

A Subjective Logic-Based Approach for Assessing Confidence in Assurance Case

Chunchun Yuan, Ji Wu*, Chao Liu, Haiyan Yang

School of Computer Science and Engineering, Beihang University, Beijing, China

Abstract

Assurance case has been widely used to justify safety, security and other properties of systems. The extent we can trust the assurance case, i.e., confidence in assurance case, is still an open issue in the area. This paper proposes a subjective logic based approach to assess the confidence in assurance case. Compare to other quantitative tools such as Bayesian Belief Network or Dempster-Shafer theory, subjective logic can (1) handle uncertainty and vagueness that usually are contained in expert opinions, and (2) provide appropriate logic operators to deal with different argument types. In the paper, we firstly define the concepts of confidence, sufficiency and necessity to measure the affecting factors to the confidence. Then, we identify four basic argument types and define confidence propagation rules for them. The confidence in assurance case can be calculated iteratively from the bottom up. The application of the proposed approach is illustrated by an industry case study.

Keywords: assurance case; confidence assessment; subjective logic

(Submitted on July 25, 2017; Revised on August 30, 2017; Accepted on September 15, 2017)

(This paper was presented at the Third International Symposium on System and Software Reliability.)

© 2017 Totem Publisher, Inc. All rights reserved.

1. Introduction

Assurance case is a collection of auditable claims, arguments, and evidence created to support the contention that a defined system/service will satisfy the particular requirements [19], such as safety (thus becoming a safety case), reliability, or security. Assurance cases have been used in many industries, especially in safety-critical areas. A structured assurance case explicitly explains how the evidence supports the claim through the argument. However, both the evidence and argument are normally imperfect because of the inevitable fallibility of human and limitations of time and technologies [2,17,18]. Thus, the argued result of claim through the argument and evidence usually are not 100% sure. To measure the imperfection and unreason in assurance case, many researchers use confidence assessment approaches to assess the confidence in assurance case [10].

Most of the existing confidence assessment approaches are based on Bayesian Belief Network (BBN) or Dempster-Shafer theory (DST) [10,21]. In approaches based on BBN, each node of the BBN usually represents a claim or evidence item in assurance case and each arrow from one node to another indicates argument relationship of them. The analyst supplies probability data for the leaf nodes and conditional probability tables or formulae for non-leaf nodes to calculate the probability of them. Approaches based on DST differ from BBN-based approaches in that they reason about both the extent of belief in opinions (e.g., {high, moderate, low}) and the uncertainty in those opinions ($P(\text{uncertainty}) = 1 - (P(\text{high}) + P(\text{moderate}) + P(\text{low}))$). DST is a potentially valuable tool when knowledge is obtained from expert's elicitation, which normally is the case of confidence assessment. The typical application of DST is belief fusion, which combines different beliefs from different sources into one belief.

* Corresponding author.

E-mail address: wuji@buaa.edu.cn.

Subjective logic [15] is another quantitative tool that takes uncertainty into consideration. Similar to DST, subjective logic also defines the belief fusion operator to combine different opinions. Moreover, subjective logic defines other logic operators, such as addition, multiplication, division and conditional reasoning. We believe that subjective logic provides more applicability than DST to deal with the diverse inference logics (i.e., argument types) in assurance case. For example, for the two evidence items which may have AND logic and OR logic between them to support one claim, we can use a multiplication operator or comultiplication operator in subjective logic to manage the logics respectively, whereas DST does not provide corresponding operators.

In this paper, we propose a novel confidence assessment approach that based on subjective logic. The paper makes the following specific contributions:

- We introduce the concepts and operators in subjective logic into the confidence assessment in assurance case. There are other researchers that try to apply subjective logic in this area [5,6]. However, they just use belief fusion operator in their papers, other operators are not explicitly discussed. Instead, we use different operators to calculate the confidence of different argument types in assurance case.
- Based on the law of total probability [16], $P(B) = P(B|A)P(A) + P(B|\bar{A})P(\bar{A})$, we define the concepts of confidence (i.e., $P(B)$ and $P(A)$), sufficiency of argument (i.e., $P(B|A)$) and necessity of argument (i.e., $1 - P(B|\bar{A})$). The concepts provide the basis for further calculation of the confidence.
- We identify four basic argument types in assurance case: one-to-one argument, alternative argument, conjunction argument and disjunction argument. Most of the arguments in assurance cases can be treated as combinations of the four argument types.
- We present a bottom-up approach to assess the confidence in assurance case. Propagation rules that deal with the four argument types are analyzed in our approach.

A case study based on a safety-critical industry case is given to show the effectiveness of the approach.

The rest of the paper is organized as follows. Section 2 presents the background. Section 3 describes our approach in detail, including definitions and assessment approach based on subjective logic. Section 4 presents an industry case study to illustrate the application of our approach. Section 5 presents related work; Section 6 concludes this paper and presents our future research directions.

2. Background

This section provides a brief overview of the relevant background information required to understand our proposed approach.

2.1. Assurance Case and GSN

Assurance case is defined as a collection of auditable claims, arguments, and evidence created to support the contention that a defined system/service will satisfy the particular requirements [19].

The idea behind an argument is reasoning from premise(s) to conclusion as follows:

Premise 1
(AND, OR, ...) Premise 2
 ...
(AND, OR, ...) Premise n
So, Conclusion

The conclusion is the claim that an argument wants to argue. The premise is a statement that used to justify a conclusion. A premise can be stated in different types: it can be an assumption, in which case the premise is accepted without further justification in the assurance case; it can be a sub-claim which is justified further; or it can be an evidence assertion which is a statement about the evidence, such as statement related to properties of evidence and interpretation of evidence. Both the premise and conclusion are a statement that can be argued to be TRUE or FALSE.

The terms “premise” and “conclusion” are relative. The premise of one reasoning step may itself need further reasoning support and will become the conclusion of a subsequent supporting argument. This gives rise to hierarchical argument

structures in which arguments are established by the composition of a number of ‘premises-conclusion’ reasoning steps in order to support an overall conclusion.

The Goal Structuring Notation (GSN) [7], a graphical argumentation notation, explicitly represents the individual elements of any argument (requirements, claims, evidence and context) and (perhaps more significantly) the relationships that exist between these elements (i.e. how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument). The principal symbols of the notation are shown in Figure 1.

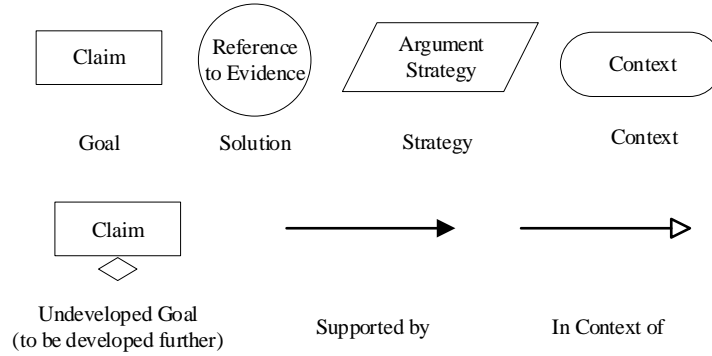


Figure 1. Principal elements of GSN

2.2. Subjective Logic

Subjective logic is a probabilistic logic that uses subjective opinions as input and output variables. The general idea of subjective logic is to extend probabilistic logic by explicitly including uncertainty about probabilities and subjectivity in different beliefs, as illustrated in Figure 2. The main concepts and formulas that used in this paper are briefly listed as follows:

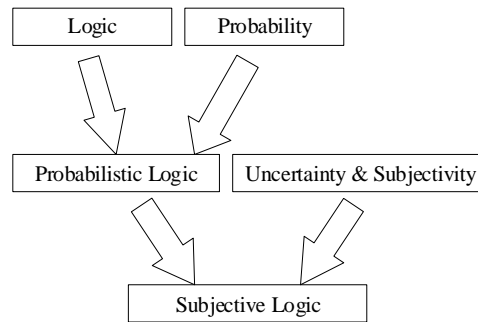


Figure 2. The general idea of subjective logic

Domain: Let \mathbf{X} denotes a domain in subjective logic. A domain represents the possible states of a variable situation. The different values of a domain are assumed to be exclusive and exhaustive, which means that the variable situation can only be in one state at any moment in time, and that all possible state values are included in the domain.

