the component is failed;
- $\{W, F\}$ means that the state of the component is unknown between W and F.

2.3. Problems in modelling epistemically uncertain states

Reliability and safety models are generally built under the condition that the knowledge about the current state of system is complete, e.g. the fault tree in Equation (1). However, such condition may not be fulfilled in all situations, i.e. that there may be some discrepancies between the diagnostic made on the state of system and its actual state. These discrepancies will implicitly increase the number of states (i.e. by introducing uncertain states) that are needed to be studied in the system. For example, the epistemic space $\Omega = 2^{\{W,F\}} \backslash \{\emptyset\} = \{\{W\}, \{F\}, \{W, F\}\}$ has an additional uncertain state $\{W, F\}$ comparing to the state space $\Theta = \{W, F\}$. This enlargement will obviously make even the Boolean components/systems become multistate.

When epistemic uncertainties are added to the model, a direct consequence is that both of the valuation domains of related variables and the valuation mappings of their operations should be adapted. In the state-of-the-art literature, this adaptation is done manually by the analysts depending on the type of system and its components. However, the manual adaptation may become time-consuming and error-prone when the number of states in the state space increases, and moreover lack of generality when the type of operations varies from one system to another.

Let's do a simple calculation to estimate the adaptations needed to be done when epistemic uncertainties are added to two components of the same type in the system under study.

Assume that the states of both two components are valued in Θ and there is n states in Θ. Then, the number of elements in their epistemic space Ω is $2^n - 1$ since $\Omega = 2^{\Theta} \backslash \{\emptyset\}$. The number of newly added elements in Ω is therefore $2^n - n - 1$. Consider a binary operation applied on those two components, i.e. $\Theta \times \Theta$. When epistemic

Table 3. Number of newly added epistemically uncertain states and valuation mappings for a binary operation.

# of states	# of epistemically uncertain states	# of new valuation mappings
n	$2^n - n - 1$	$(2^n - n - 1)^2 + 2n \cdot (2^n - n - 1)$
1	0	0
2	1	5
3	4	40
4	11	209
5	26	936

uncertainties are added to both components, the input domain of such operation is changed to $\Omega \times \Omega$. Therefore, the number of new valuation mappings needed to be added is $(2^n - n - 1)^2 + 2n \cdot (2^n - n - 1)$. Table 3 gives the concrete number of these numbers in the case of $n = 1, 2, 3, 4, 5$.

From Table 3, we can see that when $n = 2$, there is only one new state needed to be added in Ω for each component and 5 new valuation mappings to be added for each binary operation. This is exactly the case studied in Misuri et al. (2018), where valuation domains and valuation mappings are manually adjusted for adding epistemic uncertainties. However, when $n = 3$, 4 and 5, we can see that the number of new valuation mappings to be added for a binary operation increases rapidly, which is 40, 209 and 936. It means that in these cases, the manual addition of those new valuation mappings becomes almost unfeasible.

Moreover, there are also components whose states are certain (e.g. components that are continuously monitored) or whose uncertainty is not important so that can be ignored in the analysis. It means that uncertainties do not need to be added to all components of the system under study. As result, the model will be mixed up with uncertain/certain components and operations. This heterogeneity will also increase the difficulty of modelling the system as well as calculating required risk indicators.

In FDSs, the aforementioned modelling and calculation problems can all be solved. First, the problem of adding large number of valuation mappings when $n \geq 3$ can be solved by applying automatic transformations of operations on FDSs. If the original model (i.e. without uncertainty) is built on FDSs, the addition of epistemic uncertainties only requires to reassign the belief function as probability measure for those components where uncertainties are added and reinterpret the model by simply declaring which of the four transformations should be used for each operation (see Sections 4 and 5). Second, we demonstrated in Section 4 that the framework of FDSs is closed under the proposed transformations, which means that the uncertain/certain components and operations can be modelled and assessed in a uniform way using FDSs.

3. Finite degradation structures

3.1. Formal definition

In mathematical point of view, finite degradation structures (FDSs) are meet-semilattices equipped with probability measures.

Let D be a set and $\sqsubseteq$ be a *partial order* over D. The pair $\langle D, \sqsubseteq \rangle$ is a *partially ordered set* (poset) if the following axioms hold, i.e. $\forall\, x, y, z \in D$:

- $x \sqsubseteq x$ (Reflexivity)
- If $x \sqsubseteq y$ and $y \sqsubseteq z$, then $x \sqsubseteq z$ (Transitivity)
- If $x \sqsubseteq y$ and $y \sqsubseteq x$, then $x = y$ (Antisymmetry),

Definition 3.1: A *meet-semi-lattice*, denoted by $\langle D, \sqsubseteq, \bot \rangle$, is a poset $\langle D, \sqsubseteq \rangle$ that has a least element $\bot \in D$ such that $\forall\, x \in D, x \neq \bot \Rightarrow \bot \sqsubset x$.

Definition 3.2: A *finite degradation structure (FDS)* is defined as a quadruple $\langle D, \sqsubseteq, \bot, p \rangle$ such that D is finite, $\langle D, \sqsubseteq, \bot \rangle$ is a meet-semi-lattice and $p : D \to [0, 1]$ is a probability measure on D such that $\sum_{d \in D} p(d) = 1$.

FDSs are used to model state spaces.

The partial order $\sqsubseteq$ is named as *degradation order* and interpreted as 'less or equally degraded than'. For instance, the working state W is obviously less degraded than the failed state F, i.e. denoted by $W \sqsubset F$. If two states x and y are incomparable, they are denoted by $x \sim y$. For instance, we may consider that the failed-safely state Fs is incomparable with the failed-dangerously state Fd, i.e. $Fs \sim Fd$.

Figure 2 illustrates four FDSs that can be used in reliability and safety analysis. Such diagram is called Hasse diagram, where vertices are states and any relation $x \sqsubset y$ is drawn as a line segment that goes upward from x to y. For simplicity, we name respectively the FDSs in Figure 2(a–d) by **WF**, **WDF**, **SWF** and **WFdFs**.

For each FDS, it is possible to equip with a probability measure $p : D \to [0, 1]$ to record the probability of being in each state in D. The probability measure p can also evolve over time, i.e. $p : D \times \mathbb{R}^+ \to [0, 1]$ and $p(d, t)$ is the probability of being in the state $d \in D$ at time $t \in \mathbb{R}^+$.

More examples of applying FDSs in reliability modelling can be found in our paper (Yang & Rauzy, 2018).

3.2. Operations

In FDSs, two types of operations are provided to model the failure mechanism of the system under study.

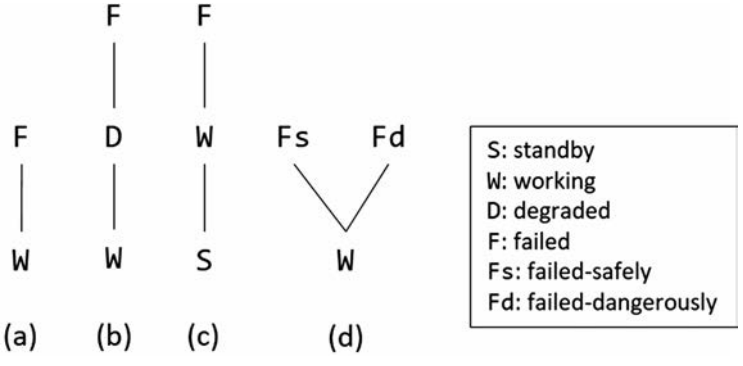

Figure 2. Examples of FDSs used in reliability and safety analysis.

The first is called the monoidal product of FDSs, denoted by $\otimes$, which achieves the composition of state spaces of components. The second is called the abstraction between FDSs, which achieves the mapping from the composed state spaces to the system's state space.

Denote the set of all FDSs by **FDS**. We can prove that **FDS** is closed under both of these two operations.

Definition 3.3: The (monoidal) *product* of FDSs is defined as the bifunctor $\otimes$: **FDS** $\times$ **FDS** $\rightarrow$ **FDS** such that for all $\mathcal{L}_1 : \langle D_1, \sqsubseteq, \bot_1, p_1 \rangle, \mathcal{L}_2 : \langle D_2, \sqsubseteq, \bot_2, p_2 \rangle \in$ **FDS**, $\mathcal{L}_1 \otimes \mathcal{L}_2 = \langle D_\otimes, \sqsubseteq, \bot_\otimes, p_\otimes \rangle$, where:

- $D_\otimes = D_1 \times D_2$;
- $\forall (x_1, x_2), (y_1, y_2) \in D_\otimes, (x_1, x_2) \sqsubseteq (y_1, y_2) \Leftrightarrow (x_1 \sqsubseteq y_1) \wedge (x_2 \sqsubseteq y_2)$;
- $\bot_\otimes = (\bot_1, \bot_2)$;
- $\forall (x, y) \in D_\otimes, p_\otimes(x, y) = p_1(x) \cdot p_2(y)$.

Figure 3 shows graphically the products **WF** $\otimes$ **WF**, **WF** $\otimes$ **WDF**, **WDF** $\otimes$ **WF** and **WDF** $\otimes$ **WDF**.

