Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

USING D-S EVIDENCE THEORY TO EVALUATION OF CONFIDENCE IN SAFETY CASE

[1]FUPING ZENG , [2]MANYAN LU AND [3]DEMING ZHONG
[1]School of Reliability and System Engineering, Beihang University, Beijing, 100191, China
E-mail: [1]zfp@buaa.edu.cn, [2]lmy@buaa.edu.cn, [3]zhongdeming.timothy@gmail.com

ABSTRACT

A safety case provides an explicit means for justifying the safety of a system through a reasoned argument and supporting evidence. However, the acceptance of a safety case requires the assessors to be confident, thus, there is some uncertainty of confidence in the safety case, and it becomes a key factor how to process the uncertainty in evaluating confidence in safety case. D-S evidence theory is fit for processing the subjective judgment and synthesizing the uncertain knowledge. So, this theory is applied to the uncertainty of assessment results. First, the related knowledge is given, including safety case and D-S evidence theory. Then the approach of evaluating confidence in safety case using D-S evidence theory is presented, and engine software is chosen as experimental example for proposed approach. At the same time, the experimental results based on the proposed approach are also presented. The algorithm has a strong versatility and an example is used to demonstrate its effectively in this text.

Keywords: *Safety Case, Uncertainty, Confidence, D-S Evidence Theory.*

1. INTRODUCTION

The concept of the ‘safety case’ has already been adopted across many industries[1-4], such as defense, aerospace, nuclear and railways. A safety case provides an explicit means for justifying the safety of a system through a reasoned argument and supporting evidence[5]. The problem is that it is always possible to find or produce evidence that something is safe, where there is no complete mathematical theory to base arguments and guarantee completeness[6]. So the acceptance of a safety case requires the assessors to be confident that the safety case meets the requirements. However, both the developers and the assessors can sometimes be uncertain that the safety case has high assurance. Because of lack of historical data, determining what amount or what types of evidence are sufficient can be extremely difficult. If we are uncertain about the sufficiency of the evidence, then our confidence in the safety case is reduced. Due to the existence of uncertainty, it becomes a key factor how to process the uncertainty in evaluating confidence in safety case.

Evidence theory is fit for processing the subjective judgment and synthesizing the uncertain knowledge. So, this theory is applied to the uncertainty of assessment results. In this paper, we explore the challenges of evaluating confidence in safety cases; in particular, we propose an approach for confidence evaluation by integrating probabilistic reasoning with D-S evidence theory into safety arguments represented in the Goal Structuring Notation (GSN). An overarching motivation for this work is, eventually, to deal with uncertainty because of expert judgment.

This paper is arranged as follows: the related knowledge of safety case and D-S evidence theory is introduced in Part 2. The proposed approach is further elaborated from three aspects of experimental example, algorithm and analysis about experiment in Part 3. Part 4 discusses the conclusions.

2. RELATED KNOWLEDGE

2.1 Safety Case & GSN

A safety case[5] consists of explicit safety requirements, the evidence that the requirements have been met, and the argument links the evidence to the requirements. Both the argument and the evidence are essential.

This paper uses GSN as the example graphics-based notation for expressing safety case. GSN[5]: a graphical notation for representing arguments in terms of basic elements such as goals, strategy, solution, context, assumption and justification. A GSN argument links these elements by using two main relationships: supported by and in context of, to form a goal structure.

2.2 D-S Evidence Theory

In the D-S evidence theory[7], the basic entity is the identification of the framework Θ. A key point of the D-S theory is the mass function m (basic probability assignment, or BPA) that is defined on 2^{Θ} as m: $2^{\Theta}\rightarrow[0, 1]$. Belief function is used to describe the results of uncertainty. From this BPA m, the credibility Bel(A) and plausibility Pl(A) can be computed from the following equations:

$$Bel(A)=\sum_{B\subseteq A}m(B)\triangleright\triangleright\triangleright Pl(A)=\sum_{B\cap A\neq\varnothing}m(B) \quad (1)$$

Bel(A) is expressed as the evidence to the results of the total support, or the decision-makers have reason to believe that the results of A.

