Safety Case Confidence Propagation Based on Dempster-Shafer theory

Rui Wang, Jérémie Guiochet, Gilles Motet, Walter Schön

Safety Case Confidence Propagation Based on Dempster-Shafer theory

Rui Wang[a,b], Jérémie Guiochet[a,*], Gilles Motet[a], Walter Schön[c]

[a] *LAAS-CNRS, Université de Toulouse, CNRS, INSA,UPS, Toulouse, France*
[b] *School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China*
[c] *Sorbonne Universités, Université de Technologie de Compiègne, Heudiasyc UMR CNRS 7253 CS 60319 Compiègne Cedex France*

Abstract

Safety arguments, also called safety cases, are commonly used to demonstrate that adequate efforts have been made to achieve safety goals. Assessing the confidence of such arguments and decision-making is usually done manually and is heavily dependent on subjective expertise. Therefore, there is an urgent need for an approach that can assess confidence in the arguments in order to support decision-making. We therefore propose a quantitative approach, based on Dempster-Shafer (D-S) theory, to formalize and propagate confidence in safety cases. Goal Structuring Notation is adopted. The proposed approach focuses on the following issues regarding argumentation assessment: 1) formal definitions of confidence measures based on belief functions from D-S theory; and 2) the development of confidence aggregation rules for structured safety arguments with the help of Dempster's rule. Definitions of confidence measures and aggregation rules are deduced for single, double, and n-node arguments. Finally, a sensitivity analysis of aggregation rules is used to preliminarily validate this approach.

Keywords:
safety case, safety argumentation, confidence assessment, Dempster-Shafer theory, evidence combination

*Corresponding authors, jeremie.guiochet@laas.fr

1. Introduction

In safety-critical domains, such as aeronautics, railways, or the automotive sector, a structured *safety argument* is often used to justify sufficient confidence in system safety (safety is defined as *freedom from unacceptable risk* in ISO/IEC-Guide51 (1999)). Currently, although most safety arguments are textual, there is a growing trend for graphical notations, and establishing an evidence-based argument is already a requirement in various industrial sectors. A safety argument consists of a top statement to be justified (e.g., "{system X} is acceptably safe" or "the failure rate of {system X} is less than 10^{-9}"). Nevertheless, issues arise when assessing a safety argument that is based on extensive documentary evidence, especially for computing systems. In practice, a regulatory body decides on the acceptability of the statement, and their decision is based on their confidence in the argument. The available arguments do not provide such confidence directly, and judgments rely heavily on subjective expertise. Thus, an approach is needed that can make explicit and measure confidence in the safety argument, and can take into account the following challenges:

- Confidence definition

  Clarifying the concept of confidence in a safety argument is clearly important. Uncertainties exist in the argument intended to demonstrate the system safety. Confidence can be derived from measuring these uncertainties. For instance, an uncertainty may relate to the degree of belief in a supporting evidence.It could also be the extent of the contribution of an evidence to the top claim. Moreover, compared to pure hardware uncertainties expressed with probabilities (usually calculated with objective measures), the assessment of uncertainties in an argument done by experts is often subjective. Thus, a suitable uncertainty theory is necessary for a formal definition of the confidence placed in an argument.

- Aggregation rules

  Aggregation rules are essential for propagating confidence in an argument. Confidence varies depending on the independent and combined contributions of different supporting premises, which relate to different argument types. Several premises that relate to the same top statement can be complementary or redundant. Hence, this should be considered when developing aggregation rules. Similarly, the choice of the mathematical method for merging confidence measures is crucial.

In this paper, we propose a quantitative approach to formalize and propagate confidence in the safety argument. This approach is based on Dempster-Shafer uncertainty theory (D-S theory). Goal Structuring Notation (GSN) is used to demonstrate the argument's structure. First, we formally define confidence measures for safety arguments using belief functions. Then, we derive confidence propagation rules using Dempster's rule. These definitions and aggregation rules are developed for both single, double-, and n-node arguments. We carry out a sensitivity analysis to observe the behaviors of aggregation rules. Our previous work (Wang et al., 2017, 2018) proposed a practical framework for safety argument assessment. This paper is a theoretical extension and a complete rework of a first version (Wang et al., 2016). New inference types and associated propagation rules are introduced, along with a detailed derivation procedure.

This paper is organized as follows. In Section 2, we introduce the structuring notation, types and uncertainty sources for safety cases. In Sections 3 and 4, formal definitions of confidence measures for arguments are proposed for single and double-node arguments, respectively. Then, we aggregate these measures consistently using D-S theory. In Section 5, aggregation rules are generalized for n-node arguments. We discuss related work and draw some conclusions in the last two sections.

2. Background

In this section, we introduce the relevant background knowledge. We start with the concept of the safety case and its method. Then, the argument types proposed in literature are presented. Finally, we discuss uncertainties that can be present in an argument.

2.1. Structured safety argument

Structured arguments play an important role in communicating a system's attributes with various names: safety case (Kelly and Weaver, 2004; Bishop and Bloomfield, 1998), assurance case (Bloomfield et al., 2006), trust case (Cyra and Gorski, 2007), dependability case (Bloomfield et al., 2007), etc. Of these, the concept of safety case has already been adopted in various safety-critical sectors. It is generally considered as "a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment" (Bishop and Bloomfield, 1998). The development of the safety case is a common way to demonstrate system safety. In several sectors, regulations require developing a safety case and some regulatory bodies explicitly require building safety assurance arguments (automotive (ISO26262, 2011), railway (EN50129, 2003),

defense (EN50129, 2003), software engineering (ISO/IEC15026-2, 2011), etc.). The Object Management Group (OMG, 2018) recently proposed a method to establish a meta-model for safety arguments.

Safety cases can be documented with plain text, which can be a flexible way to express arguments. However, the quality of such arguments is closely linked to how the argument is organized. Kelly (1998) points out that proficiency in the written language impacts the expression of arguments, and unclear semantics may introduce ambiguity. To structure the argumentation, Toulmin (1969) proposed a model including six distinctive elements: *claim, data, warrant, qualifier, rebuttal and backing*.

Based on Toulmin's model, Kelly (1998) put forward a notation specifically designed for the safety case, called Goal Structuring Notation (GSN), which helps to make the presentation of an argument more readable and adaptable. The notation aims to break down the top goal into sub-goals until there is evidence to support them. The main elements of GSN are presented in an example (Figure 1) and listed below. This safety argument fragment is derived from the Hazard Avoidance Pattern (Kelly and McDermid, 1997).

- *Goal*: the goal refers to claims regarding system design, implementation, operation or maintenance. For instance, a goal can be "G1: {System X} is acceptably safe".

- *Solution*: this refers to available information that directly supports a goal. Solutions may include all forms of evidence. For example, they can be test results, verification reports, fault trees, etc.

- *Strategy*: the description of how to decompose the goal. This always appears between parent and child goals. For instance, in Figure 1, strategy S1 shows how goal G1 is inferred from sub-goals.

- *Context*: a reference to contextual information, or a statement of contextual information. It can be related to a goal, a strategy or a solution.

These terms proposed in GSN may not always fit with other approaches. Actually, in the safety case community, alternative terminology exists, such as *claim-argument-evidence* from ASCE tool (Bishop and Bloomfield, 1998), *claim-artifact* from SACM (OMG, 2018) or *claim-evidence* from (ISO/IEC15026-2, 2011). When we refer to a GSN diagram we will use its terminology (Goal / Solution), but in other case we will use Claim/Evidence terms which are more generic in argumentation.

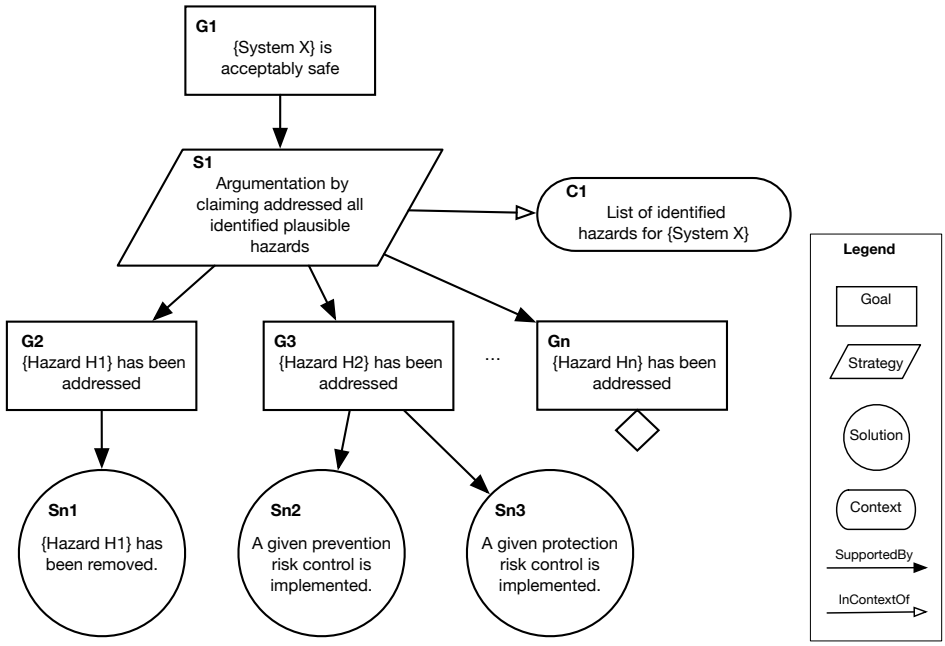


Figure 1: GSN example adapted from the Hazard Avoidance Pattern (Kelly and McDermid, 1997)

2.2. Argument types

For complex arguments in which the derivation of the conclusion (top statement) from premises is not obvious, Govier (2013) emphasized the importance of structuring arguments into argument types. A clear argument structure distinguishes the way premises contribute to the conclusion. The argument type helps to understand the line of reasoning underlying an argument, which significantly impacts its evaluation.

Given the cooperative contribution of premises, a graphical notation is used to show different argument structures (Figure 2). Premises and conclusions are not distinguished. In Figure 2, ① and ② are premises while ③ represents the conclusion. Three basic argument types (called argument patterns by Govier (2013)) are proposed for arguments with two or more premises:

1) *Linear sequential*: Premises support the conclusion in sequence. In 1) of Figure 2, ② is deduced from ①; and ③ is deduced from ②. Both premises are necessary to obtain the conclusion.
2) *Linked support*: Premises must be linked to support the conclusion. No conclusion can be deduced if one of the premises is missing. In 2) of Figure 2, both premises ① and ② are needed for conclusion ③. The falseness of either premise leads to the rejection of the conclusion based on this argument.