Definition 3.4: Let $\mathcal{S} : \langle D_S, \sqsubseteq, \bot_S, p_S \rangle$ and $\mathcal{T} : \langle D_T, \sqsubseteq, \bot_T, p_T \rangle$ be two FDSs. An *abstraction* from $\mathcal{S}$ to $\mathcal{T}$ is a mapping $\varphi : \mathcal{S} \rightarrow \mathcal{T}$ such that:

- φ is surjective, i.e. $\forall y \in D_T, \exists x \in D_S, \varphi(x) = y$,
- $\varphi(\bot_S) = \bot_T$,
- $\forall y \in D_T, p_T(y) = \sum_{x \in \varphi^{-1}[y]} p_S(x)$.

A binary operation on FDSs is therefore an abstraction ϕ in the following form:

$$\phi : \mathcal{A} \otimes \mathcal{B} \rightarrow \mathcal{C}$$

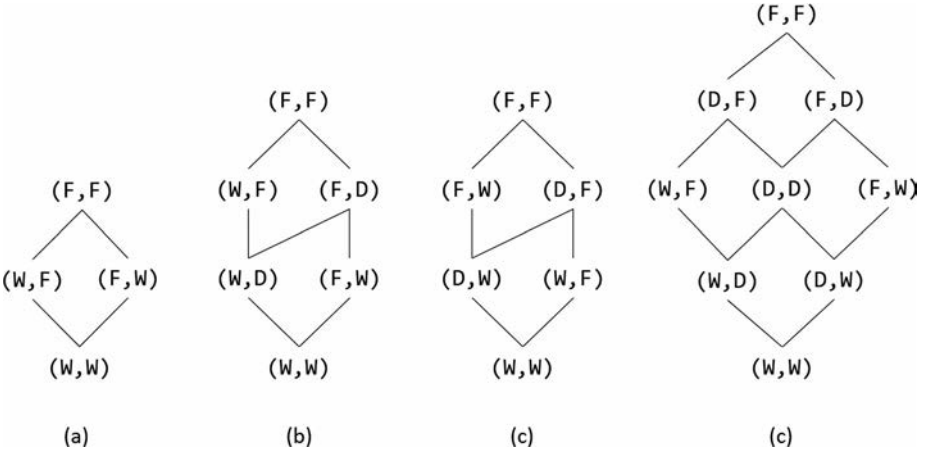

Figure 3. The resulting product of **WF** $\otimes$ **WF**, **WF** $\otimes$ **WDF**, **WDF** $\otimes$ **WF** and **WDF** $\otimes$ **WDF**.

where $\mathcal{A}, \mathcal{B} \in \mathbf{FDS}$ are the valuation domains of the two input arguments and $\mathcal{C} \in \mathbf{FDS}$ is the valuation domain of the output.

Additionally, if $\forall x_1, x_2 \in D_S, x_1 \sqsubseteq x_2 \Rightarrow \varphi(x_1) \sqsubseteq \varphi(x_2)$, then φ is also called *coherent* (or monotone).

3.3. Finite degradation models

The models built over FDSs are called finite degradation models (FDMs).

Let $\mathbf{V}$ be a set of variables, $\mathbf{O}$ be a set of operators and $\alpha : \mathbf{O} \to \mathbb{N}$ be the arity of operators.

Definition 3.5: A *finite degradation model* (FDM) $\mathcal{M}$ is a set of equations written over $\langle \mathbf{V}, \mathbf{O}, \alpha \rangle$:

$$\mathcal{M} : \begin{cases} x_1 & := f_1 \\ x_2 & := f_2 \\ \dots & \quad \dots \\ x_m & := f_m \end{cases} \tag{2}$$

such that $m \geq 1, x_1, \dots, x_m \in \mathbf{V}$, and $f_1, \dots, f_m$ are formulas written over $\langle \mathbf{V}, \mathbf{O}, \alpha \rangle$

The set of formulas written over $\langle \mathbf{V}, \mathbf{O}, \alpha \rangle$ is defined as the smallest set such that:

- Any variable $v \in \mathbf{V}$ is a formula.
- If $\diamond \in \mathbf{O}$ is an operator such that $\alpha(\diamond) = n$ and $f_1, \dots, f_n$ are formulas, then $\diamond(f_1, \dots, f_n)$ is a formula.

Similar to the intermediate events and the basic events in fault trees, the variables in $\mathcal{M}$ are also divided into two kinds:

- *Flow variables*: the variables appearing in the left side of the equations, representing the states of a group of components or the state of subsystem/system;
- *State variables*: the variables appearing only in the right side of the equations, representing the states of bottom-level components whose valuation is regarded as the input of the model.

The set of state variables is denoted by $\mathbf{S}$ and the set of flow variables is denoted by $\mathbf{F}$. Then, $\mathbf{V} = \mathbf{S} \uplus \mathbf{F}$.

The interpretation of a FDM $\mathcal{M}$ is the following abstraction of FDSs:

$$\mathcal{M} : \bigotimes_{v_s \in \mathbf{S}} dom(v_s) \to \bigotimes_{v_f \in \mathbf{F}} dom(v_f) \tag{3}$$

This abstraction realises the mapping from the valuation of state variables to the valuation of flow variables. More explanations of FDMs and their modelling language FDS-ML can be found in our paper (Yang & Rauzy, 2019).

Take the model in Equation (1) as example.

There are eight state variables (*Pat*, *DB*, *MG*, *FF*, *SF*, *IED*, *Reg* and *CCTV*) and nine flow variables (*Doc*, *FSL*, *Exp*, *UIW*, *UIG*, *AW*, *AG*, *Attck*(*OR*) and *Attack*(*XOR*)). In the framework of FDSs, each of these 17 variables can be valued in the binary FDS **WF**, see Figure 2(a), i.e. $\forall\, v \in \mathbf{V}, \mathrm{dom}(v) = \mathbf{WF}$. Therefore, the model $\mathcal{M}$ in Equation (1) can be interpreted as the following abstraction of FDSs:

$$\mathcal{M} : (\mathbf{WF})^8 \to (\mathbf{WF})^9$$

where $(\mathbf{WF})^n$ stands for n times the monoidal product $\otimes$ of **WF**.

4. Automatic transformations of FDMs into epistemic space

The automatic transformation of FDMs is made up of two constitutive parts: the transformation of FDSs and the four transformations of operations on FDSs.

4.1. Transformation of FDSs

4.1.1. Formal definition

Definition 4.1: The transformation of FDSs is defined as the unary operation $(.)^u$: **FDS** $\to$ **FDS** such that $\forall\, \mathcal{L} : \langle \Theta, \sqsubseteq, \bot, p\rangle \in \mathbf{FDS}$, $(\mathcal{L})^u = \langle \Omega/_{\equiv}, \sqsubseteq, \{\bot\}, m\rangle$, where:

- $\Omega = 2^{\Theta}\backslash\{\emptyset\}$.
- $\forall\, S, T \in \Omega, S \sqsubseteq T \Leftrightarrow (\forall\, y \in T, \exists x \in S, x \sqsubseteq y) \wedge (\forall\, x \in S, \exists y \in T, x \sqsubseteq y)$.
- $\Omega/_{\equiv}$ is the quotient set of Ω by $\equiv$ (equivalence).
- $m : \Omega \to [0, 1]$ is a mass assignment on Ω satisfying $\sum_{X\in\Omega} m(X) = 1$.

Ω is called the epistemic space of Θ, which is the same as introduced Section 2.2. The elements in Ω are called *epistemic states*, which should be distinct with the (ordinary) states in Θ.

In the following part of this article, we shall use capital letters such as X, Y, Z, S and T to denote epistemic states, while use lowercase letters like x, y and s for (ordinary) states.

For any epistemic state $X \in \Omega$, if $|X| = 1$, i.e. there is only one possible value in X, we say that X is a certain (epistemic) state; otherwise, X is an uncertain (epistemic) state.

In the following sections, we will demonstrate that **FDS** is closed under the transformation $(.)^u$.

4.1.2. Degradation orders among epistemic states

As defined in Definition 4.1, any epistemic state $X \in \Omega$ is a non-empty subset of Θ. Therefore, comparing the degradation level of two epistemic states means to compare the degradation level of two subsets of Θ.

A traditional way is to assign each subset a real number as indicator and compare their magnitude. But the problem is that all real numbers are comparable, i.e. the partial orders in the transformed FDSs will be approximated into total (or linear) orders if using real numbers to make the comparison.

In order to solve this problem, we propose to directly use the degradation orders in $\mathcal{L}$ to define the degradation orders in $(\mathcal{L})^u$, see Definition 4.1.

For all $S, T \in \Omega$, the only case that S and T are comparable is that both of the two conditions $\forall\, y \in T, \exists x \in S, x \sqsubseteq y$ and $\forall\, x \in S, \exists y \in T, x \sqsubseteq y$ are satisfied. Otherwise, S and T are incomparable. These two conditions constrain both states in S and T and ensure the comparability of S and T.

In the following part of this section, we will use the three transformed FDSs: $(\mathbf{WF})^u$, $(\mathbf{WDF})^u$ and $(\mathbf{WFdFs})^u$, to explain the meaning of degradation orders among epistemic states defined in Definition 4.1.

These three transformed FDSs are pictured in Figure 4.