D-S theory provides a method to combine the previous measures of evidence of different sources. If mi is the BPA provided by source (1<=i<=n), the combination: m_1 □m_2 □..□m_n, can also be called as orthogonal sum, and it can be defined according to the Dempster's combination rule, by

$$\begin{aligned}&(m_1\oplus m_2\oplus\cdots\oplus m_n)(A)\\&=\frac{1}{K}\sum_{A_1\cap A_2\cap\cdots\cap A_n=A}m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n)\end{aligned} \quad (2)$$

Where

$$\begin{aligned}K&=\sum_{A_1\cap\cdots\cap A_n\neq\varnothing}m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n)\\&=1-\sum_{A_1\cap\cdots\cap A_n=\varnothing}m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n)\end{aligned} \quad (3)$$

In order to reduce the conflict influence between evidences, we assign different weight to different evidences. Let the set of evidences be E={E_1, E_2,...,E_n}. The weight coefficient of evidence E_i is ωi, ωi ϵ[0,1] and the sum ω_i is 1,which reflects the importance of evidences during the combination.

Firstly, we assign bpa and build up weight vector of evidences. let ωmax={ω_1, ω_2, …, ω_n}, the relatively weight vector is ω'=(ω_1, ω_2, …, ω_n)/ω_{max}. Second the "ratio" of BPA can be obtained: $\alpha_i(0\le\alpha_i\le1),(1-\alpha_i)=\omega_i/\omega_{\max},i=1,2,...n$ .Use the "ratio" to adjust the BPA of evidences in the framework. The BPA function after adjustment is:

$$\begin{aligned}&m_i'(A_k)=(1-\alpha_i)m_i(A_k)\triangleright\triangleright\triangleright m'(\Theta)\\&=(1-\alpha_i)m(\Theta)+\alpha_i\end{aligned} \quad (4)$$

The BPA of evidences after adjustment are m_i'(A_k), m_i'(Θ) substitutes in Eq.2, then we obtain the new combination formula.

3. PROPOSED APPROACH

In our proposed approach for evaluating confidence in safety cases, we first construct the safety argument using GSN. Then we advance the process to evaluate the confidence in safety case by using D-S evidence theory. At the same time, this proposed approach is detailed represented combined with the example of safety case.

3.1 Experimental Example Of Safety Case

A safety case has been constructed for safety-critical engine software as an experimental example for proposed approach. Figure1 shows a fragment of the safety case of engine software.

Engine software is part of engine control system, and the top level claim of software safety is acquired from the system. While the necessary risk reduction of the system can be determined after its total risk, and the tolerable risk is cleared, then, the system safety requirements can be obtained. Based on which, the safety claim for software related system may be preliminary identified. We have determined that G1 'Engine software contributions to system Level Hazards are acceptable' is the top claim, supported by C1. G1 will be changed to software safety requirements. Thus, G1 can be argued over all identified software safety requirements S1, supported by C2 and software development to the integrity level appropriate to the hazards involved S2, supported by C3. Thus, C1 can be divided into two sub-goals G2 and G3. Engine software safety requirements were identified from the view of system, and four software safety requirements are acquired: start control, anti-asthma control, anti-ice control, and signal monitoring. Therefore G2 are divided into four sub-goals: G4, G5, G6 and G7. G3 can be classified into four process factors such as tool, method and environment and others. Thus, G3 are divided into four sub-goals: G8, G9, G10 and G11. Whether software safety requirement is satisfied can be confirmed on analysis and testing. Finally, the corresponding evidences may be selected and provided, that is, they are E_1, E_2, E_3, E_4, E_5 and E_6.

Whether G1 is to be accepted needs to be confirmed by assessors. Because of the lack of historical data, determining what amount or what types of evidence and argument are sufficient can be extremely difficult. There exist some uncertainties and unknowns in evaluating confidence in safety case.

In this paper, we discuss ways to evaluate confidence in the argument and quantify the uncertainty in this claim.