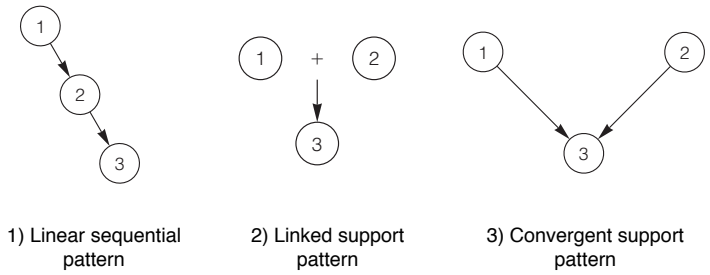


Figure 2: Govier (2013)'s three argument types

3) *Convergent support*: In contrast with the *linked support* argument, each premise of a *convergent support* argument contributes to the conclusion. In 3) of Figure 2, either premise ① or ② can support the conclusion ③. If one of the premises is false, the other is able to support it ③. The truth of both premises increases confidence in the conclusion, due to the fact that more dimensions of the topic are considered.

2.3. Sources of uncertainty in an argument

To assess confidence, we need to identify the potential uncertainties in the arguments. Taking a simple GSN safety argument as an example (shown in Figure 3): the top goal *A:* {*System X*} *is acceptably safe* is supported by the sub-goal *Tests are conclusive*. Two sources of uncertainties are identified, which are noted:

- Uncertainty in the fact that B is True

  For instance, do we consider that *Tests are conclusive* is true? We may doubt this claim after evaluating associated evidences (which are not presented here, but could be demonstration of test input coverage for instance). We propose to use the term *trustworthiness*, which assesses the degree of belief in claim B.The definition of the trustworthiness is universal for all claims, and is introduced in the following section (Section 3.1).

- Uncertainty in the fact that B effectively supports A

  For instance, is *Tests are conclusive* sufficient to support the claim {*System X*} *is acceptably safe*? We may doubt the extent to which claim A can be deduced from claim B. We add another property, named *appropriateness*, to estimate the degree of belief in the inference. The definitions of the appropriateness depend on the argument structures and they are introduced in Sections 3 and 4, respectively.

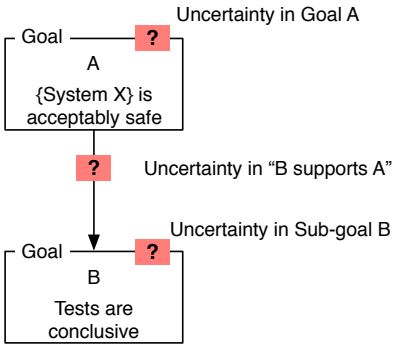


Figure 3: Sources of uncertainties in a simple inference modelled with GSN

3. Confidence propagation for a single argument

In this section, we formally define the two properties, appropriateness and trustworthiness, as confidence measures (Section 3.1). Then, we propose an approach for a single argument (linear sequential or one-node) to propagate confidence to the top goal in a safety case using these two factors

3.1. Formal definition of trustworthiness and appropriateness

A goal, in GSN, is expressed by a claim (e.g., "Tests are conclusive"). Here, the assessment of the trustworthiness of a goal is generally studied by focusing on a statement. Let us consider, for instance, the statement A "{System X} is acceptably safe". The frame of discernment Ω_A for the truth of A is binary: $\{A, \overline{A}\}$ or {True, False}.

The adoption of D-S theory, instead of classic probabilistic theory, in our approach aims to explicitly measure the uncertainty. There is a consensus that the probabilistic theory is suffering from some issues. For example, equal probabilities are always used to show the total ignorance (0.5 to win or lose the toss). The universe set of the possible results is $\Omega = \{x, \bar{x}\}$. The probabilities of x, $\bar{x}$ are $p(x) = p(\bar{x}) = 0.5$. These probabilities can be interpreted as we have no information at all for the event X; or it can be explained as there is an equal distribution. Dempster (2008) also explains the importance to *allow probabilities of "don't know"*, and introduces the same triple (p,q,r) associated with an assertion, where p and q represent respectively the probabilities "for" and "against" the assertion, and r is the probability of "don't know".

In D-S theory, the mass function of set A reflects the degree of belief in the truth of A, denoted as $m^{\Omega_A}(\{A\})$. Hence, the trustworthiness of a statement is formalized through assigning the mass function to sets representing the *belief*, *uncertainty*, and

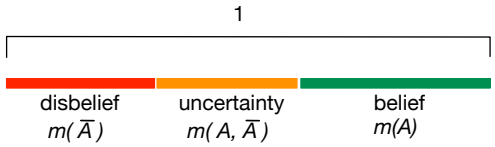


Figure 4: The measures of truth of statement A with D-S theory

disbelief. An opinion of the truth of this statement can be explicitly expressed with three masses represented in Figure 4. These measures are:

$$\begin{aligned}
&\textit{Belief in the statement } A\text{:} \quad bel_A = m^{\Omega_A}(\{A\}),\\
&\textit{Disbelief in the statement } A\text{:} \quad disb_A = m^{\Omega_A}(\{\overline{A}\}),\\
&\textit{Uncertainty in the statement } A\text{:} \quad uncer_A = m^{\Omega_A}(\{A, \overline{A}\}).
\end{aligned}$$

According to the mass function constraint, we have $m(\{A\})+m(\{\overline{A}\})+m(\{A, \overline{A}\}) = 1$, i.e., *belief + disbelief + uncertainty = 1*. Hence, we define the trustworthiness of statement of goal A based on the belief function and the mass function of D-S theory:

Definition 3.1. *The trustworthiness of the statement of goal A is a three-tuple* $trust_A = (bel_A, uncer_A, disb_A)$*:*

$$trust_A \begin{cases} bel_A \;\; = bel^{\Omega_A}(\{A\}) = m^{\Omega_A}(\{A\}) \\ disb_A \;\; = bel^{\Omega_A}(\{\overline{A}\}) = m^{\Omega_A}(\{\overline{A}\}) \\ uncer_A \;\; = m^{\Omega_A}(\{A, \overline{A}\}) = 1 - m^{\Omega_A}(\{A\}) - m^{\Omega_A}(\{\overline{A}\}) \end{cases} \tag{1}$$

where bel_A, $disb_A$, $uncer_A \in [0, 1]$. bel_A, $disb_A$ and $uncer_A$ denote the degree of our belief in, disbelief in or doubt about statement A. If $A = \{System\ X\}$ *is acceptably safe*, it depends on, for instance, the completeness of the test sequence, the correctness of the test results, the clarity of the evidence, the competence of engineers, etc.

In Figure 5, we represent the trustworthiness of goal A $(bel_A, uncer_A, disb_A)$ with a black rectangle.

As introduced in Section 2.3, appropriateness is used to evaluate inferences from child to parent goals. In Figure 6, the top goal is supported by n sub-goals: G1-Gn. Appropriateness measures are annotated to the arrows linking them. We propose three appropriateness factors that may influence the propagation of trustworthiness from sub-goals to the top-goal:

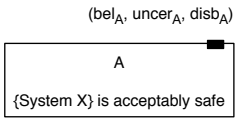


Figure 5: Goal A annotated with trustworthiness measures

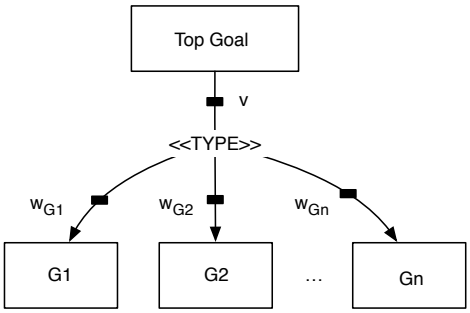


Figure 6: An argument annotated with appropriateness measures

- The *contributing weight* of each sub-goal, $w_{G1}, w_{G2}, ..., w_{Gn}$. As the name indicates, this weight is used to measure the degree of the contribution of each sub-goal to the top goal.
- The cooperative contribution of sub-goals; this is called the *argument type* and is annotated with $TYPE$. Two main types are proposed in the next section: complementary and redundant arguments.
- The overall reliability of sources of information or the completeness of premises, denoted as v. As the available premises may be not enough to justify full confidence in the top goal, this parameter provides a way to weaken the confidence obtained from sub-goals. It is also known as a discounting factor[1] in D-S theory.

[1]A discounting factor $v \in [0, 1]$ is employed to make the mass, for example, $m^{\Omega_A}(\{A\})$ less informative and to increase the mass allocated to ignorance, i.e., $m^{\Omega}_{A}(\Omega)$. $v = 0$ represents zero reliability of the source; on the contrary, while $v = 1$ implies total trust in the source. The discounting operation is defined as:

$$m^{\Omega}_{v}(A) = \begin{cases} v \cdot m^{\Omega}(A), & \text{if } A \neq \Omega, \\ 1 - v \cdot (1 - m^{\Omega}(\Omega)), & \text{if } A = \Omega. \end{cases}$$

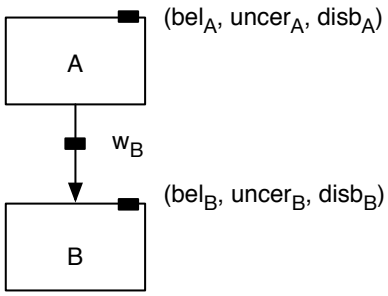


Figure 7: A single argument annotated with assessment parameters

Based on these factors, we propose a general definition of appropriateness using the example given in Figure 6:

Definition 3.2. *The appropriateness of sub-goals (*$appr_{\{G1,...Gn\}\rightarrow A}$*, simplified as* $appr_A$*) regarding the top goal is specified by the factors in the following expression:*

$$appr_A = (w_{G1}, w_{G2}, ..., w_{Gn}, < TYPE >, v) \tag{2}$$

where $w_{G_i}, v, \sum w_{G_i} \in [0, 1]$, $< TYPE > \in \{complementary, redundant\}$.

As noted above, w_{G_i}, $< TYPE >$ and v correspond to the three factors that may influence trustworthiness propagation; $< TYPE >$ is an operator for the argument type, which is only applicable if the argument has more than one premise ($n > 1$). The two options for argument types (complementary and redundant) will be defined in the following sections.

Confidence propagation starts from the simplest argument with one sub-goal. We call this the single argument (one-node argument), as shown in Figure 7. A single argument *A is supported by B* and has only one premise. Note that although we adopt the GSN notation "is supported by" arrow (from A to B), in this section, we focus on confidence propagation from B to A (bottom-up). This calculation shows the simplest case; the same rationale is applied in the next sections to double-node and n-node arguments.

3.2. Appropriateness of sub-goals

The appropriateness of sub-goals affects the trustworthiness of the top goal. The general definition of appropriateness is given in Section 3.1. Here, we specify the corresponding factors for the single argument based on Definition 3.2. In this case, only the contributing weight of the sub-goal is considered.