For $(\mathbf{WF})^u$, its epistemic space is $\Omega = 2^{\{W,F\}} \setminus \{\emptyset\} = \{\{W\}, \{F\}, \{W, F\}\}$ and the degradation orders among those epistemic states are $\{W\} \sqsubset \{W, F\} \sqsubset \{F\}$.

- $\{W\} \sqsubset \{W, F\}$ indicates that the epistemic state $\{W\}$ (i.e. the component's state is known to be working) is less degraded than the epistemic state $\{W, F\}$ (i.e. the component's state is unknown between W and F). The reason is that comparing to $\{W\}$, $\{W, F\}$ has an extra possibility to be in a more degraded state F.
- Similarly, $\{W, F\} \sqsubset \{F\}$ indicates that the degradation level of $\{W, F\}$ is lower than $\{F\}$ since comparing to $\{F\}$, $\{W, F\}$ has an extra possibility to be in a less degraded state W.

For $(\mathbf{WDF})^u$, $\Omega = 2^{\{W,D,F\}} \setminus \{\emptyset\} = \{\{W\}, \{D\}, \{F\}, \{W, D\}, \{D, F\}, \{W, F\}, \{W, D, F\}\}$. The degradation orders among those epistemic states can be found in Figure 4.

- The linear degradation orders $\{W\} \sqsubset \{W, D\} \sqsubset \{D\} \sqsubset \{F, D\} \sqsubset \{F\}$ and $\{W\} \sqsubset \{W, D\} \sqsubset \{W, F\} \equiv \{W, D, F\} \sqsubset \{F, D\} \sqsubset \{F\}$ can be understood in a similar way as those in $(\mathbf{WF})^u$.
- The equivalence $\{W, F\} \equiv \{W, D, F\}$ indicates that their degradation levels equivalent, although they are not equal.
- The incomparable pairs in $(\mathbf{WDF})^u$ are $\{D\} \sim \{W, F\}$ and $\{D\} \sim \{W, D, F\}$, since for those epistemic states the conditions in Definition 4.1 are not satisfied.

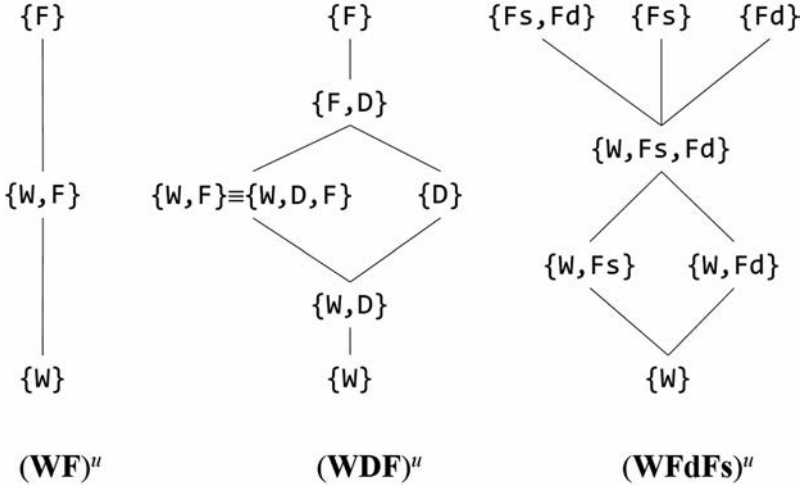

Figure 4. Graphical representation of $(\mathbf{WF})^u$, $(\mathbf{WDF})^u$ and $(\mathbf{WFdFs})^u$.

Mathematically, if $\exists X, Y \in \Omega$ such that $X \sqsubseteq Y$, $Y \sqsubseteq X$ and $X \neq Y$, then $X \equiv Y$. We can deduce from Definition 4.1 that the equivalence occurs only when there are more than three states ordered linearly.

Consider a chain $\mathcal{L}_C$ (i.e. a linearly ordered subset) of the FDS $\mathcal{L}$, such that $\mathcal{L}_C = \{\bot^c, x_1, \ldots, x_n, \top^c\}, n \geq 1$ and $\bot^c \sqsubset x_1 \sqsubset \cdots \sqsubset x_n \sqsubset \top^c$. $\bot^c$ and $\top^c$ are the two extreme elements of $\mathcal{L}_C$.

Then, we can deduce from Definition 4.1 that $\forall X \subseteq \mathcal{L}_C \backslash \{\bot^c, \top^c\}, X \neq \emptyset$:

$$\{\bot^c, \top^c\} \equiv \{\bot^c, \top^c\} \cup X$$

This equivalence means that if the two extremes $\bot^c$ and $\top^c$ are included in an epistemic state, then no matter how many intermediate states (i.e. in X) are included, the degradation level of $\{\bot^c, \top^c\} \cup X$ is bounded by $\{\bot^c, \top^c\}$.

It is worth noticing that the existence of equivalences makes the partial order $\sqsubseteq$ become a pre-order in Ω. In order to keep $\sqsubseteq$ being a partial order, the equivalent elements in Ω should be merged into quotients. Denote the quotient set of the equivalence $\equiv$ on the set Ω by $\Omega/_{\equiv}$. Then, $\sqsubseteq$ is a partial order over the quotients set $\Omega/_{\equiv}$ and it is easy to verify that $\{\bot\}$ is the least element of $\Omega/_{\equiv}$.

Therefore, the transformed result $(\mathcal{L})^u = \langle \Omega/_{\equiv}, \sqsubseteq, \{\bot\}, m \rangle$ in Definition 4.1 is still an FDS and **FDS** is closed under the transformation $(.)^u$.

(**WFdFs**)^u is the simplest case to understand the transformation of incomparable states. From Figure 4, we can see that:

- $\{W, F_1\} \sim \{W, F_2\}$, because they both have the possibility of being in the working state W and the possibility of being in one of the two incomparable failed states F_1 and F_2.
- $\{W, F_1\} \sqsubset \{W, F_1, F_2\}$ and $\{W, F_2\} \sqsubset \{W, F_1, F_2\}$, because compared to $\{W, F_1\}$ and $\{W, F_2\}$, $\{W, F_1, F_2\}$ has an extra possibility of being in another failed state. In other words, $\{W, F_1\}$ and $\{W, F_2\}$ mean that we know that one of the failed state can be excluded, while $\{W, F_1, F_2\}$ means that we know nothing about the object's state. Accordingly, $\{W, F_1, F_2\}$ has a higher degradation level than $\{W, F_1\}$ and $\{W, F_2\}$.
- $\{F_1\}$, $\{F_2\}$ and $\{F_1, F_2\}$ are all more degraded than $\{W, F_1, F_2\}$ for not having the possibility of being in the working state W.
- $\{F_1\} \sim \{F_2\} \sim \{F_1, F_2\}$, because in these three epistemic states the component is sure to be failed but the only difference is whether the failed state is certain (i.e. $\{F_1\}$ or $\{F_2\}$) or not (i.e. $\{F_1, F_2\}$). Comparing to $\{F_1\}$ and $\{F_2\}$, $\{F_1, F_2\}$ doesn't mean that there is an extra possibility of being in and extra failed state. Instead, it only means that the failed state is uncertain. Therefore, the degradation levels of these three epistemic states are considered to be incomparable.

4.1.3. Mass assignment

In epistemic space, the probability measure is not the probability of states but a subjective *belief* which measures the analysts' confidence on the occurrence of epistemic states.

The belief functions are introduced by Dempster (Dempster, 2008) and then reinforced by Shafer (Shafer, 1976). In the Dempster–Shafer theory, the allocation of belief (mass) functions to uncertain phenomena is called *basic belief assignment* (BBA) or

mass assignment. As in Definition 4.1, the mass assignment m is a function from Ω to $[0, 1]$ such that $\sum_{X\in\Omega} m(X) = 1$.

In practice, the mass assignment m is usually obtained by empirical data or expertise estimations. It cannot be directly deduced from the probability p since they are different measures of different phenomena. m is subjective while p is objective.

Given p and m, we say that p is *compatible* to m (and vice versa) if the following inequality holds $\forall\, s \in \Theta$:

$$0 \leq p(s) \leq \sum_{s\in X, X\in\Omega} m(X) \leq 1 \tag{4}$$

This inequality indicates that the 'real' probability $p(s)$ of being in the state s should not exceed the sum of mass of all epistemic states X containing s.

Table 4 gives a concrete example of the compatible m and p. In this table, the partial probability $p(s)|_X$ represents the allocation of the state probability $p(s)$ into each epistemic state X. For any state $s \in \Theta$, if $s \notin X$, then $p(s)|_X = 0$. Therefore, $\sum_{X\in\Omega} p(s)|_X = p(s)$ and the mass assignment $m(X)$ can be obtained by summing all the partial probabilities related to X, i.e. $\forall\, X \in \Omega$, $m(X) = \sum_{s\in\Theta} p(s)|_X$. It is easy to verify that the mass assignment m obtained in this way is compatible with p satisfying the inequality in Equation (4).

4.1.4. Probabilistic risk indicators

As mentioned in Section 4.1.3, we shall use those indicators in the Dempter–Shafer evidence theory, i.e. the belief and the plausibility, to quantify the occurrence possibility of epistemic states.