Opinion: Arguments in subjective logic are called subjective opinions, or opinions for short. An opinion can contain uncertainty mass in the sense of uncertainty about probabilities. An opinion can be expressed as a composite function $\omega_X^A = (\mathbf{b}_X, u_X, \mathbf{a}_X)$, consisting of the belief mass distribution \mathbf{b}_X , the uncertainty mass u_X , and the base rate distribution \mathbf{a}_X , where the subscript $X \in \mathbf{X}$ indicates the target variable or proposition to which the opinion applies, and the superscript A indicates the subject agent who holds the opinion. Notice that, an opinion is equivalent to a Dirichlet PDF (probability density function) over X , according to a specific bijective mapping.

Belief Mass Distribution: \mathbf{b}_X assigns belief mass to possible values of the variable $X \in \mathbf{X}$. The formal definition of belief mass distribution is: $\mathbf{b}_X: \mathbf{X} \rightarrow [0,1]$, with the additivity requirement $u_X + \sum_{X \in \mathbf{X}} \mathbf{b}_X(x) = 1$.

Base Rate Distribution: \mathbf{a}_X assigns base rate probability to possible values of $X \in \mathbf{X}$, is an additive probability distribution, formally expressed as: $\mathbf{a}_X: \mathbf{X} \rightarrow [0,1]$, with the additivity requirement $\sum_{X \in \mathbf{X}} \mathbf{a}_X(x) = 1$.

Binomial Opinion: Let $\mathbf{X} = \{x, \bar{x}\}$ be a binary domain with binomial random variable $\in \mathbf{X}$. A binomial opinion about the truth of value x is the ordered quadruplet $\omega_x = (b_x, d_x, u_x, a_x)$, where $b_x + d_x + u_x = 1$. A binomial opinion is equivalent to a Beta PDF under a specific bijective mapping.

Binomial Multiplication: Let $\mathbf{X} = \{x, \bar{x}\}$ and $\mathbf{Y} = \{y, \bar{y}\}$ be two separate domains, and let $\omega_x = (b_x, d_x, u_x, a_x)$ and $\omega_y = (b_y, d_y, u_y, a_y)$ be independent binomial opinions on x and y respectively. The binomial opinion $\omega_{x \wedge y}$ on the conjunction $x \wedge y$ is computed as $\omega_{x \wedge y} = \omega_x \cdot \omega_y$.

Binomial Comultiplication: Let $\mathbf{X} = \{x, \bar{x}\}$ and $\mathbf{Y} = \{y, \bar{y}\}$ be two separate domains, and let $\omega_x = (b_x, d_x, u_x, a_x)$ and $\omega_y = (b_y, d_y, u_y, a_y)$ be independent binomial opinions on x and y respectively. The binomial opinion $\omega_{x \vee y}$ on the disjunction $x \vee y$ is computed as $\omega_{x \vee y} = \omega_x \sqcup \omega_y$.

Binomial Deduction: Let $\mathbf{X} = \{x, \bar{x}\}$ and $\mathbf{Y} = \{y, \bar{y}\}$ be binary domains where there is a degree of relevance of variable $X \in \mathbf{X}$ to variable $Y \in \mathbf{Y}$. Assume an analyst who has the opinion $\omega_{y|x} = (b_{y|x}, d_{y|x}, u_{y|x}, a_y)$ about y being true given x , the opinion $\omega_{y|\bar{x}} = (b_{y|\bar{x}}, d_{y|\bar{x}}, u_{y|\bar{x}}, a_y)$ about y being true given NOT x , and finally the opinion $\omega_x = (b_x, d_x, u_x, a_x)$ about x itself. The deduced opinion $\omega_{y||x} = (b_{y||x}, d_{y||x}, u_{y||x}, a_y)$ is computed as $\omega_{y||x} = \omega_x \odot (\omega_{y|x}, \omega_{y|\bar{x}})$.

Belief Fusion: Let $\mathbf{X} = \{x, \bar{x}\}$. Let agent A hold opinion ω_X^A and agent B hold opinion ω_X^B . The superscripts A and B are attributes that identify the respective belief sources or belief owners. These two opinions can be mathematically merged using the belief fusion: $\omega_X^{(A \& B)} = \omega_X^A \diamond \omega_X^B$. There are five belief fusion methods defined in [15] to deal with different fusion situations.

More detailed descriptions of these concepts and other concepts such as Multinomial Multiplication and Multinomial Deduction can be found in [15].

3. Proposed Approach

3.1. Definitions of Affection Factors

One claim is argued to be TRUE or FALSE based on the supporting premises and argument from the premises to claim. General speaking, there are two types of factors that could affect the confidence in assurance case: defects in the premises and defects in the arguments from premises to conclusion. To measure the two types of defects, we define confidence of statement (i.e., premise or conclusion in an argument) and sufficiency and necessity of argument as follows.

3.1.1. Confidence of Statement

For each statement in the argument, there is a real state of the statement under certain contexts, we denote it as $Real(s)$, where s is the statement. The value of $Real(s)$ can be TRUE or FALSE. On the other hand, after performing argument to a statement, an argument result will assign to the statement to denote if the statement is true. We denote the argument result of the statement as $Argu(s)$. The value of $Argu(s)$ also can be TRUE or FALSE.

Note that the real state of a statement is not always equal to its argument result. If they are equal to each other, i.e., $Argu(s) = Real(s)$, then we say the argument result is correct. Otherwise, it is incorrect. Based on this, we give the definition of confidence of statement.

Definition 1 (Confidence of Statement): Confidence of statement is the extent that we believe the argument result of the statement.

We use a subjective opinion to measure the confidence of a statement. The domain of the subjective opinion can be n -ary where $n > 2$ (e.g., {very high, high, moderate, low, very low}) or binary (i.e., {belief, disbelief}). For easily understanding and computing, we use binary domain in this paper as (1). Nevertheless, the definitions and formulas can also apply to n -ary domain.

$$\omega_{conf(s)} = (b_{conf(s)}, d_{conf(s)}, u_{conf(s)}, a_{conf(s)}). \quad (1)$$

Where $b_{conf(s)} = P(Argu(s) = Real(s))$, $d_{conf(s)} = P(Argu(s) \neq Real(s))$, $u_{conf(s)} = 1 - b_{conf(s)} - d_{conf(s)}$.

The $b_{conf(s)}$ denotes the probability of belief to the argument result, $d_{conf(s)}$ denotes the probability of disbelief to the argument result, $u_{conf(s)}$ denotes the probability of uncertainty to the argument result, and $a_{conf(s)}$ is the base rate of the confidence of the statement, denotes the prior probability of confidence of the statement without any argument.

3.1.2. Sufficiency and Necessity of Argument

For a conclusion supported by premises in assurance case, the argument result of the conclusion depends on the argument result from premises. If the argument result from premises is TRUE, then the argument result of the conclusion is TRUE. If the argument result from premises is FALSE, then the argument result of the conclusion is FALSE, as illustrated in (2).

$$\begin{cases} Argu(p) = TRUE \rightarrow Argu(c|p) = TRUE \\ Argu(p) = FALSE \rightarrow Argu(c|p) = FALSE \end{cases} \quad (2)$$

Where $p = (p_1, p_2, \dots, p_n)$ denotes the premises, $Argu(p)$ denotes the argument results of premises, and $Argu(c|p)$ denotes argument result of conclusion inferred from premises p .

However, in the real situation, the real state of premises (denoted as $Real(p)$) is TRUE, the real state of the conclusion (denoted as $Real(c|p)$) is not necessary to be TRUE, since there may have some defects in the argument. We use sufficiency of argument and necessity of argument to depict the defects.