We start from the definition of the contributing weight, for instance, the weight of sub-goal B (see Figure 7). Based on the D-S theory, masses are used to express the degree of belief in certain states. A 2-tuple (X_B, X_A) presents the cross product $\Omega_B \times \Omega_A$, where X_B and X_A are elements of Ω_B and Ω_A, respectively ($\Omega_A = \{A, \overline{A}\}$, $\Omega_B = \{B, \overline{B}\}$). Therefore, the frame of discernment $\Omega_B \times \Omega_A = \{(\overline{B}, \overline{A}), (B, \overline{A}), (\overline{B}, A),\ (B, A)\}$. Among the elements of the frame, for example, $(\overline{B}, \overline{A})$ represents the situation: when B is false, A is false. In our approach, the appropriateness of B to A is defined as follows:

Definition 3.3. *The appropriateness of the sub-goal B to support the top goal A ($appr_{B\to A}$) is specified by the masses m_1 assigned to the subsets $(\{(B, A), (\overline{B}, \overline{A})\})$ and $(\Omega_B \times \Omega_A)$ considering the discounting factor v:*

$$appr_{B\to A} : \begin{cases} m_1^{\Omega_B \times \Omega_A}(\{(B, A), (\overline{B}, \overline{A})\}) = w_B v \\ m_1^{\Omega_B \times \Omega_A}(\Omega_B \times \Omega_A) = 1 - w_B v \end{cases} \tag{3}$$

where $w_B \in [0, 1]$ is the contributing weight of B, representing the degree to which A depends on B; $v \in [0, 1]$ is the discounting factor that is used to evaluate the completeness of the available premises for A.

In the above definition, masses are assigned to:

- The direct inferences $(\{(B, A), (\overline{B}, \overline{A})\})$, which is called the contributing weight of B, denoted as $w_{B\to A}$ (simplified as w_B in Figure 7 and Equation 3). $\{(B, A), (\overline{B}, \overline{A})\}$ indicates that the inference that *A is true* can be inferred from *B is true*, and conversely *B is false* leads to *A is false*.

- The uncertainty $(\Omega_B \times \Omega_A)$, where $\Omega_B \times \Omega_A$ is the simplified expression of $\{(\overline{B}, \overline{A}), (\overline{B}, A), (B, \overline{A}), (B, A)\}$. It represents uncertainty in whether B contributes to demonstrating the truth of A.

In addition, the available premises may be not enough to justify full confidence in the top goal. The discounting factor (v) is introduced. In D-S theory, the discounting factor aims to measure the reliability of the source of information (usually called an agent). It is adopted here to represent the reliability of sources or the completeness of premises. According to the discounting operation (see the footnote in Section 3.1), the support of sub-goal B is weakened and more mass is credited to the uncertain state $(\Omega_B \times \Omega_A)$. When $v = 1$, B sufficiently supports A and no other premise is needed. When $v = 0$, $m_1^{\Omega_B \times \Omega_A}(\Omega_B \times \Omega_A) = 1$, B does not provide any knowledge about A, i.e. there is complete uncertainty regarding A.

It is important to note that in a safety case, no rebuttal (as defined by Toulmin) is considered, which means that $m(\{(\overline{B}, A)\})$ and $m(\{(B, \overline{A})\})$ are included in uncertainty, and thus not expressed in the equations.

3.3. Trustworthiness of sub-goals

Even if argument B is appropriate to support A, we need to estimate the trustworthiness of B itself. The trustworthiness of a goal is introduced in the Definition 3.1. To combine these two types of confidence measures of sub-goal B and obtain the trustworthiness of top goal A, we need to unify frames of discernement (Ω_B and $\Omega_B \times \Omega_A$) to which the masses are assigned, as $\Omega_B \times \Omega_A$. This is achieved by *vacuous extension* (see (Mercier et al., 2005)) which is actually an extension of a mass defined in Ω_B to the frame of discernment $\Omega_B \times \Omega_A$. The masses m_2 represent the trustworthiness of B extended to the frame $\Omega_B \times \Omega_A$ (represented by the up arrow $\uparrow$):

$$trust_B : \begin{cases} bel^{\Omega_B}(\{B\}) = m_2^{\Omega_B \uparrow \Omega_B \times \Omega_A}(\{B\} \times \Omega_A) = bel_B \\ bel^{\Omega_B}(\{\overline{B}\}) = m_2^{\Omega_B \uparrow \Omega_B \times \Omega_A}(\{\overline{B}\} \times \Omega_A) = disb_B \\ m^{\Omega_B}(\{B, \overline{B}\}) = m_2^{\Omega_B \uparrow \Omega_B \times \Omega_A}(\Omega_B \times \Omega_A) = uncer_B = 1 - bel_B - disb_B \end{cases} \tag{4}$$

Where $bel_B, disb_B, bel_B + disb_B \in [0, 1]$. $\{B\} \times \Omega_A$ is used instead of $\{(B, A), (B, \overline{A})\}$ and $\{\overline{B}\} \times \Omega_A$ instead of $\{(\overline{B}, A), (\overline{B}, \overline{A})\}$ to highlight the focus on B.

3.4. Confidence propagation for the single argument

Our aim is to deduce the trustworthiness of A ($bel_A, disb_A, uncer_A$) based on the trustworthiness of B, $trust_B$ (4) and the appropriateness of B to A, $appr_{B \to A}$ (3). These can be regarded as two ways to assess A and the two sources of information can be combined with the help of Dempster's rule.

In order to illustrate the combination of m_1 (3) and m_2 (4), the six possible combinations and *focal sets*[2] in the frame $\Omega_B \times \Omega_A$ are shown in Table 1. The conflict factor K in this combination rule is 0, as there is no conflict in this case. Our aim is to obtain the trustworthiness of A ($bel_A, disb_A, uncer_A$) in the frame Ω_A from the combined results of $\Omega_B \times \Omega_A$. Thus, the *marginalization* operation (see (Mercier et al., 2005)) is used. For example, bel_A is obtained from the focal set $\{(B, A)\}$, which is underlined in Table 1:

$$bel^{\Omega_A}(\{A\}) = m^{\Omega_A}(A) = m^{\Omega_B \times \Omega_A \downarrow \Omega_A}(A) = m_{12}^{\Omega_B \times \Omega_A}(\{(B, A)\}) \tag{5}$$

[2]For a mass function m_k on the space Ω, a set E is a focal element of m_k iff $m_k(E) > 0$.

Table 1: Focal sets after the combination of $appr_{B\to A}$ and $trust_B$

		$\boldsymbol{m_1}$ $\boldsymbol{(appr_{B\to A})}$	
		$\boldsymbol{m_1^{\Omega_B\times\Omega_A}(\{(\overline{B},\overline{A}),(B,A)\})}$	$\boldsymbol{m_1^{\Omega_B\times\Omega_A}(\Omega_B\times\Omega_A)}$
$\boldsymbol{m_2}$ $\boldsymbol{(trust_B)}$	$\boldsymbol{m_2^{\Omega_B\uparrow\ \Omega_B\times\Omega_A}(\{B\}\times\Omega_A)}$	$\{\underline{(B,A)}\}$	$\{B\}\times\Omega_A$
	$\boldsymbol{m_2^{\Omega_B\uparrow\ \Omega_B\times\Omega_A}(\{\overline{B}\}\times\Omega_A)}$	$\{(\overline{B},\overline{A})\}$	$\{\overline{B}\}\times\Omega_A$
	$\boldsymbol{m_2^{\Omega_B\uparrow\ \Omega_B\times\Omega_A}(\Omega_B\times\Omega_A)}$	$\{(\overline{B},\overline{A}),(B,A)\}$	$\Omega_B\times\Omega_A$

Then, *belief* in A is calculated according to Dempster's rule:

$$\begin{aligned} m_{12}^{\Omega_B\times\Omega_A}(\{B,A\}) =& \frac{m_1^{\Omega_B\times\Omega_A}(\{(\overline{B},\overline{A}),(B,A)\})\times m_2^{\Omega_B\uparrow\Omega_B\times\Omega_A}(\{B\}\times\Omega_A)}{1-K} \\ =& bel_B w_B v \end{aligned} \tag{6}$$

Thus, according to (5):

$$bel^{\Omega_A}(\{A\}) = m_{12}^{\Omega_B\times\Omega_A}(\{B,A\}) = bel_B w_B v \tag{7}$$

where $bel_B, w_B, v \in [0,1]$.

Similarly, $disb_A$ is obtained from the focal set $\{(\overline{B},\overline{A})\}$; $uncer_A$ is calculated from the remaining four focal sets shown in Table 1. Therefore, we can summarize the trustworthiness of A $(bel_A, disb_A, uncer_A)$ as:

$$trust_A : \begin{cases} bel^{\Omega_A}(\{A\}) = m^{\Omega_A}(\{A\}) = bel_B w_B v \\ disb^{\Omega_A}(\{A\}) = m^{\Omega_A}(\{\overline{A}\}) = dis_B w_B v \\ uncer^{\Omega_A}(\{A\}) = m^{\Omega_A}((\{\overline{A},A\})) = 1-(bel_B+dis_B)w_B v \end{cases} \tag{8}$$

where $bel_B, disb_B, w_B, v \in [0,1]$.

For example, let us take the argument: "A: System is acceptably safe" and "B: All hazards have been addressed". Assuming the trustworthiness of goal A is $trust_B = (bel_B, uncer_B, disb_B) = (0.7, 0.2, 0.1)$, the appropriateness of goal B to A is $w_B = 0.9$, and $v = 1$. Following (8), we have:

$$trust_A = (bel_A, uncer_A, disb_A) = (0.63, 0.28, 0.09)$$

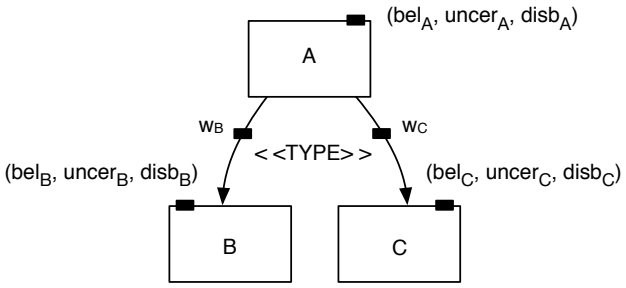


Figure 8: A double-node argument annotated with assessment parameters

4. Confidence propagation for the double-node argument

In practice, most arguments have a more complex structure, with two or more premises. As Figure 9 shows, two arguments may actually be based on different argument types. For instance, (a) is often used as it is known that there is a partial overlap between testing and formal verification in software development. In contrast, in (b), knowing that hazards are associated with different impacts, each sub-goal contributes independently to the top goal "System is acceptably safe". Thus, in this section, we focus on confidence propagation for a double-node argument.