According to the Dempster–Shafer theory, the *belief* of an epistemic state $X \in \Omega$, denoted by $\mathbf{Bel}(X)$, can be calculated as follows:

$$\mathbf{Bel}(X) = \sum_{Y\in\Omega, Y\subseteq X} m(Y) \tag{5}$$

$\mathbf{Bel}(X)$ quantifies the mass of evidences supporting X.

In Shafer's original work, if $m(\emptyset) = 0$, m is called *normalised*.

Since ø is always excluded in Ω (see Definition 4.1), the mass assignment m in Ω is always normalised and we can deduce from Equation (5) that $\mathbf{Bel}(\Theta) = 1$.

The *plausibility* of an epistemic state $X \in \Omega$, denoted by $\mathbf{Pl}(X)$, quantifies the mass potentially supporting X, i.e.

$$\mathbf{Pl}(X) = \sum_{Y\in\Omega, Y\cap X\neq\emptyset} m(Y) \tag{6}$$

If m is normalised, then $\mathbf{Pl}(X) = 1 - \mathbf{Bel}(\Theta\backslash X)$.

Table 4. Mass assignment m in $(\mathbf{WDF})^u$ and a compatible probability measure p in **WDF**.

Epistemic states	X	$\{W\}$	$\{D\}$	$\{F\}$	$\{W, D\}$	$\{W, F\}$	$\{D, F\}$	$\{W, D, F\}$	Sum
Probability measure[a]	$p(W)\|_X$	0.5	–	–	0.1	0.05	–	0.05	0.7
	$p(D)\|_X$	–	0.15	–	0.03	–	0.01	0.01	0.2
	$p(F)\|_X$	–	–	0.08	–	0.005	0.01	0.005	0.1
Mass assignment	$m(X)$	0.5	0.15	0.08	0.13	0.055	0.02	0.065	1

[a] $p(s)|_X$ represents the allocation of $p(s)$ into each epistemic state X such that $\sum_{s\in X} p(s)|_X = p(s)$ and $p(s)|_X = 0$ if $x \notin X$.

Moreover, let P be a probability function such that $\forall X \in \Omega, P(X) = \sum_{s \in X} p(s)$. Then, the belief $\mathbf{Bel}(X)$ and the plausibility $\mathbf{Pl}(X)$ can be respectively seen as a lower bound and an upper bound of $P(X)$, i.e.

$$\mathbf{Bel}(X) \leq P(X) \leq \mathbf{Pl}(X)$$

The belief and the plausibility are indicators applied on the epistemic states in Ω. However, it is also of interest to have indicators applied on the states in Θ. Following this idea, we propose two new indicators, denoted by **Best** and **Worst**.

The mathematical definitions of **Best** and **Worst** are given as follows, i.e. $\forall s \in \Theta$:

$$\mathbf{Best}(s) \stackrel{def}{=} \sum_{X \in \Omega, \{s\} \sqsubseteq X} m(X) \tag{7}$$

$$\mathbf{Worst}(s) \stackrel{def}{=} \sum_{X \in \Omega, X \sqsubseteq \{s\}} m(X) \tag{8}$$

In sense of degradation processes, $\mathbf{Best}(s)$ can be understood as the quantification of the belief that the degradation level is in the best case to be s, while $\mathbf{Worst}(s)$ can be understood as the quantification of the belief that the degradation level is in the worst case to be s. These two indicators **Best** and **Worst** can be seen as alternatives of p to support the quantitative analysis on the states in Θ from the mass assignment m on Ω.

4.2. Transformation of operations

Let $\phi : \mathcal{A} \otimes \mathcal{B} \to \mathcal{C}$ be a binary operation where $\mathcal{A}, \mathcal{B} \in \mathbf{FDS}$ are the valuation domains of the two input arguments and $\mathcal{C} \in \mathbf{FDS}$ is the valuation domain of the output of ϕ.

When epistemic uncertainties are added to $\mathcal{A}$ and/or $\mathcal{B}$, they can then propagate to $\mathcal{C}$ through the operation ϕ. In order to formally define such propagation, we propose four transformations of ϕ with respect to the four different places where uncertainties can be added.

Definition 4.2: The *left*-transformation of ϕ is defined as follows:

$$\phi_L : (\mathcal{A})^u \otimes \mathcal{B} \to (\mathcal{C})^u$$

such that $\forall (X, y) \in (\mathcal{A})^u \otimes \mathcal{B}$,

$$\phi_L(X, y) = \{\phi(x, y) \mid x \in X\}. \tag{9}$$

Definition 4.3: The *right*-transformation of ϕ is defined as follows:

$$\phi_R : \mathcal{A} \otimes (\mathcal{B})^u \to (\mathcal{C})^u$$

such that $\forall (x, Y) \in \mathcal{A} \otimes (\mathcal{B})^u$,

$$\phi_R(x, Y) = \{\phi(x, y) \mid y \in Y\}. \tag{10}$$

The left- and right-transformations of ϕ define respectively the propagation of uncertainties from $\mathcal{A}$ and $\mathcal{B}$ to $\mathcal{C}$.

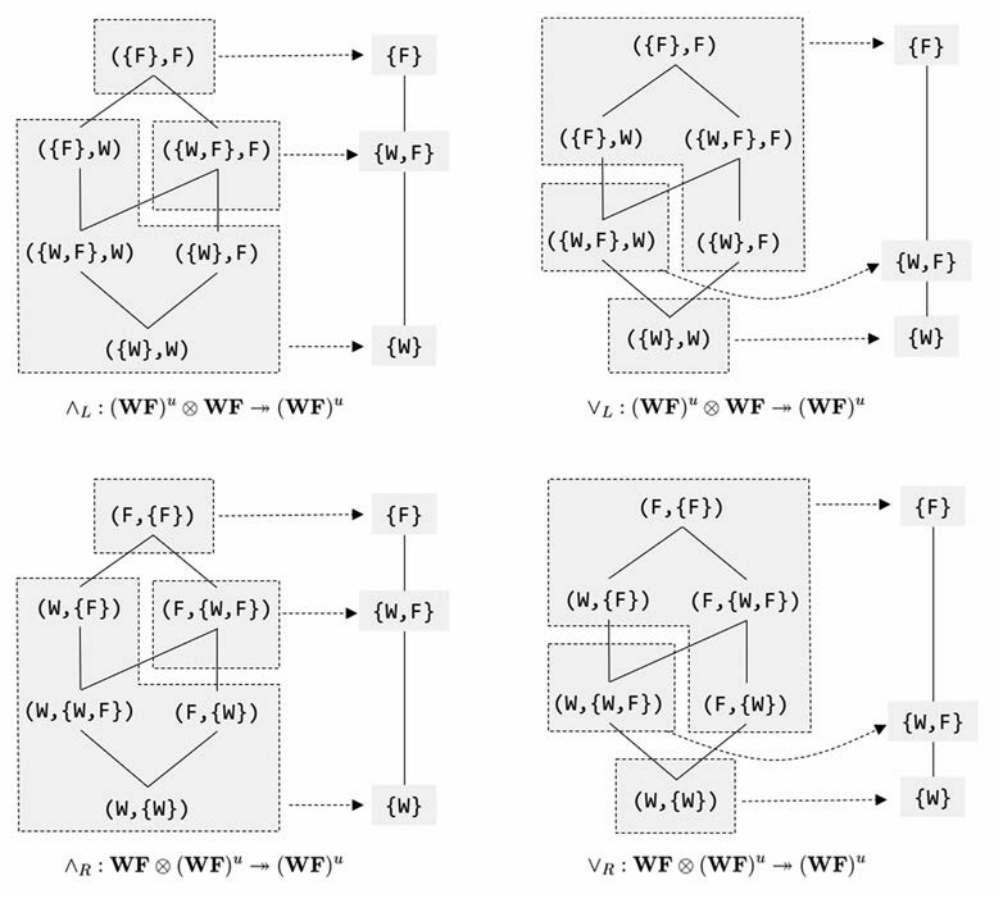

Figure 5. The left- and right-transformations of the disjunction $\vee$ and the conjunction $\wedge$.

Figure 5 shows graphically the left- and right-transformations of the disjunction $\vee$ and the conjunction $\wedge$.

Definition 4.4: The *inner*-transformation of ϕ is defined as follows:

$$\phi_u : (\mathcal{A})^u \otimes (\mathcal{B})^u \to (\mathcal{C})^u$$

such that $\forall\, (X, Y) \in (\mathcal{A})^u \otimes (\mathcal{B})^u$,

$$\phi_u(X, Y) = \{\phi(x, y) \mid x \in X, y \in Y\} \tag{11}$$

The inner-transformation ϕ_u can be seen as a composition of ϕ_L and ϕ_R.

Figure 6 shows graphically the inner-transformation of the logic disjunction $\vee$ and conjunction $\wedge$ operations. Comparing to Figure 5, the range of uncertain states in Figure 6 is augmented since uncertainties are introduced to both of the two input domains.