Definition 2 (Sufficiency of Argument): Sufficiency of argument is defined as the extent that we believe the support from premises to conclusion. We use subjective opinion to measure the sufficiency of argument as (3).

$$\omega_{suff(c|p)} = (b_{suff(c|p)}, d_{suff(c|p)}, u_{suff(c|p)}, a_{suff(c|p)}). \quad (3)$$

Where $b_{suff(c|p)} = P(Real(c) = TRUE | Real(p) = TRUE)$, $d_{suff(c|p)} = P(Real(c) = FALSE | Real(p) = TRUE)$, $u_{suff(c|p)} = 1 - b_{suff(c|p)} - d_{suff(c|p)}$.

The $b_{suff(c|p)}$ denotes the probability of belief to the support, the $d_{suff(c|p)}$ denotes the probability of disbelief to the support, the $u_{suff(c|p)}$ denotes the probability of uncertainty to the support, and the $a_{suff(c|p)}$ denotes the prior probability of the support.

Definition 3 (Necessity of Argument): Necessity of argument is defined as the extent that we believe the disputation from premises to conclusion. We use subjective opinion to measure the sufficiency of argument as (4).

$$\omega_{nece(c|p)} = (b_{nece(c|p)}, d_{nece(c|p)}, u_{nece(c|p)}, a_{nece(c|p)}). \quad (4)$$

Where $b_{nece(c|p)} = P(Real(c) = FALSE | Real(p) = FALSE)$, $d_{nece(c|p)} = P(Real(c) = TRUE | Real(p) = FALSE)$, $u_{nece(c|p)} = 1 - b_{nece(c|p)} - d_{nece(c|p)}$.

The $b_{nece(c|p)}$ denotes the probability of belief to the disputation, the $d_{nece(c|p)}$ denotes the probability of disbelief to the disputation, the $u_{nece(c|p)}$ denotes the probability of uncertainty to the disputation, and the $a_{nece(c|p)}$ denotes the prior probability of the disputation.

Sufficient condition is a special set of premises when $\omega_{suff(c|p)} = (1, 0, 0, a)$, which means if argument from the premises is true infers that conclusion is 100% true.

Necessary condition is another special set of premises when $\omega_{nece(c|p)} = (1, 0, 0, a)$, which means if argument from the premises is false infers that conclusion is 100% false.

3.2. Argument Types

The argument types between premises and conclusion can be complex. However, in this paper, we discuss four basic argument types: (1) one-to-one argument, (2) alternative argument (3) conjunction argument, and (4) disjunction argument. Most of other arguments can be seen as the combinations of the four basic argument types.

- The most basic argument, one-to-one argument, is applied in the case that the claim is supported by a sub-claim or evidence directly.
- Alternative argument is the argument that each of supporting premises could independently support or dispute the whole conclusion. It is often useful to combine the premises from different sources, viewpoints or aspects in order to produce a “*consensus*” conclusion.
- Conjunction argument is an argument that conclusion is true when all the premises are true.
- Disjunction argument is used when the conclusion can be supported by anyone of the premises. Conjunction and disjunction argument express ‘AND’ logic and ‘OR’ logic respectively.

A brief compare of alternative argument, conjunction argument, and disjunction argument is illustrated in Table 1.

Table 1. Compare of Different Argument Types

	Premise 1	Premise 2	Conclusion		
			Alternative Argument	Conjunction Argument	Disjunction Argument
Argument Result	TRUE	TRUE	TRUE	TRUE	TRUE
	TRUE	FALSE	—*	FALSE	TRUE
	FALSE	TRUE	—	FALSE	TRUE
	FALSE	FALSE	FALSE	FALSE	FALSE

*In alternative argument, if argument results of premise 1 and premise 2 are different means that at least one of them is not sufficient or necessary enough to support/dispute the conclusion.

GSN does not explicitly provide the notation to describe different argument types. We simply extend the notations by adding “CONSENSUS”, “AND” and “OR” in the linkage. Examples of the four argument types and our extensions to GSN are illustrated in Figure 3.

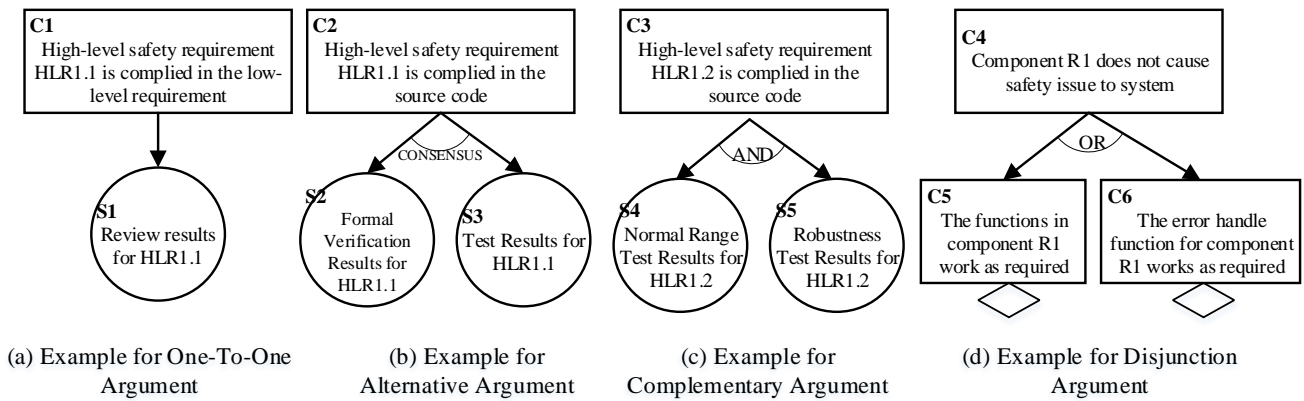


Figure 3. Examples of argument types.

3.3. Assessment Approach

Due to the hierarchical structure of assurance case, the confidence of premises will propagate to the conclusion through the argument between them. Thus, the confidence in assurance case can be assessed from the bottom up. Based on the concepts we defined in the above section, we propose a confidence calculation approach to assess the confidence in assurance case.

The first step of our approach is to collect the basic assessment data, including confidence of leaf nodes (such as evidence, assumptions) and sufficiency and necessity of each argument. Then, confidence propagation rules are iteratively applied to calculate the confidence of high-level claim until the top-level claim has been reached.

3.3.1. Step1: Collect Basic Assessment Data

The basic assessment data include confidence of each evidence, confidence of each assumption, and sufficiency and necessity of each argument. The most common sources of the data are expert judgments [18]. How to effectively collect data from expert judgments and how to judge the data if they are sufficient and trustworthy are important issues that still have not been well solved in existing work [10]. Deal with the issues is our ongoing work, however, in this paper, we do not specify it. For now, we just assume the data collected from the expert judgments are sufficient and trustworthy.

3.3.2. Step2: Calculate the Confidence of Conclusion Iteratively

After collecting the assessment data, we calculate the confidence in assurance case based on the propagation rules iteratively from the bottom up until top-level claim has been reached. Four propagation rules are discussed in the following to deal with four argument types respectively.

3.3.2.1. One-to-One argument

An example of the one-to-one argument is shown in Figure 3(a). To assess the confidence of the conclusion, following data should be already known: (1) confidence of the premise: $\omega_{conf(p)}$; (2) sufficiency of argument: $\omega_{suff(c|p)}$ and (3) necessity of argument: $\omega_{nece(c|p)}$.

Based on our definition of confidence, sufficiency and necessity, the confidence of conclusion is actually a total probability function of confidence of its premise and of the two sub-conditions: sufficiency of argument and necessity of argument. According to the conditional deduction method in [15], which calculate total probability for subjective opinion. We obtain the propagation rule for one-to-one argument as (5)

$$\omega_{conf(c)} = \omega_{conf(p)} \odot (\omega_{suff(c|p)}, \omega_{nece'(c|p)}) \quad (5)$$

Where $\omega_{nece'(c|p)} = (d_{nece(c|p)}, b_{nece(c|p)}, u_{nece(c|p)}, a_{nece(c|p)})$, ‘ \odot ’ is the deduction operator defined in [15].