4.1. Argument types

Govier (2013) emphasizes the importance of the cooperative contribution of premises in argument assessment (this 2013 edition is actually the 7th edition, first editions are in the 80's). She proposes three argument types: linear sequential (single argument), linked support ("pure AND") and convergent support ("pure OR"). These types are considered in the context of logical reasoning. A statement can only be true or false. Referring to the work of Ayoub et al. (2013), Cyra and Gorski (2011) and Guiochet et al. (2015) point out that most arguments are not "pure AND" nor "pure OR" to infer a statement. Consequently, Cyra and Gorski (2011) extend Govier's argument types by considering more complex inferences. They define two types of argument and several sub-types:

- Type 1: the falsification of a single premise leads to the rebuttal of the conclusion, including the NSC-argument (Necessary and Sufficient Condition list argument), the SC-argument (Sufficient Condition list argument) and the combination of the NSC-argument and the SC-argument

- Type 2: the falsification of one of the premises decreases, but does not nullify support for the conclusion, including the C-argument (Complementary argu-

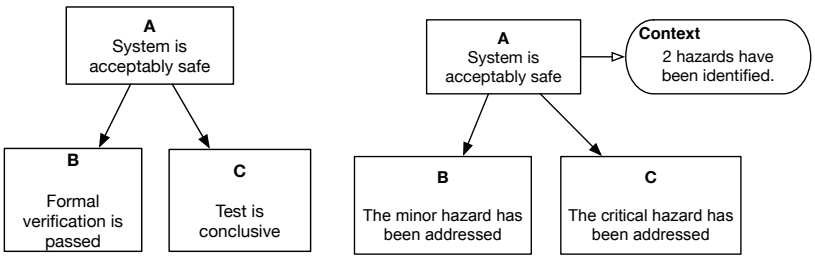


Figure 9: Argument examples with different inference complexities

ment), the A-argument (Alternative argument), and the combination of the C-argument and the A-argument

These complementary and alternative arguments are very useful in naming the mutual contribution of premises. However, they remain descriptive, and the two combinations are not clearly explained regarding both their definition and processing. Consequently, the corresponding confidence aggregation rules have little justification and lack consistency for different types. Ayoub et al. (2013) classified argument types based on the degree of overlap between premises into *alternative, disjoint, overlap and containment*. This is similar to Cyra and Gorski (2011)'s classification except for *overlap*.

Drawing upon this work on argument type classification, we propose an approach to formally define argument types as a part of the definition of the appropriateness of sub-goals. Here, we use the same approach to extend the confidence assessment of the single argument to the double-node argument. A typical double-node argument is presented in Figure 8: goal A is supported by two sub-goals B and C. As in the single argument example, confidence assessment parameters are annotated.

These parameters are:

- The appropriateness of sub-goals B and C (see expression below), including the contributing weights, ($w_{B\to A}$, $w_{C\to A}$, simplified as w_B, w_C), the operator for the argument type operator ($< TYPE >$), and the completeness of the premises (the discounting factor v). Argument types are defined later in this section.

$$appr_A = (w_B, w_C, < TYPE >, v) \tag{9}$$

- The trustworthiness of goals A: $trust_A = (bel_A, disb_A, uncer_A)$, B: $trust_B = (bel_B, disb_B, uncer_B)$ and C: $trust_C = (bel_C, disb_C, uncer_C)$.

4.2. Appropriateness of sub-goals in double-node argument

This subsection presents how the sub-goals in a double-node argument support the top goal. For the single argument, we evaluated the contribution of a single sub-goal. The contributing weight of the sub-goal was introduced in the previous subsection. When there are multiple sub-goals, their mutual influence on the higher-level goal must be examined, and the distinction between disjoint and joint contributions of sub-goals B and C must be made clear. Thus, we consider that sub-goals B and C support the top goal A in four ways.

Based on D-S theory, we assign masses to model these four ways. Since there are three statements (A, B and C), a three-dimension frame of discernment is adopted $\Omega = \Omega_B \times \Omega_C \times \Omega_A$ (following the order of inference $B, C \rightarrow A$), which is equivalent to $\{(\overline{B}, \overline{C}, \overline{A}), (B, \overline{C}, \overline{A}), (\overline{B}, C, \overline{A}), (\overline{B}, \overline{C}, A), (B, C, \overline{A}), (\overline{B}, C, A), (B, \overline{C}, A), (B, C, A)\}$. The subsets of Ω denote the possible inferences among A, B and C: e.g. $\{(\overline{B}, \overline{C}, \overline{A})\}$ stands for "when both B and C are false, A is false".

All frames of discernment of trustworthiness and appropriateness need to be unified as $\Omega = \Omega_B \times \Omega_C \times \Omega_A$ using the vacuous extension. For instance, the mass in the frame $\Omega_B \times \Omega_A$, $m_1^{\Omega_B \times \Omega_A}(\{(B, A), (\overline{B}, \overline{A})\})$, given in Definition 3.3 turns to $m_1^{\Omega_B \times \Omega_A \uparrow \Omega}(\{B\} \times \Omega_C \times \{A\} \cup \{\overline{B}\} \times \Omega_C \times \{\overline{A}\})$, which is simplified as $m_1^{\Omega}(\{B\} \times \Omega_C \times \{A\} \cup \{\overline{B}\} \times \Omega_C \times \{\overline{A}\})$.

In our approach, the different ways that B and C support A correspond to four "pure" cases: *pure B alone, pure C alone, pure AND and pure OR*. They will be used as basic elements to present "mixed" complex arguments that are described hereafter. The appropriateness of sub-goals for these "pure" cases are respectively formalized as follows (the discounting factor v will be discussed later):

- *Pure B alone*: A exclusively depends on B. This case is equivalent to the single argument with the weight of the sub-goal equal to 1.

$$m^{\Omega}(\{B\} \times \Omega_C \times \{A\} \cup \{\overline{B}\} \times \Omega_C \times \{\overline{A}\}) = w_B = 1 \tag{10}$$

  w_B is the contributing weight of B, denoting the degree that A depends on B.

- *Pure C alone*: A exclusively depends on C.

$$m^{\Omega}(\Omega_B \times \{C\} \times \{A\} \cup \Omega_B \times \{\overline{C}\} \times \{\overline{A}\}) = w_C = 1 \tag{11}$$

  w_C is the contributing weight of C, denoting the degree that A depends on C.

- *Pure AND*: B and C contribute to A with an AND logic gate.

$$m^{\Omega}(\{(\overline{B},\overline{C},\overline{A}),(\overline{B},C,\overline{A}),(B,\overline{C},\overline{A}),(B,C,A)\}) = w_{B\times C\to A} = 1 \tag{12}$$

  $w_{B\times C\to A}$ denotes the degree of AND gate relation between B and C when they contribute to A.

- *Pure OR*: B and C contribute to A with an OR logic gate.

$$m^{\Omega}(\{(\overline{B},\overline{C},\overline{A}),(\overline{B},C,A),(B,\overline{C},A),(B,C,A)\}) = w_{B+C\to A} = 1 \tag{13}$$

  $w_{B+C\to A}$ denotes the degree of OR gate relation between B and C when they contribute to A.

As discussed in Section 4.1, not all arguments are "pure" cases. In fact, most arguments are not. Therefore, we propose two "mixed" types: *complementary and redundant arguments*. Then, three particular types (*fully complementary and fully redundant arguments, and disparate argument*) are derived from these two types for certain limit cases. These argument types are formally distinguished by the definitions of the appropriateness of the sub-goals to the top goal. Similarly, the discounting factor v, which evaluates the completeness of the available premises for A, is taken into account in the following definitions.

- The *complementary argument (C-Arg)* is the combination of "Pure B alone" (10), "Pure C alone" (11) and "Pure AND" (12). According to the constraint of mass function, $w_B + w_C + w_{B\times C\to A} = 1$ (before consideration of the discounting factor v). Thus, $w_{B\times C\to A} = 1 - w_B - w_C$, denotes the degree of the complementarity between sub-goals.

  Definition 4.1. *The appropriateness of sub-goals for the complementary argument (C-Arg) is defined as:*

  $appr_{\{B,C\}\to A}$*:*

$$\begin{cases} m_1^{\Omega}(\{B\}\times\Omega_C\times\{A\}\cup\{\overline{B}\}\times\Omega_C\times\{\overline{A}\}) = w_B\cdot v \quad (Pure\ B\ alone) \\ m_1^{\Omega}(\Omega_B\times\{C\}\times\{A\}\cup\Omega_B\times\{\overline{C}\}\times\{\overline{A}\}) = w_C\cdot v \quad (Pure\ C\ alone) \\ m_1^{\Omega}(\{(\overline{B},\overline{C},\overline{A}),(\overline{B},C,\overline{A}),(B,\overline{C},\overline{A}),(B,C,A)\}) = w_{B\times C\to A}\cdot v \quad (Pure\ AND) \\ m_1^{\Omega}(\Omega) = 1 - v \end{cases} \tag{14}$$

where $v, w_B, w_C \in [0,1]$, and $w_{B\times C\to A} = 1 - w_B - w_C \geq 0$.

- The *redundant argument* (R-Arg) is the combination of "Pure B alone" (10), "Pure C alone" (11) and "Pure OR" (13). Similarly, $w_B + w_C + w_{B+C\to A} = 1$. $w_{B+C\to A} = 1 - w_B - w_C$, denoting the degree of the redundancy between sub-goals.

  Definition 4.2. *The appropriateness of sub-goals for the redundant argument (R-Arg) is defined as:*

  $appr_{\{B,C\}\to A}$*:*

$$\begin{cases} m_1^\Omega(\{B\}\times\Omega_C\times\{A\}\cup\{\overline{B}\}\times\Omega_C\times\{\overline{A}\}) = w_B\cdot v \quad (Pure\ B\ alone) \\ m_1^\Omega(\Omega_B\times\{C\}\times\{A\}\cup\Omega_B\times\{\overline{C}\}\times\{\overline{A}\}) = w_C\cdot v \quad (Pure\ C\ alone) \\ m_1^\Omega(\{(\overline{B},\overline{C},\overline{A}),(\overline{B},C,A),(B,\overline{C},A),(B,C,A)\}) = w_{B+C\to A}\cdot v \quad (Pure\ OR) \\ m_1^\Omega(\Omega) = 1 - v \end{cases} \tag{15}$$

  where $v, w_B, w_C \in [0,1]$, and $w_{B+C\to A} = 1 - w_B - w_C \geq 0$.