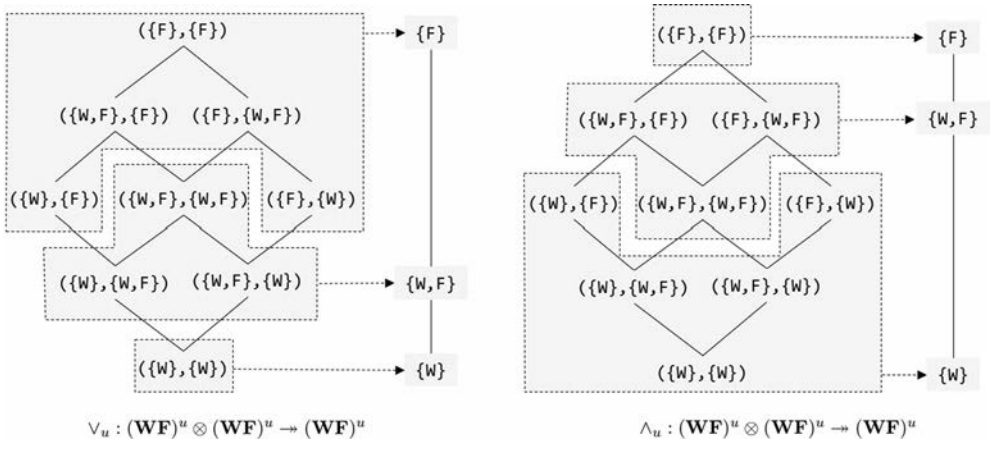

Figure 6. The inner-transformation of the disjunction $\vee$ and the conjunction $\wedge$.

Definition 4.5: The *outer*-transformation of ϕ is defined as follows:

$$\phi^u : (\mathcal{A} \otimes \mathcal{B})^u \to (\mathcal{C})^u$$

such that $\forall Z \in (\mathcal{A} \otimes \mathcal{B})^u$,

$$\phi^u(Z) = \{\phi(x,y) \mid (x,y) \in Z\} \tag{12}$$

The outer-transformation is applied to the case where the uncertainties are directly introduced to the composed state space $\mathcal{A} \otimes \mathcal{B}$.

Proposition 4.6: $\forall \mathcal{A}, \mathcal{B} \in$ **FDS**, *there exists a coherent abstraction* $\alpha_{\mathcal{AB}} : (\mathcal{A} \otimes \mathcal{B})^u \to (\mathcal{A})^u \otimes (\mathcal{B})^u$ *such that:*

- $\forall Z \in (\mathcal{A} \otimes \mathcal{B})^u, \alpha_{\mathcal{AB}}(Z) = (\{x \mid (x,y) \in Z\}, \{y \mid (x,y) \in Z\})$
- $\forall Z_1, Z_2 \in (\mathcal{A} \otimes \mathcal{B})^u, Z_1 \sqsubseteq Z_2 \Rightarrow \alpha_{\mathcal{AB}}(Z_1) \sqsubseteq \alpha_{\mathcal{AB}}(Z_2)$.

The proof of this proposition is given in Appendix.

The existence of $\alpha_{\mathcal{AB}}$ indicates that the abstraction level of $(\mathcal{A})^u \otimes (\mathcal{B})^u$ is, to some extent, higher than $(\mathcal{A} \otimes \mathcal{B})^u$.

Figure 7 pictures the coherent abstraction $\alpha_{\mathcal{AB}} : (\mathbf{WF} \otimes \mathbf{WF})^u \to (\mathbf{WF})^u \otimes (\mathbf{WF})^u$. In this figure, we can see that the epistemic states outside of the grey rectangle are one-to-one mapped from $(\mathbf{WF} \otimes \mathbf{WF})^u$ to $(\mathbf{WF})^u \otimes (\mathbf{WF})^u$. The seven epistemic states inside of the grey rectangle of $(\mathbf{WF} \otimes \mathbf{WF})^u$ are abstracted into only one epistemic state $(\{W,F\},\{W,F\})$ in $(\mathbf{WF})^u \otimes (\mathbf{WF})^u$.

We can also prove that the resulted operations ϕ_L, ϕ_R, ϕ_u and ϕ^u are also abstractions of FDSs satisfying Definition 3.4. Therefore, the framework of FDSs is closed under these four transformations $(.)_L$, $(.)_R$, $(.)_u$ and $(.)^u$.

To summarise, Table 5 compares the FDMs in state space and in epistemic space by comparing the formation of FDSs, operations and indicators.

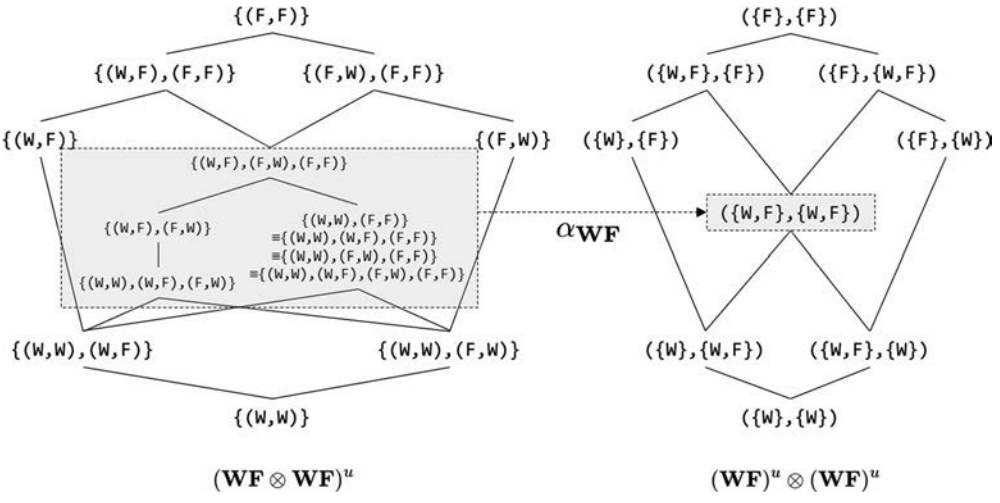

Figure 7. The coherent abstraction $\alpha_{\mathbf{WF}} : (\mathbf{WF} \otimes \mathbf{WF})^u \to (\mathbf{WF})^u \otimes (\mathbf{WF})^u$.

Table 5. Summary of FDMs in state space and in epistemic space.

	State space $\mathcal{L} : \langle \Theta, \sqsubseteq, \bot, p \rangle$	Epistemic space $(\mathcal{L})^u : \langle \Omega/_{\equiv}, \sqsubseteq, \bot^u, m \rangle$
Set	Θ	$\Omega = 2^{\Theta} \backslash \{\emptyset\}$
Element	State $s \in \Theta$	Epistemic state $X \subseteq \Theta$
Probability measure	$p(s)$: probability of being in s	$m(X)$: mass assignment of X
Degradation order $\sqsubseteq$	Partial order on Θ	Partial order on $\Omega/_{\equiv}$ (pre-order on Ω)
Least element	$\bot$	$\bot^u = \{\bot\}$
Operations	$\phi : \mathcal{A} \otimes \mathcal{B} \to \mathcal{C}$	$\phi_L : (\mathcal{A})^u \otimes \mathcal{B} \to (\mathcal{C})^u$ $\phi_R : \mathcal{A} \otimes (\mathcal{B})^u \to (\mathcal{C})^u$ $\phi_u : (\mathcal{A})^u \otimes (\mathcal{B})^u \to (\mathcal{C})^u$ $\phi^u : (\mathcal{A} \otimes \mathcal{B})^u \to (\mathcal{C})^u$ $\alpha_{\mathcal{AB}} : (\mathcal{A} \otimes \mathcal{B})^u \to (\mathcal{A})^u \otimes (\mathcal{B})^u$
Probabilistic indicators	$p : \Theta \to [0, 1]$ **Best** : $\Theta \to [0, 1]$ **Worst** : $\Theta \to [0, 1]$	$m : \Omega \to [0, 1]$ **Bel** : $\Omega \to [0, 1]$ **Pl** : $\Omega \to [0, 1]$

5. Reinterpretation of FDMs

The reinterpretation of FDMs is proceeded as follows:

- First, transform the domain of the variables where uncertainties should be added using the transformation $(.)^u$ in Definition 4.1.
- If probabilistic calculations are required, the mass assignment of each transformed FDS should be assigned as input of the calculation.
- Depending on the places where FDSs are transformed, use appropriate transformation (i.e. left-, right-, inner- or outer-transformation) for each related operation and declare it in the model.

In this section, we will use two cases as examples to explain the reinterpretation of FDMs. The mode in Equation (1) in Section 2.1 will be used as the original model of the two reinterpretations.

5.1. Case 1

In this case, all the eight state variables (i.e. *Pat*, *DB*, *MG*, *FF*, *SF*, *IED*, *Reg* and *CCTV*) in the model of Equation (1) are assumed to be epistemically uncertain, which is also the case analysed in Misuri et al. (2018).