We give a simple example to show the confidence propagation. As shown in Figure 3(a), claim C1 “High-level safety requirement HLR1.1 is complied with in the low-level requirement” is supported by evidence S1 “Review results for HLR1.1”. The basic data are set as:

- The confidence of evidence S1 is set as $\omega_{conf(s1)} = (0.95, 0.03, 0.02, 0.5)$, which means that the belief in the confidence of evidence S1 is 95%, disbelief in it is 3%, and 2% uncertain about it.
- The sufficiency of argument is set as $\omega_{suff(c1|s1)} = (0.7, 0.2, 0.1, 0.7)$, which means if S1 support C1, 70% we believe the support, 20% we do not believe the support and 10% uncertain.
- The necessity of argument is set as $\omega_{nece(c1|s1)} = (0.9, 0.05, 0.05, 0.9)$, which means if S1 dispute C1, 90% we believe the disputation, 5% we do not believe the disputation and 5% uncertain.

According to (5), we obtain the confidence of C1: $\omega_{conf(c)} = (0.67, 0.22, 0.11, 0.41)$, which means that in this example if C1 is argued to be TRUE, 67% that the argument result is believable, 22% that the argument result is not believable and 11% of uncertain about the argument result is believable or not.

3.3.2.2. Alternative argument

A simple example of alternative argument is given in Figure 3(b). Both formal verification results and test results can independently support the claim “High-level safety requirement HLR1.2 is complied with in the source code”.

To assess the confidence of the conclusion, following data should be already known: (1) confidence of the premise: $\omega_{conf(p1)}$ and $\omega_{conf(p2)}$, (2) sufficiency of argument from each premise to the conclusion: $\omega_{suff(c|p1)}$ and $\omega_{suff(c|p2)}$, and (3) necessity of argument from each premise to the conclusion: $\omega_{nece(c|p1)}$ and $\omega_{nece(c|p2)}$.

To calculate the confidence of conclusion, firstly we decompose the conclusion C to two conclusions C' and C'' , which are supported by $P1$ and $P2$ respectively, as illustrated in Figure 4.

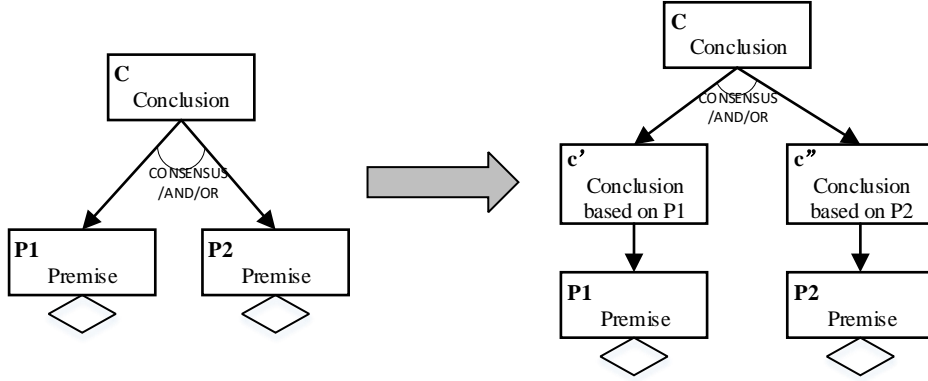


Figure 4. Decomposition of alternative/conjunction/disjunction argument.

According to (5), it is easy to calculate the confidences of C' and C'' :

$$\begin{aligned}\omega_{conf}(c') &= \omega_{conf}(p1) \odot (\omega_{suff}(c|p1), \omega_{nece'}(c|p1)) \\ \omega_{conf}(c'') &= \omega_{conf}(p2) \odot (\omega_{suff}(c|p2), \omega_{nece'}(c|p2))\end{aligned}\quad (6)$$

Note that C' and C'' share the same conclusion with C but from different sources. In the subjective logic, belief fusion method allows evidence and opinions from different sources about the same domain of interest to be merged. Thus, we can use belief fusion method in subjective logic to calculate the confidence of the claim:

$$\omega_{conf}(c) = \omega_{conf}(c') \diamond \omega_{conf}(c'') \quad (7)$$

Where ' \diamond ' is the belief fusion operator. Belief can be fused in various ways to fit with different fusion situations, such as belief constraint fusion, cumulative belief fusion, weighted belief fusion and so on. Detailed analysis of the different belief fusions can be found in [15]. We choose weighted belief fusion operator in our case study.

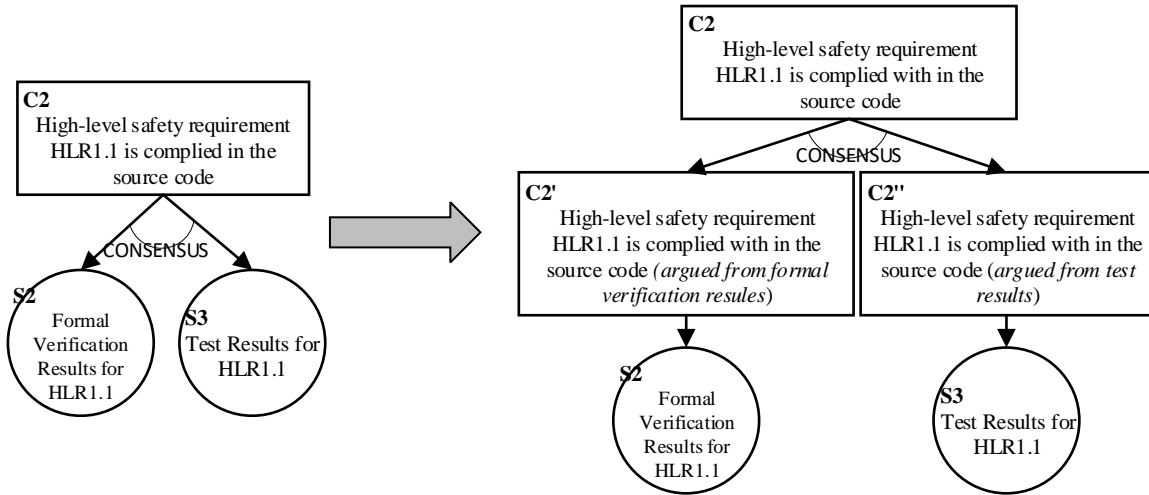


Figure 5. Examples of alternative argument decomposition.

Taking Figure 3(b) as an example, the argument can decompose into assurance case illustrated in Figure 5. The basic data are set as:

- The confidence of evidence S2 is set as $\omega_{conf}(s_2) = (0.9, 0.05, 0.05, 0.5)$, the sufficiency of argument from S2 to the claim C2 is set as $\omega_{suff}(c_2|s_2) = (1, 0, 0, 0.5)$, and the necessity of argument from S2 to the claim C2 is set as $\omega_{nece}(c_2|s_2) = (1, 0, 0, 0.5)$, which means S2 is sufficient and necessary condition to C2.
- The confidence of evidence S3 is set as $\omega_{conf}(s_3) = (0.8, 0.1, 0.1, 0.5)$, the sufficiency of argument from S3 to the claim C2 is set as $\omega_{suff}(c_2|s_3) = (0.9, 0, 0.1, 0.5)$, and the necessity of argument from S3 to the claim C2 is set as $\omega_{nece}(c_2|s_3) = (1, 0, 0, 0.5)$, which means S3 is necessary condition to C2.

According to (6) and (7), we obtain the confidence of C2: $\omega_{conf}(c_2) = (0.865, 0.060, 0.075, 0.488)$, which means that in this example if C2 is argued to be TRUE, 86.5% probability that the argument result is believable, 6.0% probability that the argument result is not believable and 7.5% uncertain about if the argument result is believable or not.

3.3.2.3. Conjunction argument

Figure 3(c) gives an example of the conjunction argument. S4 and S5 support normal range and abnormal range of the requirement HLR1.1 respectively.