- The *fully complementary argument (FC-Arg).* When $w_{B\times C\to A} = 1$ for the complementary argument (C-Arg), we call this argument fully complementary. It corresponds to the "Pure AND" case (12). $w_{B\times C\to A} = 1$ denotes full complementarity between sub-goals. The appropriateness of sub-goals for FC-Arg is:

  $appr_{\{B,C\}\to A}$:

$$\begin{cases} m_1^\Omega(\{(\overline{B},\overline{C},\overline{A}),(\overline{B},C,\overline{A}),(B,\overline{C},\overline{A}),(B,C,A)\}) = w_{B\times C\to A}\cdot v = v \\ m_1^\Omega(\Omega) = 1 - w_{B\times C\to A}\cdot v = 1 - v \end{cases} \tag{16}$$

  where $v \in [0,1]$

- The *fully redundant argument (FR-Arg).* When $w_{B+C\to A} = 1$ for the redundant argument (R-Arg), we call this argument fully redundant argument. It corresponds to the "Pure OR" case (13). $w_{B+C\to A} = 1$ denotes the full redundancy between sub-goals. The appropriateness of sub-goals for FR-Arg is:

$appr_{\{B,C\}\to A}$:

$$\begin{cases} m_1^{\Omega}(\{(\overline{B},\overline{C},\overline{A}),(\overline{B},C,A),(B,\overline{C},A),(B,C,A)\}) = w_{B+C\to A}\cdot v = v \\ m_1^{\Omega}(\Omega) = 1 - w_{B\times C\to A}\cdot v = 1 - v \end{cases} \tag{17}$$

where $v \in [0,1]$

- The *Disparate argument (D-Arg)* is the combination of "Pure B alone" (10) and "Pure C alone" (11). It can be seen as the limit case of redundancy when $w_{B\times C\to A} = 0$, or the limit case of complementarity when $w_{B+C\to A} = 0$. Then, $w_B + w_C = 1$. The appropriateness of sub-goals for D-Arg is:

  $appr_{\{B,C\}\to A}$:

$$\begin{cases} m_1^{\Omega}(\{B\}\times\Omega_C\times\{A\}\cup\{\overline{B}\}\times\Omega_C\times\{\overline{A}\}) = w_B\cdot v \\ m_1^{\Omega}(\Omega_B\times\{C\}\times\{A\}\cup\Omega_B\times\{\overline{C}\}\times\{\overline{A}\}) = w_C\cdot v \\ m_1^{\Omega}(\Omega) = 1 - v \end{cases} \tag{18}$$

  where $v, w_B, w_C \in [0,1]$, and $w_B + w_C = 1$.

All of the above argument types are derived from the two basic types: the redundant argument and the complementary argument. The fully redundant/complementary argument can become disparate by continuously changing the values of weights. Table 2 compares the different classifications of argument types. As this table shows, our proposed classification encapsulates all of the argument types mentioned in related work.

4.3. Trustworthiness of sub-goals in double-node argument

The trustworthiness of a goal is given in the Definition 3.1. In order to aggregate the two types of confidence assessment measures for sub-goals B and C, the trustworthiness must be in the frame of discernment $\Omega = \Omega_B \times \Omega_C \times \Omega_A$. With the help of the vacuous extension, the trustworthiness of sub-claims B and C are:

$$trust_B : \begin{cases} bel^{\Omega_B}(\{B\}) = m_2^{\Omega_B\uparrow\Omega}(\{B\}\times\Omega_C\times\Omega_A) = bel_B \\ bel^{\Omega_B}(\{\overline{B}\}) = m_2^{\Omega_B\uparrow\Omega}(\{\overline{B}\}\times\Omega_C\times\Omega_A) = disb_B \\ m^{\Omega_B}(\{B,\overline{B}\}) = m_2^{\Omega_B\uparrow\Omega}(\Omega) = uncer_B = 1 - bel_B - disb_B \end{cases} \tag{19}$$

Table 2: Comparison of different proposals for argument classification

	Govier [2013]	Cyra and Gorski (2011)		Ayoub et al. [2013]	Guiochet et al. [2015]	Proposal in this paper
Argument Types	Convergent	-		-	Alternative	FR-Arg
	-	Type2	A-argument/ Combination of A,C-argument	Alternative/ Overlap/ Containment		R-Arg
	-		C-argument/ Combination of A,C-argument	Disjoint	-	D-Arg
	-	-		-	Complementary	C-Arg
	Linked	Type1		-		FC-Arg
	Linear sequential	-		-	Simple argument	Simple argument

$$trust_C : \begin{cases} bel^{\Omega_C}(\{C\}) = m_3^{\Omega_C \uparrow \Omega}(\Omega_B \times \{C\} \times \times \Omega_A) = bel_C \\ bel^{\Omega_C}(\{\overline{C}\}) = m_3^{\Omega_C \uparrow \Omega}(\Omega_B \times \{\overline{C}\} \times \Omega_A) = disb_C \\ m^{\Omega_C}(\{C, \overline{C}\}) = m_3^{\Omega_C \uparrow \Omega}(\Omega) = uncer_C = 1 - bel_C - disb_C \end{cases} \quad (20)$$

Where $bel_B, disb_B, bel_B + disb_B, bel_C, disb_C, bel_C + disb_C \in [0, 1]$.

4.4. Confidence aggregation for complementary arguments

All confidence assessment parameters for sub-goals have been identified for the double-node argument. Different argument types have different behaviors in terms of their contribution to confidence in A. This section addresses confidence aggregation for complementary arguments. The aim is still to calculate the trustworthiness of the top goal A ($bel_A, disb_A, uncer_A$) based on the combination of the appropriateness of sub-goals to A (14) and the trustworthiness of sub-goals (19) and (20). The combination is based on Dempster's rule. Regarding mass definitions for confidence assessment parameters, the issue of combination conflict is avoided by how masses are defined.

The masses of assessment parameters m_1, m_2 and m_3 are considered as independent pieces of evidence. According to Dempster's rule, only two pieces of evidence can be combined at the same time. However, given the associativity of Dempster's

rule (Shafer, 1976), the order of combinations does not change the result. As equations for the trustworthiness of B, m_2 (19) and C, m_3 (20) have a similar form, they are combined first ($m_{23} = m_2 \oplus m_3$); then we combine intermediate results with the appropriateness of sub-goals for the complementary argument m_1.

There are nine possible combinations of the masses m_2 and m_3 for trustworthiness B and C, leading to nine focal sets for mass m_{23}. For all combinations, the conflict factor K is 0. This intermediate, combined result is presented in Table 3. Because all of the intermediate results are useful in the next step, masses are presented in this table.

Next, we combine masses for the appropriateness of sub-goals, m_1 (14) with intermediate masses, m_{23}. Combined masses are denoted as m_{1-3}. As some of the subsets of combinations are the same, they contribute to the same new focal elements. The masses of these subsets are added up following Dempster's rule ($K = 0$). For instance, the mass of the focal set $\{B, C, A\}$ is calculated as follows:

$$\begin{aligned}
m^{\Omega}_{1-3}(\{B,C,A\}) &= m_1 \oplus m_{23} \\
&= m^{\Omega}_1(\{B\} \times \Omega_C \times \{A\} \cup \{\overline{B}\} \times \Omega_C \times \{\overline{A}\}) \cdot m^{\Omega}_{23}(\{B\} \times \{C\} \times \Omega_A) + \\
&\quad m^{\Omega}_1(\Omega_B \times \{C\} \times \{A\} \cup \Omega_B \times \{\overline{C}\} \times \{\overline{A}\}) \cdot m^{\Omega}_{23}(\{B\} \times \{C\} \times \Omega_A) + \\
&\quad m^{\Omega}_1(\{(\overline{B},\overline{C},\overline{A}),(\overline{B},C,\overline{A}),(B,\overline{C},\overline{A}),(B,C,A)\}) \cdot m^{\Omega}_{23}(\{B\} \times \{C\} \times \Omega_A) \\
&= w_B \cdot v \cdot bel_B \cdot bel_C + w_C \cdot v \cdot bel_B \cdot bel_C + (1 - w_B - w_C) \cdot v \cdot bel_B \cdot bel_C \\
&= bel_B \cdot bel_C \cdot v
\end{aligned} \tag{21}$$

Belief in A (bel_A) is calculated by adding up all the masses of all the focal sets that contribute to the mass $m^{\Omega\downarrow\Omega_A}(\{A\})$ after marginalization.

$$\begin{aligned}
bel_A = bel^{\Omega_A}(\{A\}) = m^{\Omega\downarrow\Omega_A}(\{A\}) &= \sum_{Q \subset \Omega, Q\downarrow\Omega_A = \{A\}} m^{\Omega}(Q) \\
&= m^{\Omega}_{1-3}(\{\overline{B},C,A\}) + m^{\Omega}_{1-3}(\{B,\overline{C},A\}) + m^{\Omega}_{1-3}(\{B,C,A\}) + \\
&\quad m^{\Omega}_{1-3}(\{(B,\overline{C},A),(B,C,A)\}) + m^{\Omega}_{1-3}(\{(\overline{B},C,A),(B,C,A)\}) \\
&= [bel_B \cdot w_b + bel_C \cdot w_C + bel_B \cdot bel_C(1 - w_B - w_c)]v
\end{aligned} \tag{22}$$

Similarly, disbelief ($disb_A$) and uncertainty ($uncer_A$) in A are calculated and presented below.

Table 3: Intermediate combination results (m_{23}) of trustworthiness of B and C

		$\boldsymbol{m_2\ (trust_B)}$		
		$\boldsymbol{m_2^\Omega(\{B\} \times \Omega_C \times \Omega_A) = bel_B}$	$\boldsymbol{m_2^\Omega(\{\overline{B}\} \times \Omega_C \times \Omega_A) = disb_B}$	$\boldsymbol{m_2^\Omega(\Omega) = 1 - bel_B - disb_B}$
$\boldsymbol{m_3\ (trust_C)}$	$\boldsymbol{m_3^\Omega(\Omega_B \times \{C\} \times \Omega_A) = bel_C}$	$m_{23}(\{B\} \times \{C\} \times \Omega_A) = bel_B \cdot bel_C$	$m_{23}(\{\overline{B}\} \times \{C\} \times \Omega_A) = disb_B \cdot bel_C$	$m_{23}(\Omega_B \times \{C\} \times \Omega_A) = (1 - bel_B - disb_B)bel_C$
	$\boldsymbol{m_3^\Omega(\Omega_B \times \{\overline{C}\} \times \Omega_A) = = disb_C}$	$m_{23}(\{B\} \times \{\overline{C}\} \times \Omega_A) = = bel_B \cdot disb_C$	$m_{23}(\{\overline{B}\} \times \{\overline{C}\} \times \Omega_A) = = disb_B \cdot disb_C$	$m_{23}(\Omega_B \times \{\overline{C}\} \times \Omega_A) = = (1 - bel_B - disb_B)disb_C$
	$\boldsymbol{m_3^\Omega(\Omega) = 1 - bel_C - disb_C}$	$m_{23}(\{B\} \times \Omega_C \times \Omega_A) = bel_B(1 - bel_C - disb_C)$	$m_{23}(\{\overline{B}\} \times \Omega_C \times \Omega_A) = disb_B(1 - bel_C - disb_C)$	$m_{23}(\Omega) = (1 - bel_B - disb_B)(1 - bel_C - disb_C)$