Following the above procedure, the reinterpreted model $\mathcal{M}_1$ is written as follows:

$$\mathcal{M}_1 : \begin{cases} Attack(OR) := \vee_u(AG, AW) \\ Attack(XOR) := (\sqcup_{XOR})_u(AG, AW) \\ AG := \wedge_u(UIG, Exp) \\ AW := \wedge_u(UIW, Exp) \\ UIG := \wedge_u(\wedge_u(FSL, CCTV), SF) \\ UIW := \wedge_u(\wedge_u(CCTV, SF), Doc) \\ Exp := \wedge_u(IED, Reg) \\ FSL := \wedge_u(\vee_u(MG, FF), Pat) \\ Doc := \wedge_u(Pat, DB) \end{cases} \tag{13}$$

In this case, $\mathcal{M}_1$ is interpreted as the following abstraction:

$$\mathcal{M}_1 : ((\mathbf{WF})^u)^8 \rightarrow ((\mathbf{WF})^u)^9 \tag{14}$$

5.2. Case 2

Instead of adding epistemic uncertainties to all variables, sometimes only part of them need to be considered, such as components without monitoring devices or those whose uncertainty may bring significant impacts.

In this case, we randomly choose two variables: *Pat* and *Reg*, to add epistemic uncertainties while the other state variables remain certain. Following the same procedure, the reinterpreted model $\mathcal{M}_2$ is written as follows:

$$\mathcal{M}_2 : \begin{cases} Attack(OR) := \vee_u(AG, AW) \\ Attack(XOR) := (\sqcup_{XOR})_u(AG, AW) \\ AG := \wedge_u(UIG, Exp) \\ AW := \wedge_u(UIW, Exp) \\ UIG := \wedge_L(\wedge_L(FSL, CCTV), SF) \\ UIW := \wedge_R(\wedge(CCTV, SF), Doc) \\ Exp := \wedge_R(IED, (Reg)^u) \\ FSL := \wedge_R(\vee(MG, FF), (Pat)^u) \\ Doc := \wedge_L((Pat)^u, DB) \end{cases} \tag{15}$$

We can see that $\mathcal{M}_2$ contains both uncertain/certain components and operations. Since the framework of FDSs is closed under the transformations to epistemic space,

the interpretation of $\mathcal{M}_2$ is still an abstraction of FDSs, which is:

$$\mathcal{M}_2 : ((\mathbf{WF})^u)^2 \otimes (\mathbf{WF})^6 \to ((\mathbf{WF})^u)^9 \tag{16}$$

6. Assessment of FDMs and results

6.1. Scenarios and critical scenarios

The qualitative assessment of FDMs is proceeded by the scenarios analysis of given observer(s) in the FDM.

An observer of $\mathcal{M}$ is a predicate $w = Y$, where w is a flow variable in $\mathcal{M}$ and Y is an epistemic state in $\mathrm{dom}(w)$. The observer indicates the target variable and the target epistemic state of the current scenarios analysis.

In this section, the observers for case 1 and 2 are selected as $Attact(OR) = Y$ and $Attact(XOR) = Y$, where $Y \in \{\{W\}, \{W, F\}, \{F\}\}$.

Definition 6.1: Given an observer $w = Y$, we define the set of *scenarios* satisfying $w = Y$, denoted by $\mathbf{Sce}(w = Y)$, as follows:

$$\mathbf{Sce}(w = Y) \stackrel{def}{=} \left\{ \overline{\mathbf{v}} \;\middle|\; \overline{\mathbf{v}} \in \bigotimes_{v \in \mathbf{S}} \mathrm{dom}(v), \mathcal{M}_w(\overline{\mathbf{v}}) = Y \right\} \tag{17}$$

$\overline{\mathbf{v}}$ is called a state vector or a scenario in $\bigotimes_{v \in \mathbf{S}} \mathrm{dom}(v)$. $\mathcal{M}_w$ is the solution of w, i.e. the partial abstraction of $\mathcal{M}$ in Equation (3) such that $\mathcal{M}_w : \bigotimes_{v \in \mathbf{S}} \mathrm{dom}(v) \to \mathrm{dom}(w)$.

Definition 6.2: Given a set of scenarios $\mathbf{Sce}(w = Y)$, we define its set of *minimal* scenarios and set of *maximal* scenarios, denoted respectively by $\mathrm{Min}\mathbf{Sce}(w = Y)$ and $\mathrm{Max}\mathbf{Sce}(w = Y)$, as follows:

$$\begin{aligned} \mathrm{Min}\mathbf{Sce}(w = Y) &\stackrel{def}{=} \min(\mathbf{Sce}(w = Y)) \\ &= \{\overline{\mathbf{v}} \in \mathbf{Sce}(w = Y) \mid \nexists \overline{\mathbf{u}} \in \mathbf{Sce}(w = Y), \overline{\mathbf{u}} \sqsubset \overline{\mathbf{v}}\} \\ \mathrm{Max}\mathbf{Sce}(w = Y) &\stackrel{def}{=} \max(\mathbf{Sce}(w = Y)) \\ &= \{\overline{\mathbf{v}} \in \mathbf{Sce}(w = Y) \mid \nexists \overline{\mathbf{u}} \in \mathbf{Sce}(w = Y), \overline{\mathbf{v}} \sqsubset \overline{\mathbf{u}}\}. \end{aligned} \tag{18}$$

It is easy to prove that the notion of minimal scenarios generalises the notion of minimal cutsets while the notion of maximal scenarios generalises the notion of minimal path sets from FTA into FDSs.

For coherent systems, the minimal/maximal scenarios are the critical scenarios, from which any improvement/degradation will immediately leads to the improvement/degradation of the system's state.

The calculation of scenarios and critical scenarios is implemented by means of decision diagrams. The algorithms can be found in our papers (Rauzy & Yang, 2019a; Yang & Rauzy, 2019).

The calculation results for both case 1 and 2 are given in Table 6.

Table 6. Numbers of scenarios and critical scenarios for $\mathcal{M}_1$ and $\mathcal{M}_2$.

	$\mathcal{M}_1$			$\mathcal{M}_2$		
Y	$\{W\}$	$\{W,F\}$	$\{F\}$	$\{W\}$	$\{W,F\}$	$\{F\}$
$\lvert\mathbf{Sce}(Attack(OR)=Y)\rvert$	5729	813	19	548	21	7
$\lvert\mathrm{Min}\mathbf{Sce}(Attack(OR)=Y)\rvert$	1	3	3	1	3	3
$\lvert\mathrm{Max}\mathbf{Sce}(Attack(OR)=Y)\rvert$	6	6	1	6	2	1
$\lvert\mathbf{Sce}(Attack(XOR)=Y)\rvert$	5734	821	6	551	21	4
$\lvert\mathrm{Min}\mathbf{Sce}(Attack(XOR)=Y)\rvert$	1	3	3	1	3	3
$\lvert\mathrm{Max}\mathbf{Sce}(Attack(XOR)=Y)\rvert$	1	7	2	1	2	2

For case 1, we list the maximal scenarios of the observer $Attack(OR)=\{W\}$ and the minimal scenarios of the observer $Attack(OR)=\{F\}$ as follows:

$$\begin{aligned}\mathrm{Max}\mathbf{Sce}(Attack(OR)=\{W\}) = \{&(\{F\},\{F\},\{F\},\{F\},\{F\},\{F\},\{W\},\{F\}),\\ &(\{F\},\{F\},\{F\},\{F\},\{F\},\{W\},\{F\},\{F\}),\\ &(\{F\},\{F\},\{F\},\{F\},\{W\},\{F\},\{F\},\{F\}),\\ &(\{F\},\{F\},\{F\},\{W\},\{F\},\{F\},\{F\},\{F\}),\\ &(\{F\},\{F\},\{W\},\{F\},\{F\},\{F\},\{F\},\{F\}),\\ &(\{W\},\{W\},\{F\},\{F\},\{F\},\{F\},\{F\},\{W\})\}\\ \mathrm{Min}\mathbf{Sce}(Attack(OR)=\{F\}) = \{&(\{W\},\{W\},\{F\},\{F\},\{F\},\{F\},\{F\},\{F\}),\\ &(\{W\},\{F\},\{F\},\{F\},\{F\},\{F\},\{F\},\{W\}),\\ &(\{F\},\{W\},\{F\},\{F\},\{F\},\{F\},\{F\},\{W\})\}\end{aligned}$$

The valuation ordering of the variables in the above (as well as the following) scenarios is: $(MG, FF, Pat, CCTV, SF, IED, Reg, DB)$.

$\mathrm{Max}\mathbf{Sce}(Attack(OR)=\{W\})$ and $\mathrm{Min}\mathbf{Sce}(Attack(OR)=\{F\})$ are analogues of minimal path sets and minimal cutsets. The maximal scenarios in the former can be used to identify the most degraded situations that the system still remains in the certainly working state $\{W\}$ and the minimal scenarios in the latter can be used to identify the least degraded situations that the system already enters into the certainly failed state $\{F\}$.

As the solution $\mathcal{M}_{Attack(OR)}$ is coherent, we can deduce that any degradation of the scenarios in $\mathrm{Min}\mathbf{Sce}(Attack(OR)=\{W\})$ will degrade the system's state from $\{W\}$ to $\{W,F\}$ and any improvement of the scenarios in $\mathrm{Min}\mathbf{Sce}(Attack(OR)=\{F\})$ will improve the system's state from $\{F\}$ to $\{W,F\}$.

It is also of interest to perform the analysis on the observer $Attack(OR)=\{W,F\}$. For the sake of simplicity, $Attack(OR)=\{W,F\}$ is denoted by u.