Notice that, since each premise only supports part of the conclusion, sufficiency and necessity of each argument from premise to the whole conclusion may not easy to obtain. Thus, in our approach, we decompose the conclusion into two conclusions C' and C'', which is the covered parts of conclusion argued from P1 and P2 respectively, as illustrated in Figure 4. The sufficiency and necessity of argument from P1 and P2 to C' and C'' are more convenient to get.

To assess the confidence of the conclusion, following data should be already known: (1) confidence of the premises: $\omega_{conf}(p_1)$ and $\omega_{conf}(p_2)$, (2) sufficiency of argument from premise to its covered part of conclusion: $\omega_{suff}(c'|p_1)$ and $\omega_{suff}(c''|p_2)$, (3) necessity of argument from premise to its covered part of conclusion: $\omega_{nece}(c'|p_1)$ and $\omega_{nece}(c''|p_2)$, and (4) sufficiency and necessity of argument from C' and C'' to C: $\omega_{suff}(c|c'\wedge c'')$ and $\omega_{nece}(c|c'\wedge c'')$.

We say P1 and P2 are *homogeneous* if $\omega_{suff}(c'|p_1) = \omega_{suff}(c''|p_2)$ and $\omega_{nece}(c'|p_1) = \omega_{nece}(c''|p_2)$, otherwise they are *heterogeneous*.

The confidences of C' and C'' can be obtained from (6). Notice that, C is the function of logic AND on C' and C''. Thus, we use multiplication operator in subjective logic that corresponds to logic AND to compute the confidence of C as (8) and (9).

$$\omega_{conf}(c|c'\wedge c'') = \omega_{conf}(c') \cdot \omega_{conf}(c'') \quad (8)$$

$$\omega_{conf}(c) = \omega_{conf}(c|c'\wedge c'') \odot (\omega_{suff}(c|c'\wedge c''), \omega_{nece}(c|c'\wedge c'')) \quad (9)$$

Where ' \cdot ' is multiplication operator that corresponds to the AND operator in subjective logic.

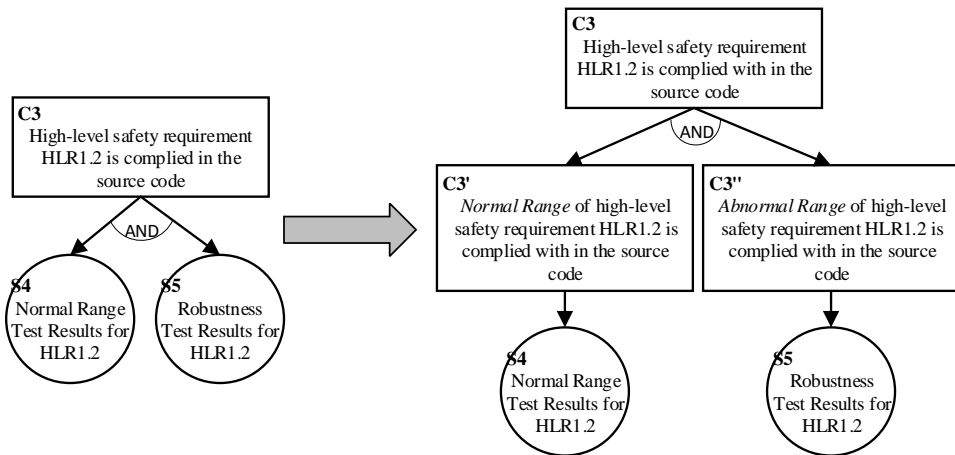


Figure 6. Examples of conjunction argument decomposition.

Take Figure 3(c) as an example, the argument can decompose into assurance case illustrated in Figure 6. The basic data are set as:

- The confidence of evidence S4 is set as $\omega_{conf}(s_4) = (0.9, 0, 0.1, 0.5)$, the sufficiency of argument from S4 to the claim C3' is set as $\omega_{suff}(c3'|s_4) = (0.8, 0.1, 0.1, 0.5)$, and the necessity of argument from S4 to the claim C3' is set as $\omega_{nece}(c3'|s_4) = (1, 0, 0, 1)$, which means S4 is necessary condition to C3'.
- The confidence of evidence S5 is set as $\omega_{conf}(s_5) = (0.7, 0.1, 0.2, 0.5)$, the sufficiency of argument from S5 to the claim C3'' is set as $\omega_{suff}(c3''|s_5) = (0.8, 0.1, 0.1, 0.5)$, and the necessity of argument from S5 to the claim C3'' is set as $\omega_{nece}(c3''|s_5) = (1, 0, 0, 1)$, which means S5 is necessary condition to C3''.
- the sufficiency of argument from (C3' \wedge C3'') to the claim C3 is set as $\omega_{suff}(c|c' \wedge c'') = (1, 0, 0, 1)$, and the necessity of argument from (C3' \wedge C3'') to the claim C3 is set as $\omega_{nece}(c|c' \wedge c'') = (1, 0, 0, 1)$, which means (C3' \wedge C3'') is sufficient and necessary condition to C3.

According to (6), (8) and (9) we obtain the confidence of C3: $\omega_{conf}(c_3) = (0.498, 0.271, 0.231, 0.177)$, which means that in this example if C3 is argued to be TRUE, 49.8% probability that the argument result is believable, 27.1% probability that the argument result is not believable and 2% uncertain about if the argument result is believable or not.

3.3.2.4. Disjunction Argument

An example of a disjunction argument is illustrated in Figure 3(d). The functions in component R1 work as required or the error handler function for component R1 works as required can infer that component R1 does not cause safety issues to the system.

To assess the confidence of the conclusion, we decompose the conclusion C to two conclusions C' and C'', which are supported by P1 and P2 respectively. The following data should be already known: (1) confidence of the premise: $\omega_{conf}(p_1)$ and $\omega_{conf}(p_2)$, (2) sufficiency of argument from each premise to the conclusion: $\omega_{suff}(c|p_1)$ and $\omega_{suff}(c|p_2)$, and (3) necessity of argument from each premise to the conclusion: $\omega_{nece}(c|p_1)$ and $\omega_{nece}(c|p_2)$.

The confidences of C' and C'' can be obtained from (6). Notice that, C is the function of logic OR on C' and C''. Thus, we use comultiplication operator in subjective logic that corresponds to logic OR to compute the confidence of C as (10).

$$\omega_{conf}(c) = \omega_{conf}(c') \sqcup \omega_{conf}(c''). \quad (10)$$

Where ' \sqcup ' is multiplication operator that corresponds to the OR operator in subjective logic.

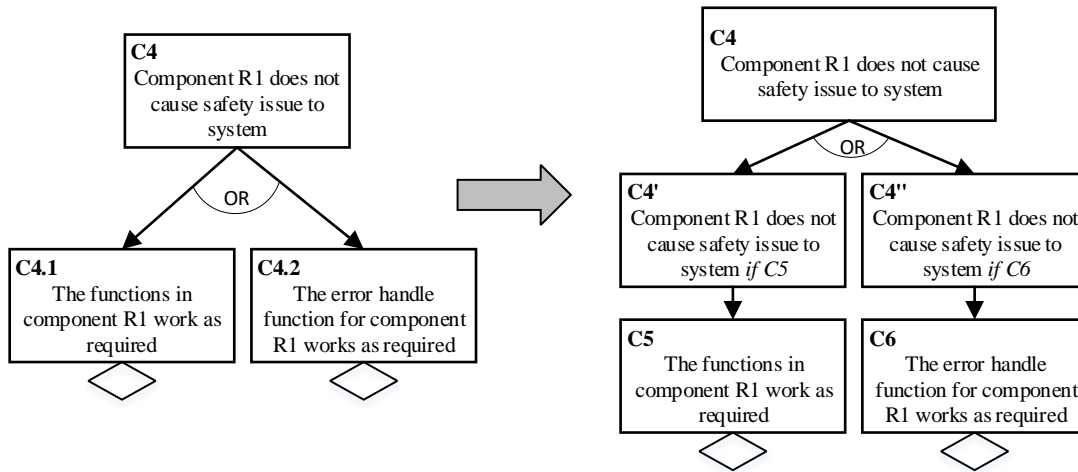


Figure 7. Examples of disjunction argument decomposition.