Table 4: Aggregation rules for complementary arguments

Types	Aggregation rules
C-Arg	$\begin{cases} bel_A & = [bel_B \cdot w_B + bel_C \cdot w_C + bel_B \cdot bel_C(1 - w_B - w_C)]v \\ disb_A & = \{disb_B \cdot w_B + disb_C \cdot w_C + [1 - (1 - disb_B)(1 - disb_C)](1 - w_B - w_C)\}v \\ uncer_A & = 1 - bel_A - disb_A \end{cases}$

$$
\begin{aligned}
disb_A =& bel^{\Omega_A}(\{\overline{A}\}) = m^{\Omega\downarrow\Omega_A}(\{\overline{A}\}) = \sum_{Q\subset\Omega, Q\downarrow\Omega_A=\{\overline{A}\}} m^{\Omega}(Q) \\
=& m^{\Omega}_{1-3}(\{\overline{B},\overline{C},\overline{A}\}) + m^{\Omega}_{1-3}(\{\overline{B},C,\overline{A}\}) + m^{\Omega}_{1-3}(\{B,\overline{C},\overline{A}\}) + \\
& m^{\Omega}_{1-3}(\{(\overline{B},\overline{C},\overline{A}),(\overline{B},C,\overline{A})\}) + m^{\Omega}_{1-3}(\{(\overline{B},\overline{C},\overline{A}),(B,\overline{C},\overline{A})\}) \\
=& [disb_B(1 - w_C) + disb_C(1 - w_B) - disb_B \cdot disb_C(1 - w_B - w_C)]v \\
=& \{disb_B \cdot w_B + disb_C \cdot w_C + [1 - (1 - disb_B)(1 - disb_C)](1 - w_B - w_C)\}v
\end{aligned} \tag{23}
$$

$$
\begin{aligned}
uncer_A =& m^{\Omega_A}(\{A,\overline{A}\}) = \sum_{Q\subset\Omega, Q\downarrow\Omega_A=\{A,\overline{A}\}} m^{\Omega}(Q) \\
=& 1 - [bel_B \cdot w_b + bel_C \cdot w_C + bel_B \cdot bel_C(1 - w_B - w_c)]v - \\
& [disb_B(1 - w_C) + disb_C(1 - w_B) - disb_B \cdot disb_C(1 - w_B - w_C)]v \\
=& 1 - bel^{\Omega_A}(\{A\}) - bel^{\Omega_A}(\{\overline{A}\})
\end{aligned} \tag{24}
$$

Confidence aggregation rules for the complementary argument with two sub-goals are developed (presented in (22), (23) and (24)). The trustworthiness of the top goal A (bel_A, $disb_A$, $uncer_A$) can be deduced based on these aggregation rules (see Table 4).

4.5. Confidence aggregation for redundant arguments

As sub-goals can support the top goal in various ways, confidence propagation in redundant arguments is unlike complementary arguments. However, the procedure to calculate confidence aggregation rules is the same as described in the previous section. We assume that the double-node argument shown in Figure 8 is a redundant argument. The trustworthiness of the top goal A ($bel_A, disb_A, uncer_A$) is calculated

Table 5: Aggregation rules for redundant arguments

Types	Aggregation rules
R-Arg	$\begin{cases} bel_A = \{bel_B \cdot w_B + bel_C \cdot w_C + [1-(1-bel_B)(1-bel_C)](1-w_B-w_C)\}v \\ disb_A = [disb_B \cdot w_B + disb_C \cdot w_C + disb_B \cdot disb_C(1-w_B-w_C)]v \\ uncer_A = 1 - bel_A - disb_A \end{cases}$

based on the combination of the appropriateness of sub-goals to A, m_1 (15), and the trustworthiness of sub-goals m_2 (19) and m_3 (20). Since masses m_1 and m_2 are combined, we can use the results shown in Table 3.

Once this is done, the calculation is similar to the one used for the complementary argument presented in the previous section. We directly give confidence aggregation rules for the redundant argument in Table 5.

4.6. Aggregation rules for particular argument types

In Section 4.2, three argument types (FC-Arg, FR-Arg, and D-Arg) were introduced to supplement the two basic types. As mentioned in that section, these three types refer to particular cases where the weights of sub-goals are equal to a limit value. In this subsection, we determine their confidence aggregation rules based on rules for complementary and redundant arguments.

- *The fully complementary argument (FC-Arg)*:

  For the fully complementary argument, $w_{B\times C\to A} = 1$, i.e. $w_B = w_C = 0$. The trustworthiness of A, $trust_A = (bel_A, disb_A, uncer_A)$ can be calculated with the formula:

$$trust_A : \begin{cases} bel_A = bel_B \cdot bel_C \cdot v \\ disb_A = [1-(1-disb_B)(1-disb_C)]v \\ uncer_A = 1 - bel_A - disb_A \end{cases} \tag{25}$$

  In this case, the way that sub-goals B and C contribute to confidence in goal A becomes a "pure AND". In contrast, disbelief propagates as an OR logic gate from sub-goals to the top goal. These characteristics are, in turn, consistent with the initial definition based on an AND logic gate.

- *The fully redundant argument (FR-Arg)*:

For the fully redundant argument (FR-Arg), $w_{B+C\to A} = 1$, i.e. $w_B = w_C = 0$. The trustworthiness of A, $trust_A = (bel_A, disb_A, uncer_A)$ can be calculated with the formula:

$$trust_A : \begin{cases} bel_A = [1 - (1 - bel_B)(1 - bel_C)]v \\ disb_A = disb_B \cdot disb_C \cdot v \\ uncer_A = 1 - bel_A - disb_A \end{cases} \tag{26}$$

In this case, the way that the sub-goals B and C contribute to confidence in goal A becomes a "pure OR". In contrast, disbelief propagates as an AND logic gate from sub-goals to the top goal. These characteristics are also consistent with the initial definition based on an OR logic gate.

- The *disparate argument (D-Arg)*:

  For both complementary and redundant arguments, if the $w_{B\times C\to A}$ and $w_{B+C\to A}$ decrease (i.e. w_B and w_C increase) to $w_{B\times C\to A} = 0$ and $w_{B+C\to A} = 0$ (i.e. $w_B + w_C = 1$), the aggregation rules for complementary and redundant arguments become the same:

$$trust_A : \begin{cases} bel_A = (bel_B w_B + bel_C w_C)v \\ disb_A = (disb_B w_B + disb_C w_C)v \\ uncer_A = 1 - bel_A - disb_A \end{cases} \tag{27}$$

  In this case, B and C contribute independently to the top goal A with their own weights. Confidence aggregation rules are the weighted sum of the trustworthiness of sub-goals.

4.7. Sensitivity analysis

This section presents the sensitivity analysis used to evaluate the behavior of confidence aggregation rules. The aim is to determine whether they are consistent with the corresponding argument types, and to validate propagation operators.

The analysis uses a tornado graph. This simple statistical tool shows the positive or negative influence of basic elements on a main function. Taking the function $f(x_1, ...x_n)$, where values $X_1, ..., X_n$ of variables x_i have been estimated, the tornado analysis consists in the estimation (for each $x_i \in [X_{min}, X_{max}]$) of the values $f(X_1, ..., X_{i-1}, X_{min}, X_{i+1}, ...X_n)$ and $f(X_1, ..., X_{i-1}, X_{max}, X_{i+1}, ...X_n)$, where X_{min} and X_{max} are the maximum and minimum admissible values of variables x_i. Hence

for each x_i, there is an interval of possible variations of function f. The tornado graph presents ordered intervals visually. In our case, we estimate the confidence in A, $m(A)$, with corresponding intervals for v, bel_B, bel_C, $disb_B$, $disb_C$, w_B and w_C.

We take the example of the double-node argument to analyze the confidence aggregation rules for both complementary (see Table 4) and redundant (see Table 5) arguments. The basic values (X_i) and intervals $[X_{min}, X_{max}]$ for each parameter are shown in Table 6. The basic values (X_i) are given arbitrarily and the intervals $[X_{min}, X_{max}]$ are deduced as a function of the requirements applied to parameters in the formulas: $bel_i, disb_i, w_i, v \in [0, 1]$, and $\sum_{i=1}^{n} w_i \leq 1$. For instance, the interval for w_B is [0,0.9], because $w_C = 0.1$ and the sum of them should not be more than 1.

Table 6: Values and intervals chosen for the sensitivity analysis

	v	bel_B	bel_C	$disb_B$	$disb_C$	w_B	w_C
Basic value X_i	0.9	0.5	0.8	0.2	0.1	0.4	0.1
$[X_{min}, X_{max}]$	[0,1]	[0,0.8]	[0,0.9]	[0,0.5]	[0,0.2]	[0,0.9]	[0,0.6]

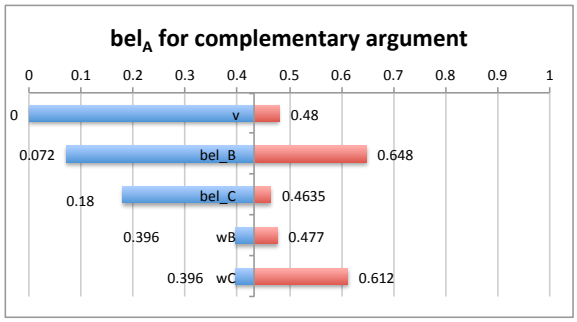
With the basic values above, the trustworthiness of A are $(bel_A, disb_A, uncer_A) = (0.432, 0.207, 0.361)$ for the complementary argument, and $(0.657, 0.09, 0.253)$ for the redundant argument. These values denote the position of the vertical axis in the corresponding tornado graphs. To determine the sensitivity to bel_B, we retain the basic values for all other variables and only calculate the values bel_A for $bel_B = 0$ and $bel_B = 0.8$: this gives values for the confidence in A [0.072, 0.648] for the complementary argument, and [0.432, 0.792] for the redundant argument. The same approach is applied to the other parameters. The results of the analysis are presented in Figure 10.

All of these graphs show that v has the most influence. When $v = 0$, confidence in A is 0. The structure of aggregation formulas shows that v remains the common factor in formulas after multiple combinations. This is consistent with the idea of using a discounting factor. Thus, v is the most sensitive point. In terms of interpretation, v is used to measure the overall reliability of sources, or the completeness of premises, and it makes it possible to evaluate all of the sub-goals as a whole. In general, we assume that $v = 1$, indicating that complete confidence in sub-goals leads to complete confidence in the top goal. In the inverse case ($v \neq 1$), we should be very cautious in determining the value of v.