The critical scenarios of u for cases 1 and 2 (subscripted by 1 and 2) are listed as follows:

$$\begin{aligned}\mathrm{Min}\mathbf{Sce}(u)_1 = \{&(\{W,F\},\{W\},\{W,F\},\{W,F\},\{W,F\},\{W,F\},\{W,F\},\{W\}),\\ &(\{W\},\{W,F\},\{W,F\},\{W,F\},\{W,F\},\{W,F\},\{W,F\},\{W\}),\\ &(\{W\},\{W\},\{W,F\},\{W,F\},\{W,F\},\{W,F\},\{W,F\},\{W,F\})\}\end{aligned}$$

$$\begin{aligned}
\text{Max}\mathbf{Sce}(u)_1 = \{&(\{F\},\{F\},\{W,F\},\{F\},\{F\},\{F\},\{F\},\{F\}),\\
&(\{F\},\{F\},\{F\},\{W,F\},\{F\},\{F\},\{F\},\{F\}),\\
&(\{F\},\{F\},\{F\},\{F\},\{W,F\},\{F\},\{F\},\{F\}),\\
&(\{F\},\{F\},\{F\},\{F\},\{F\},\{W,F\},\{F\},\{F\}),\\
&(\{F\},\{F\},\{F\},\{F\},\{F\},\{F\},\{W,F\},\{F\}),\\
&(\{W,F\},\{W,F\},\{F\},\{F\},\{F\},\{F\},\{F\},\{W,F\})\}\\
\text{Min}\mathbf{Sce}(u)_2 = \{&(W,W,\{W,F\},F,F,F,\{W,F\},F),\\
&(W,F,\{W,F\},F,F,F,\{W,F\},W),\\
&(F,W,\{W,F\},F,F,F,\{W,F\},W)\}\\
\text{Max}\mathbf{Sce}(u)_2 = \{&(F,F,\{F\},F,F,F,\{W,F\},F),\\
&(F,F,\{W,F\},F,F,F,\{F\},F)\}
\end{aligned}$$

We can see that the two scenarios in Max**Sce**$(u)_2$ are included in Max**Sce**$(u)_1$. The three scenarios in Min**Sce**$(u)_2$ are more degraded than the three scenarios in Min**Sce**$(u)_1$. These results show qualitatively that the range of uncertainties is enlarged from $\mathcal{M}_2$ to $\mathcal{M}_1$. This result is in accordance with the fact that we have more uncertain variables in $\mathcal{M}_1$ than in $\mathcal{M}_2$. This enlargement can also be observed from the number of scenarios and critical scenarios between $\mathcal{M}_2$ and $\mathcal{M}_1$ in Table 6.

It is worth emphasising here that although the case study used here is a Boolean system, the proposed modelling approach can also be applied to multistate systems that are modelled by multivalued operations other than $\vee$ and $\wedge$.

6.2. Probabilistic indicators

To calculate the proposed indicators **Bel**, **Pl**, **Best** and **Worst** defined in Section 4.1.4, we should first calculate the mass assignment in the domain of the target flow variable w.

According to Definitions 3.1 and 3.4, the mass assignment m in the valuation domain of any flow variable w of the model can be calculated as follows, i.e. $\forall\ Y \in \text{dom}(w)$:

$$m(Y) \overset{def}{=} \sum_{\overline{\mathbf{v}} \in \mathbf{Sce}(w=Y)} m(\overline{\mathbf{v}}) = \sum_{\overline{\mathbf{v}} \in \mathbf{Sce}(w=Y)} \left(\prod_{i=1}^{n} m_i(X_i) \right) \tag{19}$$

m_i is the mass assignment in the domain of the ith state variable in $\bigotimes_{v \in \mathbf{S}} \text{dom}(v)$, which should be given as input of the calculation.

Table 7 gives the mass assignments for the eight state variables in Equation (1), which are extracted from Misuri et al. (2018). To support the calculation for case 2, we also propose a compatible probability measure p on the state spaces of the eight state variables in Table 8.

The calculation of Equation (19) relies on the results of the set of scenarios **Sce**$(w = Y)$. As mentioned in Section 6.1, the sets of scenarios are calculated by

Table 7. Mass assignments on the epistemic space $(\mathbf{WF})^u$ of the eight state variables of the model in Equation (1).

State variables	MG	FF	Pat	DB	CCTV	SF	IED	Reg
$m(\{W\})$	0.8	0.6	0.7	0.7	0.7	0.6	0.2	0.5
$m(\{W,F\})$	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
$m(\{F\})$	0.1	0.3	0.2	0.2	0.2	0.3	0.7	0.4

Table 8. Compatible probability measure on the state space **WF** of the eight state variables of the model in Equation (1).

State variables	MG	FF	Pat	DB	CCTV	SF	IED	Reg
$p(W)$	0.85	0.65	0.75	0.75	0.75	0.65	0.25	0.55
$p(F)$	0.15	0.35	0.25	0.25	0.25	0.35	0.75	0.45

Table 9. Results of **Bel**, **Pl**, **Best** and **Worst** of the observers $Attack(OR) = Y$ and $Attack(XOR) = Y$ for case 1 and 2.

	$\mathcal{M}_1$		$\mathcal{M}_2$	
	$Attack(OR)$	$Attack(XOR)$	$Attack(OR)$	$Attack(XOR)$
$m(\{W\})$	9.904×10^{-1}	9.906×10^{-1}	9.942×10^{-1}	9.948×10^{-1}
$m(\{W,F\})$	7.895×10^{-3}	8.12×10^{-3}	2.69×10^{-3}	2.69×10^{-3}
$m(\{F\})$	1.667×10^{-3}	1.193×10^{-3}	3.075×10^{-3}	2.487×10^{-3}
Bel$(\{W\})$	9.904×10^{-1}	9.906×10^{-1}	9.942×10^{-1}	9.948×10^{-1}
Bel$(\{W,F\})$	1.000	1.000	1.000	1.000
Bel$(\{F\})$	1.667×10^{-3}	1.193×10^{-3}	3.075×10^{-3}	2.487×10^{-3}
Pl$(\{W\})$	9.983×10^{-1}	9.987×10^{-1}	9.969×10^{-1}	9.975×10^{-1}
Pl$(\{W,F\})$	1.000	1.000	1.000	1.000
Pl$(\{F\})$	9.562×10^{-3}	9.313×10^{-3}	5.765×10^{-3}	5.177×10^{-3}
Best(W)	1.000	1.000	1.000	1.000
Best(F)	1.667×10^{-3}	1.193×10^{-3}	3.075×10^{-3}	2.487×10^{-3}
Worst(W)	9.904×10^{-1}	9.906×10^{-1}	9.942×10^{-1}	9.948×10^{-1}
Worst(F)	1.000	1.000	1.000	1.000

means of decision diagrams. The calculation algorithms can be found in Yang and Rauzy (2019).

Once the mass assignment is obtained, the four indicators **Bel**, **Pl**, **Best** and **Worst** can be calculated according to the formulas defined in Section 4.1.4.

The results of the mass assignment in the domain of the two flow variables $Attack(OR)$ and $Attack(XOR)$ for both case 1 and 2 are given in Table 9. These results are in accordance with those calculated in Misuri et al. (2018). The results of the four indicators **Bel**, **Pl**, **Best** and **Worst** are also given in Table 9.

To be more comparative, we picture the mass assignment of $Attack(OR)$ and $Attack(XOR)$ in Figure 8. From this figure, we can clearly see the enlargement of range of uncertainties from $\mathcal{M}_2$ to $\mathcal{M}_1$.

7. Conclusion

In this article, we present a new approach of modelling epistemic uncertainties in degradation processes. This approach is established in the framework of finite

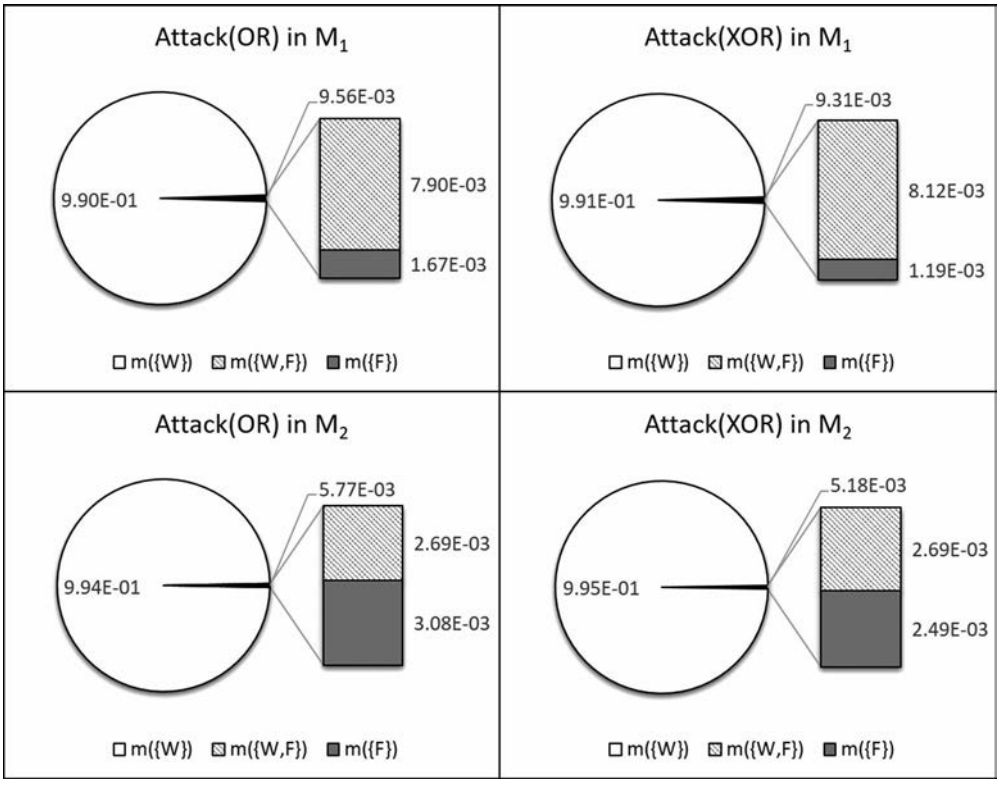

Figure 8. The mass assignment in the domain of *Attack*(*OR*) and *Attack*(*XOR*) for cases 1 and 2.

degradation structures (FDSs), which is recently proposed by the authors and can be seen as a formal extension of the fault tree analysis into multistate systems.