Take Figure 3(d) as an example, the argument can decompose into assurance case illustrated in Figure 7. The basic data are set as:

- The confidence of claim C5 is set as $\omega_{conf}(c5) = (0.9, 0.05, 0.05, 0.5)$, the sufficiency of argument from C5 to the claim C4' is set as $\omega_{suff}(c4|c5) = (0.8, 0.1, 0.1, 0.5)$, and the necessity of argument from C5 to the claim C4' is set as $\omega_{nece}(c4|c5) = (0.7, 0.2, 0.1, 0.5)$.
- The confidence of claim C6 is set as $\omega_{conf}(c6) = (0.6, 0.2, 0.2, 0.5)$, the sufficiency of argument from S5 to the claim C4'' is set as $\omega_{suff}(c4|c6) = (0.7, 0.1, 0.2, 0.5)$, and the necessity of argument from S5 to the claim C3'' is set as $\omega_{nece}(c4|c6) = (0.4, 0.2, 0.4, 0.5)$.

According to (6) and (10), we obtain the confidence of C4: $\omega_{conf}(c4) = (0.870, 0.039, 0.091, 0.841)$, which means that in this example if C4 is argued to be TRUE, 87.0% probability that the argument result is believable, 3.9% probability that the argument result is not believable and 9.1% uncertain about if the argument result is believable or not.

4. Industry Case Study

Our case study system is a Real Time Operating System for Avionics (RTOS4A) [24]. RTOS4A provides services and APIs for user applications. Services provided include task management, time management, health management, communication and synchronization, error handling, input and output, memory management, and task scheduling. The RTOS4A system is a safety-critical system since safety-critical avionics applications are deployed on it. The development and verification process of RTOS4A is compliant with DO-178C [20]. To argue the safety of the system, we built a safety case using GSN and collect an amount of data from the development and verification processes. The data have two main characteristics. One characteristic is the data are huge and heterogeneous. We collect data from five continuous releases of the RTOS4A, and the data storage types are various, such as electronic documents, paper documents, logs, manager tools, etc. Another characteristic is that even our industry partner claims the development and verification process is compliant with DO-178C, there are still a lot of inconsistencies between data can be found, and that is also the first motivation that we want use confidence to assess its affecting to assurance case.

Due to the complexity of the system and the confidentiality issues, we cannot provide our safety case detailed in regards to requirements, architecture and the verification results of the system. In the paper, we extract a fragment of our safety case to illustrate our approach, as shown in Figure 8.

One of our strategies to argue the safety of the system is all the safety requirements (include high-level safety requirements and low-level safety requirements) are satisfied in software. The top-level claim of our example is one of the high-level safety requirements, HRA.7.9, is satisfied in software (C1). One strategy to argue the claim is if the claim supported by requirement-based integration testing results (S1.3). Another strategy to argue the claim is the low-level requirements that addressed HRA.7.9 is sufficiently and correctly developed (C1.1) and satisfied in software (C1.2). Review results for low-level requirement (S1.1.1) give supports to the C1.1. And the requirement-based low-level integration testing results for each low-level requirement (S1.2.1.1~S1.2.8.1) are used to argue the claim C1.2 (C1.2.1~C1.2.8).

To assess the confidence in the illustrated assurance case, we perform the approach that defined in section 3.

4.1. Step1: Collect Basic Assessment Data

There are some features of the evidence we found during the data collection:

- The testing for low-level requirements RA7.1~RA7.8 is performed by the same testing group (testing group 1), used same testing tools and conformed to same testing standards. Thus, the evidence S1.2.1.1~S1.2.8.1 are *homogeneous* to each other.
- The testing for high-level requirements is performed by a different testing group (testing group 2) with the testing for low-level requirements. Thus, S1.3 is *heterogeneous* to S1.2.1.1~S1.2.8.1.
- According to the past experience and implementation effect, testing group 1 has more domain experience and competency than testing group 2. Therefore, the sufficiency and necessity of the argument from evidence S1.2.1.1~S1.2.8.1 to claim C1.2.1~C1.2.8 is better than the argument from evidence S1.3 to claim C1.
- Some of the testing results for RA.7.8 are lost, due to negligence in the management of evidence. Other testing results are perfectly saved and managed. Thus, the confidence of evidence S1.2.8.1 is worse than evidence S1.2.1.1~S1.2.7.1.
- Some of the evidence is produced in the early release of the system, such as S1.1.1. That will bring negative affecting to the sufficiency and necessity of argument from evidence S1.1.1 to claim C1.1.

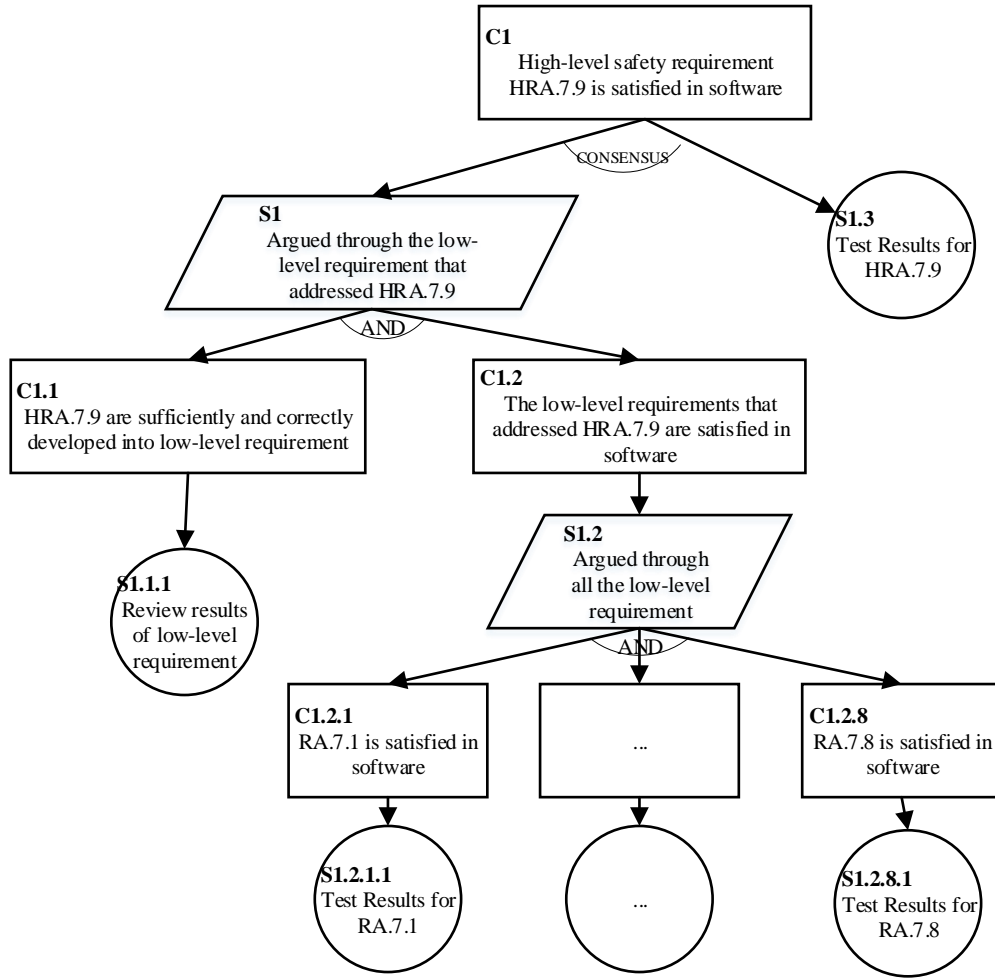


Figure 8. Assurance case of our case study

The experts give the assessment data as Table 2 by reference to the features of the evidence and experiences of past project.