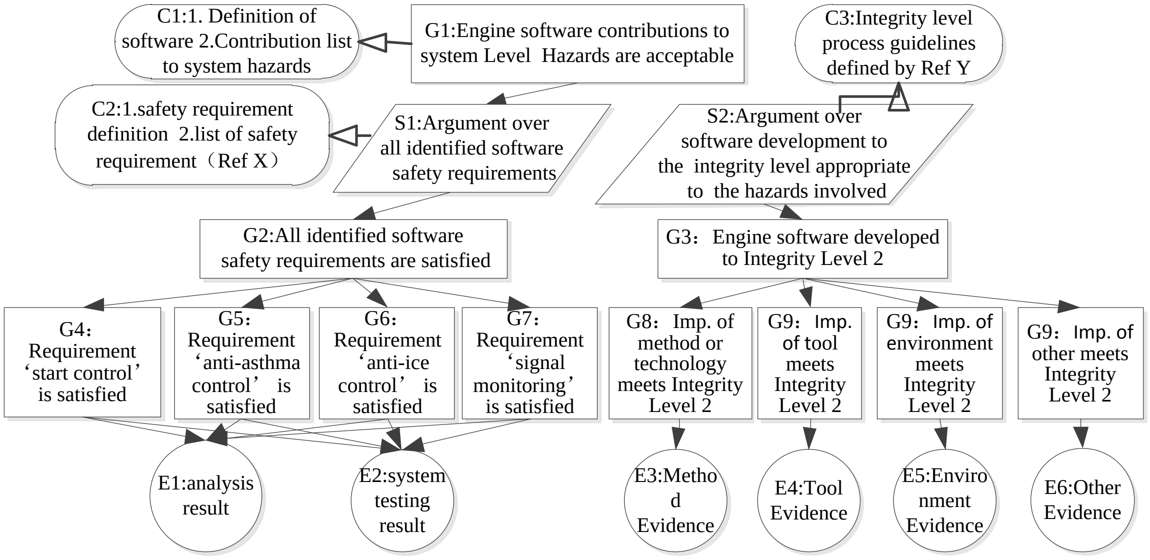
C1:1. Definition of software 2.Contribution list to system hazards
G1:Engine software contributions to system Level Hazards are acceptable
C3:Integrity level process guidelines defined by Ref Y
C2:1.safety requirement definition 2.list of safety requirement（Ref X）
S1:Argument over all identified software safety requirements
S2:Argument over software development to the integrity level appropriate to the hazards involved
G2:All identified software safety requirements are satisfied
G3：Engine software developed to Integrity Level 2
G4：Requirement ‘start control’ is satisfied
G5：Requirement ‘anti-asthma control’ is satisfied
G6：Requirement ‘anti-ice control’ is satisfied
G7：Requirement ‘signal monitoring’ is satisfied
G8：Imp. of method or technology meets Integrity Level 2
G9：Imp. of tool meets Integrity Level 2
G9：Imp. of environment meets Integrity Level 2
G9：Imp. of other meets Integrity Level 2
E1:analysis result
E2:system testing result
E3:Method Evidence
E4:Tool Evidence
E5:Environment Evidence
E6:Other Evidence

Figure1 Fragment Of The Safety Case Of Engine Software

3.2 Algorithm Of Evaluating Confidence In Safety Case Using D-S Evidence Theory

The assessors are not easy given the direct results of the evaluation to the top level claim in safety case. In general, the evaluation results of sub-goals in the lowest layer are firstly obtained based on evidences. Then the evaluation results of sub-goals in the higher layer are given, till the top level claim. By dynamic real-time access to evidence data and the use of DS evidence theory, this paper uses the probability of a large synthetic as the qualitative results of the assessment, which makes its results more objective and credible.

Goals need to be extracted from the safety argument by using GSN. Then, take evaluation ranks and BPA represents goals of the safety case. Then the improved Dempster's rule is used to combine the goals layer by layer, we can obtain the BPA value of the top level claim. The concrete algorithm is as follows:

3.2.1 Extraction goals

There exists the challenge of confidence only in the goals of safety case and the object of evaluation is the goals of safety case. Therefore, the first step is to extraction goals from safety case. In general, the structure of goals of safety case is a hierarchical inverted tree structure, in which, the top tier is software safety top level claim, the middle layer and the bottom layer is multi-layer sub-goals. Figure 2 shows the result of extraction from fragment of the safety case of engine software, as shown in Figure1.