In the framework of FDSs, the state spaces of components are modelled by FDSs and the failure mechanisms of the system are modelled by operations on FDSs. When the states of components become epistemically uncertain, we transform their corresponding FDSs into epistemic space using the unary operation $(.)^u$ and transform related operations using the left-, right-, inner- and outer transformations. These transformations are mathematically defined and can be done automatically for all FDSs and for all operations on FDSs. Compared to the manual adaptations used in the state-of-the-art literature, these automatic transformations are more efficient, less error-prone and more generic. Moreover, both uncertain and certain components and operations can be modelled and assessed uniformly in one finite degradation model since we have proven that the framework of FDSs is closed under the proposed transformations. As assessment results, the uncertainty-embedded (critical) scenarios and probabilistic indicators such as belief, plausibility, **Best** and **Worst** can be calculated to support the required reliability and safety analysis.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Liu Yang http://orcid.org/0000-0002-8106-6866
Antoine Rauzy http://orcid.org/0000-0003-0926-5286

References

Bjerring, J. (2014). Problems in epistemic space. *Journal of Philosophical Logic*, *43*(1), 153–170. https://doi.org/10.1007/s10992-012-9257-z

Dempster, A. P. (2008). Upper and lower probabilities induced by a multivalued mapping. *The Annals of Mathematical Statistics*, *38*(2), 325–339. https://doi.org/10.1214/aoms/1177698950

Helton, J. C., & Burmaster, D. E. (1996). Guest editorial: Treatment of aleatory and epistemic uncertainty in performance assessments for complex systems. *Reliability Engineering and System Safety*, *54*, 91–94. https://doi.org/10.1016/S0951-8320(96)00066-X

Levitin, G. (2005). *The universal generating function in reliability analysis and optimization*. Springer series in reliability engineering. Springer.

Misuri, A., Khakzad, N., Reniers, G., & Cozzani, V. (2018). Tackling uncertainty in security assessment of critical infrastructures: Dempster–Shafer theory vs. credal sets theory. *Safety Science*, *107*, 62–76. https://doi.org/10.1016/j.ssci.2018.04.007

Nakahara, H., Jinguji, A., Sato, S., & Sasao, T. (2017). A random forest using a multi-valued decision diagram on an FPGA. In *2017 IEEE 47th international symposium on multiple-valued logic (ISMVL)* (pp. 266–271), IEEE.

Parry, G. W. (1996). The characterization of uncertainty in probabilistic risk assessments of complex systems. *Reliability Engineering and System Safety*, *54*, 119–126. https://doi.org/10.1016/S0951-8320(96)00069-5

Rauzy, A. (2001). Mathematical foundations of minimal cutsets. *IEEE Transactions on Reliability*, *50*(4), 389–396. https://doi.org/10.1109/24.983400

Rauzy, A. (2008). Guarded transition systems: A new states/events formalism for reliability studies. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *222*(4), 495–505. https://doi.org/10.1243/09544054JEM822

Rauzy, A. (2018). Notes on computational uncertainties in probabilistic risk/safety assessment. *Entropy*, *20*(3), 162. https://doi.org/10.3390/e20030162

Rauzy, A., & Yang, L. (2019a). Decision diagram algorithms to extract minimal cutsets of finite degradation models. *Information*, *10*(12), 368. https://doi.org/10.3390/info10120368

Rauzy, A., & Yang, L. (2019b). Finite degradation structures. *FLAP*, *6*(6), 1447–1474.

Ruijters, E., & Stoelinga, M. (2015). Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer Science Review*, *15–16*(C), 29–62. https://doi.org/10.1016/j.cosrev.2015.03.001

Salicone, S. (2007). *Measurement uncertainty: An approach via the mathematical theory of evidence*. Springer series in reliability engineering, Springer.

Shafer, G. (1976). *A mathematical theory of evidence*. Princeton University Press.

Ushakov, I. (2012). Multistate systems. In *Probabilistic reliability models* (pp. 169–193). John Wiley & Sons.

Yang, L., & Rauzy, A. (2018). Reliability modeling using finite degradation structures. In *2018 3rd International conference on system reliability and safety (ICSRS)* (pp. 168–175). IEEE.

Yang, L., & Rauzy, A. (2019). FDS-ML: A new modeling framework for probabilistic risk and safety analyses. In *International symposium on model-based safety and assessment (IMBSA)* (pp. 78–92). Springer.

Zadeh, L. (1965). Fuzzy sets. *Information and Control*, *8*(3), 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X

Zadeh, L. (1999). Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems*, *100*(1), 9–34. https://doi.org/10.1016/S0165-0114(99)80004-9

Zaitseva, E., & Levashenko, V. (2017). Reliability analysis of multi-state system with application of multiple-valued logic. *The International Journal of Quality & Reliability Management*, *34*(6), 862–878. https://doi.org/10.1108/IJQRM-06-2016-0081

Zhai, Q., Xing, L., Peng, R., & Yang, J. (2015). Multi-valued decision diagram-based reliability analysis of *k*-out-of-*n* cold standby systems subject to scheduled backups. *IEEE Transactions on Reliability*, *64*(4), 1310–1324. https://doi.org/10.1109/TR.2015.2404891

Appendix. Proofs

Proof: First, we prove that $\alpha_{\mathcal{AB}}$ is surjective.

$\forall\,(X,Y) \in (\mathcal{A})^u \otimes (\mathcal{B})^u$, we define that $Z = \{(x,y) \mid x \in X, y \in Y\}$. It is obvious that $Z \subseteq \mathcal{A} \otimes \mathcal{B}$ so that $Z \in (\mathcal{A} \otimes \mathcal{B})^u$. By definition, we have $\alpha_{\mathcal{AB}}(Z) = (X,Y)$, which implicates that $\alpha_{\mathcal{AB}}$ is surjective.

Second, we prove that $\alpha_{\mathcal{AB}}$ is monotone.

$\forall\, X, Y \in (\mathcal{A} \otimes \mathcal{B})^u$, if $X \sqsubseteq Y$, according to Definition 4.1, we have

$$X \sqsubseteq Y \Leftrightarrow \begin{cases} \forall\,(a,b) \in X, \exists (c,d) \in Y \text{s.t.} a \sqsubseteq c, b \sqsubseteq d \\ \forall\,(c,d) \in Y, \exists (a,b) \in X \text{s.t.} a \sqsubseteq c, b \sqsubseteq d. \end{cases}$$

Let $R_1 = \{x \mid (x,y) \in X\}$, $R_2 = \{y \mid (x,y) \in X\}$, $R_3 = \{x \mid (x,y) \in Y\}$, $R_4 = \{y \mid (x,y) \in Y\}$. Then, we can decompose the above propositions as follows:

$$X \sqsubseteq Y \Leftrightarrow \begin{cases} \forall\, a \in R_1, \exists c \in R_3, a \sqsubseteq c \\ \forall\, c \in R_3, \exists a \in R_1, a \sqsubseteq c \\ \forall\, b \in R_2, \exists d \in R_4, b \sqsubseteq d \\ \forall\, d \in R_4, \exists b \in R_2, b \sqsubseteq d \end{cases}$$

$$\Leftrightarrow \begin{cases} R_1 \sqsubseteq R_3 \\ R_2 \sqsubseteq R_4. \end{cases}$$

According to the definition of $\alpha_{\mathcal{AB}}$, we have $\alpha_{\mathcal{AB}}(X) = (R_1, R_2)$ and $\alpha_{\mathcal{AB}}(Y) = (R_3, R_4)$, $(R_1,R_2), (R_3,R_4) \in (\mathcal{A})^u \otimes (\mathcal{B})^u$. Together with $R_1 \sqsubseteq R_3$ and $R_2 \sqsubseteq R_4$, we can deduce that $\alpha_{\mathcal{AB}}(X) \sqsubseteq \alpha_{\mathcal{AB}}(Y)$, i.e. $\alpha_{\mathcal{AB}}$ is monotone. ■