Table 2. Assessment Data of Our Example

Premise(s) / Evidence	Conclusion	Assessment Data		
		Confidence of Evidence	Sufficiency of premise(s) to claim	Necessity of premise(s) to claim
S1.1.1	C1.1	(1, 0, 0, 0.8)	(0.9, 0.05, 0.05, 0.9)	(1, 0, 0, 1)
S1.2.1.1~ S1.2.1.7	C1.2.1~C1.2.7	(1, 0, 0, 0.9)	(0.99, 0.005, 0.005, 0.9)	(1, 0, 0, 1)
S1.2.1.8	C1.2.8	(0.9, 0, 0.1, 0.9)	(0.99, 0.005, 0.005, 0.5)	(1, 0, 0, 1)
S1.3	C1	(1, 0, 0, 0.5)	(0.95, 0.01, 0.04, 0.9)	(1, 0, 0, 1)
(C1.2.1~C1.2.8)	C1.2	-	(1, 0, 0, 1)	(1, 0, 0, 1)
(C1.1, C1.2)	C1	-	(1, 0, 0, 0.9)	(0.9, 0.02, 0.08, 0.8)

4.2. Step2: Calculate the Confidence of Conclusion Iteratively

According to the propagation rules based on different argument types defined before, we iteratively calculate the confidence of each claim until to the top-level claim. The argument types between premises and conclusion are summarized in Table 3. The results of the calculation of the confidence of conclusion are also shown in Table 3.

Table 3. Assessment Results

Premise(s)	Conclusion	Argument Type	Confidence of Conclusion
S1.1.1	C1.1	One-to-One Argument	(0.9, 0.05, 0.05, 0.9)
S1.2.1.1~S1.2.1.7	C1.2.1~C1.2.7	One-to-One Argument	(0.99, 0.005, 0.005, 0.9)
S1.2.1.8	C1.2.8	One-to-One Argument	(0.895, 0.005, 0.100, 0.895)
S1.3	C1'	One-to-One Argument	(0.95, 0.01, 0.04, 0.9)
(C1.2.1~C1.2.8)	C1.2	Conjunction Argument	(0.937, 0.039, 0.024, 0.428)
(C1.1, C1.2)	C1''	Conjunction Argument	(0.884, 0.087, 0.029, 0.385)
(C1', C1'')	C1	Alternative Argument	(0.911, 0.055, 0.034, 0.641)

As the result shows, the confidence of top-level claim is $\omega_{conf(c1)} = (0.911, 0.055, 0.034, 0.641)$, which means that if top-level claim C1 is argued to be TRUE, 91.1% probability that the argument result is believable, 5.5% probability that the argument result is not believable and 3.4% uncertain about if the argument result is believable or not. Using the results, the project managers can decide if the safety claim should be accepted or not.

5. Related Work

The issue of confidence in assurance case has already been addressed by several works.

5.1. Qualitative Approaches

In [13], they introduce *assured safety arguments*, a new structure for arguing safety in which the *safety argument* is accompanied by a *confidence argument* that documents the confidence in the structure and bases of the safety argument. This confidence argument is also represented with GSN as safety argument. For each possible uncertainty source in safety argument, such as inference, context, or solution, they add an Assurance Claim Point (ACP) to it. Then, for each ACP, they build a confidence argument to demonstrate that the ACP is trustworthy and appropriate.

Another proposal [2] also proposes an approach to construct confidence arguments in safety arguments. The authors propose to use *Common Characteristic Map* as a checklist to identify sources of uncertainties and then construct confident arguments.

In summary, qualitative approaches mostly focus on the identification of the weaknesses in an assurance case, and construct another assurance case to illustrate that the weaknesses are acceptable. One potential disadvantage of qualitative approach is that it may lead to complex confidence cases.

5.2. Quantitative Approaches

Although controversial, we still believe that quantitative assessment approaches could help analyze the confidence in assurance case. Beyond our approach, there are some other approaches that aim at quantitatively assessing confidence in assurance case. The different considerations of quantitative tools and argument types of those approaches are summarized in Table 4.

5.2.1. BBN-Based Approach

Some of the proposed approaches are based on Bayesian Belief Network (BBN) [4,14,27]. They construct a BBN by analyzing the factors that could affect the confidence (represented as nodes in BBN) and dependencies among them (represented as edges in BBN). Each leaf node in BBN is associated with a probability, and the probability of non-leaf nodes will be computed by conditional probability tables or other probability functions.

The main difference between subjective logic and BBN is subjective logic takes the uncertainty of probabilities into consideration. We think the inputs of confidence assessment approach are mostly derived from expert's opinion, which often includes uncertainty and subjective in it. Thus, in our approach, we use subjective logic as our mathematic basis.

Table 4. Different Approaches for Quantitative Confidence Assessment

Proposed Approaches	Quantitative Tool	Argument Types and Propagation rules
Our Approach	Subjective Logic	✓
Hobbs 2012 [14]	BBN	×
Zhao 2012 [27]	BBN	×
Denney 2011 [4]	BBN	×
Wang 2016 [22,23]	Dempster-Shafer Theory	✓
Guiochet 2015 [12]	Dempster-Shafer Theory	✓
Ayoub 2013 [1]	Dempster-Shafer Theory	✓
Zeng 2013 [26]	Dempster-Shafer Theory	×
Cyra 2011 [3]	Dempster-Shafer Theory	✓
Duan 2016 [5]	Baconian Probability & Subjective Logic	○
Goodenough 2012 [8]	Baconian Probability	×
Goodenough 2015 [9]	Baconian Probability	×
Yamamoto 2015 [25]	Attribute Value	×
Duan 2015 [6]	Subjective Logic	○
× means the argument type is not considered in the approach; ✓ means the argument types and propagation rules are explicitly defined in the approach; ○ means the argument types are mentioned, however, the propagation rules are not defined in the approach.		

5.2.2. Dempster-Shafer Theory Based Approach

References [1,3,12,22,23,26] are all based on DST. DST is a mathematical theory of evidence, which also consider uncertainty in the opinions. DST use basic probability assignment (BPA) to present an opinion about a statement.

As proved in [15], there is a direct bijective mapping between an opinion in DST and an opinion in subjective logic. The belief fusion operator in DST also can translate to belief constraint fusion operator in subjective logic. Beyond the belief fusion, the subjective logic defines other functions such as conditional reasoning, multiplication and other operators. Lots of them contribute to our work. That is the main reason we use subjective logic rather than DST in our work.

Some of the approaches [1,12,22,23] also identify different argument types and define corresponding propagation rules. However, since there are no logic operators such as multiplication and comultiplication operator in DST, the calculation rules can be very different between them and us. For example, for the conjunction argument (named as disjoint /complementary argument in their approaches), they normally use *weighted average method* to calculate the confidence. That means, the confidence of conclusion is the *middle value* between its premises in their approach no matter what the weights of premises are. However, in our opinion, the logic relationship between premises and conclusion in the conjunction argument is an AND logic, which means the confidence of conclusion must be *smaller* than its two premises. Thus, we believe subjective logic provides more applicability than DST in assessing confidence for different argument types in assurance case.

5.2.3. Others

References [5,6] also use subjective logic as the quantitative tool to assess the confidence in assurance case. However, although they implicitly mention different argument types, they do not provide proper propagation rules for the argument types.

References [5,8,9] use Baconian probability [11] to measure confidence in assurance case. The general premise in Baconian confidence is that there are lists of all “defeaters” (doubts about claim) and eliminated defeaters of them. Suppose a Baconian probability $B(c) = i/n$, means i out of n defeaters have been eliminated. The ratio in Baconian probability is

irreducible, as $3/6$ would represent an entirely different value than $1/2$. The main difficulty in applying Baconian confidence is the collection of the whole list of defeaters.

Yamamoto [25] proposes an approach based on attribute value. The attribute value is defined as a five-point Likert scale $\{-2$ (Strongly unsatisfied), -1 (Unsatisfied), 0 (Unknown), 1 (satisfied), 2 (Strong satisfied) $\}$. They do not consider the uncertainty and other operators either.