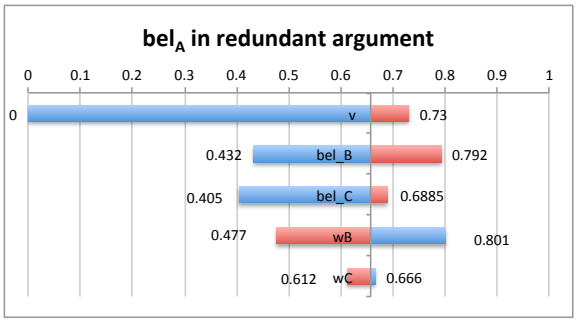
The trustworthiness of B has more impact on the trustworthiness of A than that of C in all six graphs. This is consistent with the higher weight of B compared to C. Comparing the impacts of B and C for the two types of arguments, the difference

Complementary argument

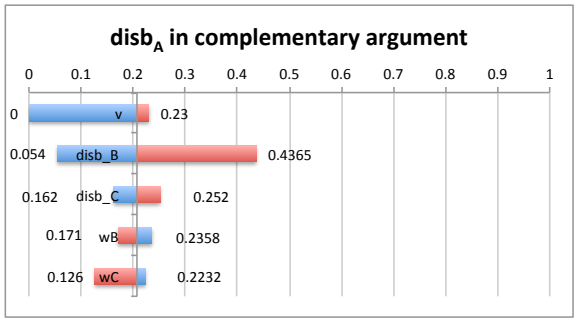
Redundant argument



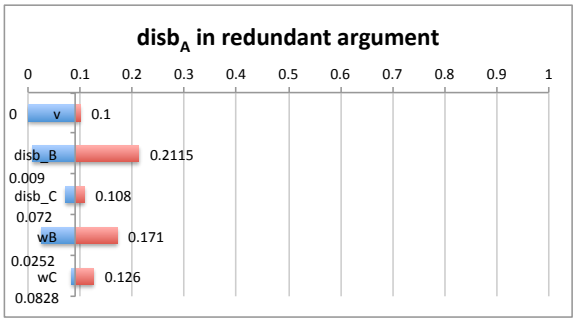
(a)



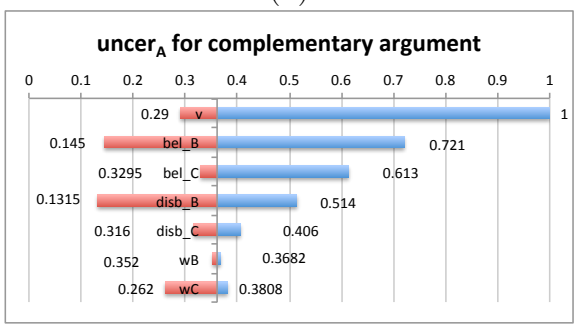
(d)



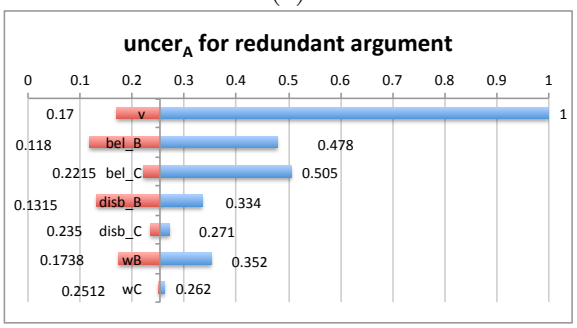
(b)



(e)



(c)



(f)

Figure 10: Tornado graphs for two types of double-node arguments

in the impact between B and C for the complementary argument is greater than for the redundant argument. This indicates that confidence in the top goal of a complementary argument relies more on the confidence in each of the sub-goals. Both $trust_B$ and $trust_C$ must be increased to effectively maximize $trust_A$.

Furthermore, an interesting consequence for the redundant argument is that when the weight w_B increases, confidence in A decreases (see Figure 10 (d)). When $w_B = 0.9$, then $bel_A = 0.432$. This is due to the constraint that $w_{B+C\to A} = 1 - w_B - w_C$. In other words, increasing w_B reduces redundancy. Therefore, confidence in A declines. This implies that, for redundant arguments, increasing the redundancy of B and C (i.e. decreasing w_B and w_C) increases confidence in A. This result shows that the correct interpretation of the weights w_B or w_C relies on both the impact of $trust_B$ or $trust_C$ on $trust_A$, and a representation of the degree of redundancy (or complementarity for the complementary argument).

This sensitivity analysis shows that the behavior of aggregation rules is consistent with our expectations regarding the influence of each of the parameters on the trustworthiness of the top goal ($trust_A = (bel_A, uncer_A, disb_A)$). Intuitively, the different impacts of the appropriateness of sub-goals on $trust_A$ differentiates how trustworthiness is propagated in complementary and redundant arguments. Generally, the complementary argument is more sensitive to variation in assessment measures. Given the same values for all measures, belief (bel_A) in the top goal of a complementary argument is lower than for a redundant argument, whereas disbelief ($disb_A$) and uncertainty ($uncer_A$) are always higher.

A specific difference relates to the impacts of w_B and w_C shown in graphs (a) and (d). This indicates that variation in the weights of sub-goals can also strengthen or weaken an "AND gate" or an "OR gate" (the complementarity or redundancy of sub-goals) and is a reflection of the original idea of defining mixed propagation operators: B alone, C alone and pure AND/OR.

5. Generalization of confidence propagation to the N-node argument

It is common for an argument to have more than two premises. In this section, we study confidence propagation and related issues applied to the N-node argument. The aim is to broaden the application of our approach.

5.1. Re-structuring the n-node argument

In order to employ the same approach to developing aggregation rules and to avoid, to the maximum extent, introducing new uncertainties, we require every branch in the n-node argument to belong to only one argument type. Complementary and redundant premises cannot be mixed to support the same goal. However,

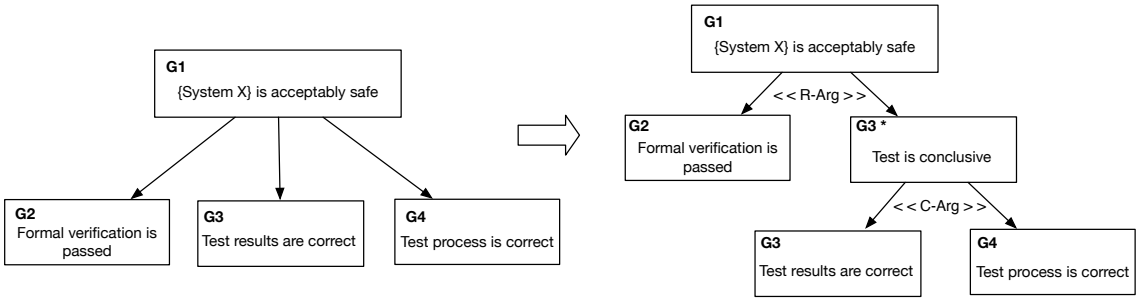


Figure 11: Re-structuring an argument for confidence propagation

the argument needs to be modified. For example, in Figure 11, the top goal "G1: System is acceptably safe" is supported by three sub-goals. They are, respectively, "G2: Formal verification is passed", "G3: Test results are correct" and "G4: Test process is correct". Formal verification and testing are two different techniques that are used to validate and verify, for instance, compliance with system safety requirements. The evidence related to these two techniques may have some degree of redundancy (R-Arg). However, G3 and G4 are premises related to testing, and are typically complementary (C-Arg). In this case, these premises are regrouped and new intermediate goals are proposed (G3* to the right of Figure 11).

5.2. Confidence aggregation for n-node arguments

For n-node arguments, the process is complex due to the number of combinations of assessment parameters. As the number of premises increases, the calculation increases exponentially, and includes the combination of masses and the simplification of the expression for non-linear polynomials. Regarding the former, for an argument with 2 to n premises, the number of possible combinations is shown in Table 7. Thus, it is better to have general confidence aggregation rules for n-node arguments for both types of arguments.

We propose an inductive approach to deduce confidence aggregation rules. The three-step process for single and double-node arguments is repeated for an argument with three sub-goals: B, C and D. Due to space limitations, we refer the reader to (Wang, 2018) for a thorough presentation of the formula deduction.

This shows that aggregation rules for double-node and three-node arguments have a similar structure, indicating that aggregation rules for any n-node argument (for $n > 1$) should be developed based on the same approach. Thus, we induct that the general confidence aggregation rules for n-node complementary and redundant arguments are as shown in Table 8.

Table 7: Number of possible combinations to develop aggregation rules

N	$\#C_1$	$\#C_2$	$\#C_{total}$
2	9	36	45
3	27	135	162
		...	
n	3^n	$3^n(n+2)$	$3^n(n+3)$

C_1: combination of the trustworthiness of sub-goals, C_2: combination of the appropriateness of sub-goals to the top goal with the results of C_1, C_{total}: total combinations

Table 8: Aggregation rules for n-node arguments supporting A

Types	Aggregation rules
C-Arg	$\begin{cases} bel_A = & [\sum_{i=1}^{n} bel_i w_i + (1 - \sum_{i=1}^{n} w_i) \prod_{i=1}^{n} bel_i]v \\ disb_A = & \{\sum_{i=1}^{n} disb_i w_i + (1 - \sum_{i=1}^{n} w_i)[1 - \prod_{i=1}^{n} (1 - disb_i)]\}v \\ uncer_A = & 1 - bel_A - disb_A \end{cases}$
R-Arg	$\begin{cases} bel_A = & \{\sum_{i=1}^{n} bel_i w_i + (1 - \sum_{i=1}^{n} w_i)[1 - \prod_{i=1}^{n} (1 - bel_i)]\}v \\ disb_A = & [\sum_{i=1}^{n} disb_i w_i + (1 - \sum_{i=1}^{n} w_i) \prod_{i=1}^{n} disb_i]v \\ uncer_A = & 1 - bel_A - disb_A \end{cases}$

Where $n > 1$, $bel_i, disb_i, w_i, v \in [0, 1]$, and $\sum_{i=1}^{n} w_i \leq 1$

6. Related work

Several other studies have examined the question of confidence assessment in safety cases. They mainly address the problem from two perspectives. One approach focuses on providing more qualitative justification (Kelly and Weaver, 2004; Hawkins et al., 2011; Menon et al., 2009; Ayoub et al., 2012). A second trend, which is closer to our work, is the development of quantitative approaches. An excessive increase in the number of arguments increases the complexity of the confidence estimation, and quantitative tools can be helpful for analysts. According to Nair et al. (2015a), quantitative approaches to evidence assessment are sometimes used in critical domains. Menon et al. (2009) note that there is a demand to combine and propagate confidence measures within an argument. These studies suggest that the issue of quantitatively assessing confidence in an argument has become an interesting topic for researchers in recent years. Concerning quantitative approaches, most work is based on Bayesian Belief Networks (Guo, 2003; Denney et al., 2011; Hobbs and Lloyd, 2012) and D-S theory (Cyra and Gorski, 2011; Ayoub et al., 2013; Duan et al., 2014; Nair et al., 2015b). Guiochet et al. (2015) put forward a mixed approach using both methods. Yuan et al. (2017) adopt subjective logic, in which confidence measures are also related to belief in D-S theory. In general, non-probabilistic approaches are preferred for assessing arguments, as most evidence evaluations are imprecise and based on expert knowledge. Nair et al. (2015b) provide a method for extracting and propagating expert judgments using D-S theory. This method is based on the confidence argument proposed by (Hawkins et al., 2011). Nevertheless, they do not consider inference types when aggregating information. Ayoub et al. (2013) introduce four argument types (alternative, disjoint, overlap and containment) and provide corresponding formulas to combine confidence in arguments; however, there is little detail given regarding how to deduct formulas. Cyra and Gorski (2011) provide a practical confidence propagation method to extract expert judgments. They transform decision and confidence levels into belief parameters (belief, disbelief, and uncertainty). Six types of arguments are proposed, based on the work of Govier (2013), but the parameters that relate to each of the types are not easy to interpret. Graydon and Holloway (2017) review several other quantitative approaches to the assessment of confidence in safety arguments. While they find them very interesting, the authors conclude that none of the methods can be applied in practice. This is due to various limitations, such as a lack of consideration of "counter-evidence" (Ayoub et al., 2013), sensitivity to the arbitrary scope of hazards (Cyra and Gorski, 2011), and the problem of extracting expert judgments (Nair et al., 2015b).