3.2.2 Result set

The result set is space of hypothesis which is the assessor make the results of the various elements of the assessment result. A set of result we defined and denoted R as follows: $R=\{r_1, r_2, ..., r_n\}$

Where ri represent the various possible evaluation results. Goal of confidence evaluation is derived from one of the best results of the evaluation that based on comprehensive consideration of all goals.

In the confidence evaluation in safety case, the results of the assessment can be classified as very low, low, medium, high and very high. So the result set $R=\{verylow, low, medium, high, veryhigh\}$. That is, the value of identification framework

$$\Theta=\{verylow=A_1, low=A_2, medium=A_3, high=A_4, veryhigh=A_5\}$$

3.2.3 BPA and weight

Ascertain all layers' weights between goals in the same layer and BPA $m_i(A_j)$ of sub-goals layer with regard to A_j(j=1,2,…k), that is, A_1 is very low, A_2 is low, A_3 is medium, A_4 is high and A_5 is very high, where Θ represents the uncertainty. The BPA of sub-goals can be obtained by Delphi Method, the weights value between of goals can be obtained by Analytic Hierarchy Process Method (AHP). In addition, in the result set, we only interested in one result which identifying the framework of the element (such as a single hypothesis) rather than its subset (composed of a number of assumptions).

Table 1 shows the weights of goals in safety case of engine software and Table 2 shows its BPA $m_i(A_j)$ of the second layer sub-goals.

Table 1 The Weights of All of Goals in Safety Case of Engine Software

Top Level Claim	First Layer Sub-goals	Weight ω_n	Second Layer Sub-goals	Weight ω_n
G1	G2	0.731	G4	0.250
			G5	0.250
			G6	0.312
			G7	0.188
	G3	0.269	G8	0.336
			G9	0.234
			G10	0.257
			G11	0.173

Table 2 The BPA $m_i(A_j)$ of .the Second Layer Sub-goals in Safety Case of Engine Software

Sub-goals	BPA $m_i(A_j)$					
	A_1	A_2	A_3	A_4	A_5	Θ
G4	0.03	0.1	0.48	0.34	0.05	0
G5	0.1	0.1	0.35	0.37	0.05	0.03
G6	0.02	0.1	0.46	0.36	0.05	0.01
G7	0.01	0.1	0.53	0.29	0.05	0.02
G8	0	0.05	0.31	0.47	0.17	0
G9	0	0.05	0.23	0.54	0.18	0
G10	0	0.05	0.28	0.58	0.08	0.01
G11	0	0.05	0.33	0.55	0.05	0.02

3.2.3.1improved bpa of the second layer sub-goals

Use Eq.4 to calculate BPA, Table 3 shows BPA after ratio. In this table the uncertainty increased, this is induced by inflicts of evidences. This situation is attributed to the using of Eq.4. Conflicts between evidences are ascribed to the uncertainty of the discernment.

Table 4 The BPA $m_i(A_j)$ of .the First Layer Sub-goals

		The Second Layer Sub-goals	
		G2(ω=0.731)	G3(ω=0.269)
BPA $m_i(A_j)$	A_1	0.0041	0
	A_2	0.0262	0.0108
	A_3	0.6290	0.1913
	A_4	0.3303	0.7473
	A_5	0.0093	0.0506
	Θ	0.0011	0

Table 3 The Improved BPA mi(Aj) of .the Second Layer Sub-goals

Sub-goals	BPA mi(Aj)					
	A_1	A_2	A_3	A_4	A_5	Θ
G4	0.02	0.08	0.39	0.27	0.04	0.2
G5	0.08	0.08	0.28	0.3	0.04	0.22
G6	0.02	0.1	0.46	0.36	0.05	0.01
G7	0.01	0.06	0.32	0.18	0.03	0.4
G8	0	0.05	0.31	0.47	0.17	0
G9	0	0.03	0.20	0.40	0.06	0.31
G10	0	0.04	0.21	0.45	0.06	0.24
G11	0	0.03	0.17	0.29	0.03	0.48

3.2.3.2 Calculation bpa of the first layer sub-goals of engine software

When the BPA of the second layer sub-goals is obtained, they are combined by using Eq.2 and Eq.3 in turn. The combination result of G4, G5, G6 and G7 is the BPA of G2, and the combination result of G8, G9, G10 and G11 by Eq.2 and Eq.3 is the BPA of G3, as shown in Table 4.