In summary, compare with other quantitative tools, subjective logic has following advantages:

- Uncertainty of opinions is considered in subjective logic.
- Subjective logic provides many logic operators. Based on the operators, we can define appropriate propagation rules for different argument types.

Based on those advantages, we use subjective logic as quantitative tool rather than others.

6. Conclusions

In this paper, we propose a subjective logic based approach to assess the confidence in assurance case. In our approach, we follow the law of total probability to define the concepts of confidence, sufficiency of argument and necessity of argument to represent the extent that we believe in the premise and argument respectively. Our approach identifies four basic argument types: one-to-one argument, alternative argument, conjunction argument and disjunction argument. For each argument type, we define propagation rules to assess the confidence in the argument. Then, the confidence in assurance case can be calculated from the bottom up.

How to collect trustworthy assessment data is our immediate future work. Reference [18] provides an inspiring work to do the collection. They develop some confidence argument patterns and questionnaires to collect the assessment data. However, in our opinion, their confidence argument patterns mainly focus on the personnel and processes that produce the evidence. The defects of evidence itself, such as the consistency and completeness of evidence, are not explicitly mentioned in their work. Based on our industry experiences, the defects of evidence appear very often and apparently would affect the confidence in assurance case. One of our future works is to consider them in the collection of assessment data.

Acknowledgements

The work is supported by the Technology Foundation Program (JSZL2014601B008) of the National Defense Technology Industry Ministry.

References

1. A. Ayoub, J. Chang, O. Sokolsky, and I. Lee, "Assessing the Overall Sufficiency of Safety Arguments," in *Safety-Critical Systems Symposium*, SSS'13, Bristol, UK, 2013
2. A. Ayoub, B. G. Kim, I. Lee, and O. Sokolsky, "A Systematic Approach to Justifying Sufficient Confidence in Software Safety Arguments," *Computer Safety, Reliability, and Security*, Springer Berlin Heidelberg, pp. 305-316, 2012
3. L. Cyra and J. Górski, "Support for Argument Structures Review and Assessment," *Reliability Engineering & System Safety*, vol. 96, no. 1, pp. 26-37, 2011
4. E. Denney, G. Pai, and I. Habli, "Towards Measurement of Confidence in Safety Cases," in *2011 International Symposium on Empirical Software Engineering and Measurement*, pp. 380-383, 2011
5. L. Duan, S. Rayadurgam, M. Heimdahl, and O. Sokolsky, "Representation of Confidence in Assurance Cases Using the Beta Distribution," in *IEEE International Symposium on High Assurance Systems Engineering*, pp. 86-93, 2016
6. L. Duan, S. Rayadurgam, M. Heimdahl, O. Sokolsky, and I. Lee, "Representing Confidence in Assurance Case Evidence," *Computer Safety, Reliability, and Security*, Springer International Publishing, pp. 15-26, 2015
7. Goal Structuring Notation Working Group, "GSN Community Standard Version 1," <http://www.goalstructuringnotation.info/>, 2011.
8. J. Goodenough, C. B. Weinstock, and A. Z. Klein, "Toward a Theory of Assurance Case Confidence," Technical Report, Carnegie Mellon University, 2012
9. J. Goodenough, C. B. Weinstock, and A. Z. Klein, "Eliminative Argumentation: A Basis for Arguing Confidence in System Properties," Technical Report, Carnegie Mellon University, 2015
10. P. J. Graydon and C. M. Holloway, "An Investigation of Proposed Techniques for Quantifying Confidence in Assurance Arguments," *Safety Science*, vol. 92, pp. 53-65, 2016
11. P. J. Graydon and C. M. Holloway, "Defining Baconian Probability for Use in Assurance Argumentation," Technical Report, NASA, 2016.

12. J. Guiochet, Q. A. D. Hoang, and M. Kaaniche, "A Model for Safety Case Confidence Assessment," *International Conference on Computer Safety, Reliability, and Security*, pp. 313-327, 2015
13. R. Hawkins, T. Kelly, J. Knight, and P. Graydon, "A New Approach to Creating Clear Safety Arguments," in *Advances in Systems Safety*, pp. 3-23 2011
14. C. Hobbs and M. Lloyd, "The Application of Bayesian Belief Networks to Assurance Case Preparation," *Achieving Systems Safety*, Springer London, 2012, pp. 159-176.
15. A. Jøsang, "Subjective Logic," Springer International Publishing, 2016
16. S. Kokoska and D. Zwillinger, "CRC Standard Probability and Statistics Tables and Formulae, Student Edition," Taylor & Francis, 2000
17. C. I. Menon, R. Hawkins, and J. Mcdermid, "Defence Standard 00-56 Issue 4: Towards Evidence-Based Safety Standards," *Safety-Critical Systems: Problems, Process and Practice*, pp. 223-243, 2013
18. S. Nair, N. Walkinshaw, T. Kelly, and J. L. D. L. Vara, "An Evidential Reasoning Approach for Assessing Confidence in Safety Evidence," in *International Symposium on Software Reliability Engineering*, pp. 541-552, 2015
19. Object Management Group, "Structured Assurance Case Metamodel (SACM)," OMG Document Number: formal/2015-07-01. Object Management Group, 2015
20. RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification, RATC, Inc, 2011.
21. G. Shafer, "A Mathematical Theory of Evidence," Princeton University Press, 1976
22. R. Wang, J. Guiochet, and G. Motet, "A Framework for Assessing Safety Argumentation Confidence," *Software Engineering for Resilient Systems*, pp.3-12, 2016.
23. R. Wang, J. Guiochet, G. Motet, and W. Schön, "D-S Theory for Argument Confidence Assessment," *International Conference on Belief Functions*, Springer International Publishing, 2016.
24. J. Wu, S. Ali, T. Yue, and J. Tian, "Experience Report: Assessing the Reliability of An Industrial Avionics Software: Results, Insights and Recommendations," in *IEEE International Symposium on Software Reliability Engineering*, pp. 218-227, 2013
25. S. Yamamoto, "Assuring Security through Attribute GSN," in *International Conference on It Convergence and Security*, 2015, pp. 1-5.
26. F. Zeng, L. U. Manyan, and D. Zhong, "Using D-S Evidence Theory to Evaluation of Confidence in Safety Case," *Journal of Theoretical & Applied Information Technology*, 2013.
27. X. Zhao, D. Zhang, M. Lu, and F. Zeng, "A New Approach to Assessment of Confidence in Assurance Cases," in *International Conference on Computer Safety, Reliability, and Security*, pp. 79-91, 2012

Chunchun Yuan is currently pursuing his PhD degree at Beihang University. He received his MS degree in JiangSu Aotumation Research Institute in 2011 and BS degree Nankai University in 2007. His research is focused on modelling and verification of safety critical system and software.

Ji Wu is an associate professor and assistant dean of the School of Computer Science and Engineering (SCSE) at Beihang University. He received his PhD degree from Beihang University in 2003 and MS degree from the Second Research Institute of the China Aerospace Science and Industry Group in 1999. He focuses on the industry-oriented researches. His research interests include embedded system and software modeling and verification, software requirement and architecture modeling and verification, safety and reliability assessment, and software testing. He was invited to visit Simula Research Laboratory for 1 year in 2012.

Chao Liu is the Director of Software Engineering Institute (SEI) and Director of Beihang Software Testing and Evaluation Laboratory (BH-STEL), Beihang University, Beijing, China. He is vice director of Software Engineering Technical Committee of China Computer Federation (CCF), vice director of Software Engineering Branch and vice director of System and Software Process Improvement Branch, China Software Industry Association (CSIA). His research interests include software quality engineering, software testing, as well as software process improvement. He received his PhD and MS degrees in Computer Software and Theory at Beihang University and his BS degree in Mathematics at Beijing University of Posts and Telecommunication.

Haiyan Yang, born in 1974. Master and lecturer in Beihang University. Her main research interests include software engineering, software safety and software testing.