From another perspective, our work is an application of D-S theory on safety or risk assessment. Similar applications aim to overcome the issue of the lack of precise

data. Démotier et al. (2006) was one of the first paper to deal with uncertainties in dependability analyses, presenting an application in the water treatment. However this paper only considered uncertainties on basic input data (failure rates, latency), and not uncertainties in the logic itself (only pure OR and pure AND gates were considered and not mixed gates, which is one of the major originality of the present paper). Abdallah et al. (2014) model and combine statistical observations (probabilistic uncertainty) and expert assessment (epistemic uncertainty) to predict the centennial sea level for future flood risk analysis. The combination is a nominal application of Dempster's rule.

7. Conclusion

In this paper, we studied the issue of the justification of safety assurances in critical systems via an evidence-based approach. In particular, we focus on the quantitative assessment of confidence in safety cases. We propose a confidence propagation model that integrates different inference types. Our systematic approach uses D-S theory to develop the confidence propagation model. First, we identify the factors that influence confidence in an argument; they are formally defined as *trustworthiness:* $trust = (bel, uncer, disb)$ and *appropriateness:* $appr = (w_i, < TYPE >, v)$. These definitions are specified in more detail as a function of different argument structures (simple and multi-node), and inference types (complementary and redundant). Corresponding confidence aggregation rules are developed, and finally they are generalized into aggregation rules for n-node arguments.

This study concerns a relatively novel subject that combines quantitative uncertainty assessment with subjective reasoning. The proposed approach overcomes many of the limitations identified in the literature regarding the definition and aggregation of confidence measures. Nonetheless, several issues remain to be resolved:

- How to include counterarguments in the confidence assessment? In this paper, we only consider safety cases with positive evidence. To be more compatible with other safety argument notations, the implications of counterarguments should be developed.

- How to combine expert opinions? We made the assumption that only one expert judgment is given for a statement and therefore do not need to combine several judgments. But combining expert judgments for a same statement may face two major issues: conflict an dependency. To deal with the second issue it is commonly admitted that the combination rule used must be idempotent. Some rules, like the cautious rule (Denœux, 2008), the cautious-adaptive

rule (Kallel and Le Hégarat-Mascle, 2009) or the idempotent conjunctive and disjunctive rules (Klein et al., 2018) have this property

- How to integrate the proposed model into a comprehensive framework that encompasses confidence parameter determination through to final decision-making? We proposed a framework in a previous paper (Wang et al., 2017), which is based on a transformation of qualitative expert opinions into quantitative belief parameters, and then back to qualitative values for decision making. Many issues remain open; in particular we plan to explore a qualitative approach from the experts opinions to the decision.

- How our approach could be included in a certification process? Currently, for instance, for hardware, we must demonstrate that a system is "acceptably safe" by calculating failure rates or probabilities. When it comes to software, process-based approaches applying best practices are used to ensure integrity. This paper proposes an approach to make explicit the rationale of combining these best practices and their impact on confidence on the system integrity. Many benefits can be induced, such as allowing more flexibility in the choices of the best practices, or even including new technologies usually avoided in safety critical domain.

References

Abdallah, N. B., Mouhous-Voyneau, N., Denoeux, T., 2014. Combining statistical and expert evidence using belief functions: Application to centennial sea level estimation taking into account climate change. International Journal of Approximate Reasoning 55 (1), 341–354.

Ayoub, A., Chang, J., Sokolsky, O., Lee, I., 2013. Assessing the overall sufficiency of safety arguments. In: 21st Safety-Critical Systems Symposium (SSS'13), Bristol, UK. pp. 127–144.

Ayoub, A., Kim, B., Lee, I., Sokolsky, O., 2012. A systematic approach to justifying sufficient confidence in software safety arguments. In: Conf. on Computer Safety, Reliability, and Security (Safecomp), Magdeburg, Germany. Springer, pp. 305–316.

Bishop, P., Bloomfield, R., 1998. A methodology for safety case development. In: Industrial Perspectives of Safety-Critical Systems, Proceedings of the Sixth Safety-critical Systems Symposium, Birmingham, UK. Springer, pp. 194–203.

Bloomfield, R., Littlewood, B., Wright, D., 2007. Confidence: its role in dependability cases for risk assessment. In: 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK. pp. 338–346.

Bloomfield, R. E., Guerra, S., Miller, A., Masera, M., Weinstock, C. B., 2006. International working group on assurance cases (for security). Security & Privacy, IEEE 4 (3), 66–68.

Cyra, L., Gorski, J., 2007. Supporting compliance with security standards by trust case templates. In: 2nd International Conference on Dependability of Computer Systems (DepCoS-RELCOMEX). IEEE, Wrocaw, Poland, pp. 91–98.

Cyra, L., Gorski, J., 2011. Support for argument structures review and assessment. Reliability Engineering & System Safety 96 (1), 26–37.

Démotier, S., Schon, W., Denœux, T., 2006. Risk assessment based on weak information using belief functions: a case study in water treatment. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 36 (3), 382–396.

Dempster, A. P., 2008. The dempster-shafer calculus for statisticians. International Journal of Approximate Reasoning 48 (2), 365–377.

Denney, E., Pai, G., Habli, I., 2011. Towards measurement of confidence in safety cases. In: International Symposium on Empirical Software Engineering and Measurement (ESEM), Alberta, Canada. IEEE, pp. 380–383.

Denœux, T., 2008. Conjunctive and disjunctive combination of belief functions induced by nondistinct bodies of evidence. Artificial Intelligence 172 (2-3), 234–264.

Duan, L., Rayadurgam, S., Heimdahl, M. P., Ayoub, A., Sokolsky, O., Lee, I., 2014. Reasoning about confidence and uncertainty in assurance cases: A survey. In: Software Engineering in Health Care, International Workshop on Software Engineering in Health Care, International Symposium on Foundations of Health Informatics Engineering and Systems (SEHC 2014, FHIES 2014), Washington, USA. Springer, pp. 64–80.

EN50129, 2003. Railway applications - Safety related electronic systems for signaling. CENELEC, European Committee for Electrotechnical Standardization.

Govier, T., 2013. A practical study of argument. Wadsworth, Cengage Learning.

Graydon, P. J., Holloway, C. M., 2017. An investigation of proposed techniques for quantifying confidence in assurance arguments. Safety Science 92, 53 – 65.

Guiochet, J., Do Hoang, Q. A., Kaaniche, M., 2015. A model for safety case confidence assessment. In: Computer Safety, Reliability, and Security (Safecomp), Delft, Netherlands. Springer, pp. 313–327.

Guo, B., 2003. Knowledge representation and uncertainty management: applying bayesian belief networks to a safety assessment expert system. In: International Conference on Natural Language Processing and Knowledge Engineering. IEEE, Beijing, China, pp. 114–119.

Hawkins, R., Kelly, T., Knight, J., Graydon, P., 2011. A new approach to creating clear safety arguments. In: Advances in systems safety, Proceedings of the Nineteenth Safety-Critical Systems Symposium, Southampton, UK. Springer, pp. 3–23.

Hobbs, C., Lloyd, M., 2012. The application of bayesian belief networks to assurance case preparation. In: Achieving Systems Safety, Proceedings of the Twentieth Safety-Critical Systems Symposium, Bristol, UK. Springer, pp. 159–176.

ISO26262, 2011. Software considerations in airborne systems and equipment certification. International Organization for Standardization (ISO).

ISO/IEC-Guide51, 1999. Safety aspects guidelines for their inclusion in standards. Organisation internationale de normalisation (ISO) / Commision Internationale d'Électrotechnique (IEC).

ISO/IEC15026-2, 2011. Systems and software engineering - systems and software assurance - part 2: Assurance case. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC).

Kallel, A., Le Hégarat-Mascle, S., 2009. Combination of partially non-distinct beliefs: The cautious-adaptive rule. International Journal of Approximate Reasoning 50 (7), 1000–1021.

Kelly, T., 1998. Arguing safety - a systematic approach to safety case management. Ph.D. thesis, Department of Computer Science, University of York.

Kelly, T., McDermid, J., 1997. Safety case construction and reuse using patterns. In: Computer Safety, Reliability, and Security (Safecomp),York, UK. Springer, pp. 55–69.

Kelly, T., Weaver, R., 2004. The goal structuring notation–a safety argument notation. In: Proceedings of the Dependable Systems and Networks 2004, workshop on assurance cases, Florence, Italy.

Klein, J., Destercke, S., Colot, O., 2018. Idempotent conjunctive and disjunctive combination of belief functions by distance minimization. International Journal of Approximate Reasoning 92, 32–48.

Menon, Catherine, C., Hawkins, R., McDermid, J., 2009. Defence standard 00-56 issue 4: Towards evidence-based safety standards. In: Safety-Critical Systems: Problems, Process and Practice. Springer, pp. 223–243.

Mercier, D., Quost, B., Denœux, T., 2005. Contextual discounting of belief functions. In: European Conference on Symbolic and Quantitative Approaches to Reasoning and Uncertainty, Barcelona, Spain. Springer, pp. 552–562.

Nair, S., de la Vara, J. L., Sabetzadeh, M., Falessi, D., 2015a. Evidence management for compliance of critical systems with safety standards: A survey on the state of practice. Information and Software Technology 60, 1–15.

Nair, S., Walkinshaw, N., Kelly, T., de la Vara, J. L., Nov 2015b. An evidential reasoning approach for assessing confidence in safety evidence. In: 2015 IEEE 26th International Symposium on Software Reliability Engineering (ISSRE), Washington DC, USA. pp. 541–552.

OMG, 2018. Object managment group: Structured assurance case metamodel - SACM, version 2.0.

Shafer, G., 1976. A mathematical theory of evidence. Vol. 1. Princeton university press Princeton.

Toulmin, S. E., 1969. The uses of argument. Cambridge University Press.

Wang, R., May 2018. Confidence in safety argument - An assessment framework based on belief function theory. Ph.D. thesis, Institut national des sciences appliquées de Toulouse.

Wang, R., Guiochet, J., Motet, G., 2017. Confidence assessment framework for safety arguments. In: International Conference on Computer Safety, Reliability, and Security (Safecomp), Trento, Italy. Springer, pp. 55–68.

Wang, R., Guiochet, J., Motet, G., Schön, W., 2016. DS theory for argument confidence assessment. In: International Conference on Belief Functions. Springer, Prague, Czech, pp. 190–200.

Wang, R., Guiochet, J., Motet, G., Schn, W., 2018. Modelling confidence in railway safety case. Safety Science 110, 286–299.

Yuan, C., Wu, J., Liu, C., Yang, H., 2017. A subjective logic-based approach for assessing confidence in assurance case. International Journal of Performability Engineering 13 (6), 807.