3.2.3.3 Calculation bpa of the top level claim of engine software

The combination result of G2 and G3 by Eq.2 and Eq.3 is the BPA of G1, as shown in Table 5

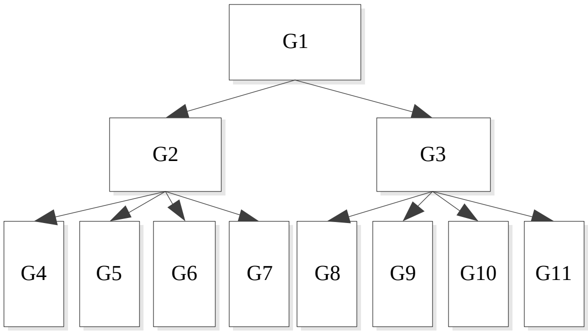

Figure 2 The Goals For Experimental Example

3.2.3.4 Choose one of the largest number of synthetic probability as assessment result.

From the table 5 shows that the probability of confidence for a maximum of 0.5755, so the result A3 of this assessment as confidence in safety case of engine software.

Table 5 The BPA $M_i(A_j)$ Of .The Top Level Claim In Safety Case Of Engine Software

		The Top Level Claim G1
BPA $m_i(A_j)$	A_1	0.0034
	A_2	0.0217
	A_3	0.5755
	A_4	0.3906
	A_5	0.0079
	Θ	0.0009

3.2.3.5 Calculation bel(a) and pl(a)

We can obtain the belief value and plausibility value of confidence from Eq.1. As the subset of X_i is singleton sets, the belief value is $Bel(A_j) = m'(A_j)[j = 1,2,3,4,5,6]$ .the belief value is $Pl(A_j) = m'(A_j) + m'(\Theta)[j = 1,2,3,4,5,6]$.

Therefore, for the proposition p “the confidence of ‘Engine software contributions to system Level Hazards are acceptable’ is above medium”, the certainty value Bel(p)=0.5755, the unknown value m’(Θ)=0.009, and the belief interval [Bel(p), Pl(p)]=[0.5755, 0.5764], the uncertainty value of the proposition p is 0.009.

So far, the task processing is complete.

3.3 Analysis About Experiment

Table 5 shows the BPA and the uncertainty of the evaluation rank of confidence. From the compare of table 4 and table 5 we can see that the various change of BPA value after the combination of Dempster’s rule of combination. The belief values which are high before combination become higher after combination; the belief values which are low before combination become lower after combination; the uncertainty become lower and lower during the combination process, at last it reduced to 0.009. In whole process, we can see G2 ‘All identified software safety requirements are satisfied’ is the more degree contributions to the confidence in safety case, which results are consistent with common sense. Therefore considered that D-S evidence theory in the application of qualitative assessment is valid, and can better solve uncertainty of assessment result that come from the subjective and rigid division of the quantitative data.

4. CONCLUSIONS

Because of the deficiency of the historical data and the preference of experts while evaluating the acceptance of a safety case, there is some uncertainty of confidence in the safety case. So we use D-S evidence theory to deal with the problem of subjective judgments and uncertainties of knowledge synthesis advantages, and the improved Dempster’s rule of combination is adopted to combine the BPA. The characteristics of this proposed approach is that the certainty and uncertainty value can be distinguished of evaluating confidence in safety case. It is proved that D-S evidence theory has advantages in evaluating confidence in safety case which has some uncertainty. The usage of D-S evidence theory reduced the effect of the uncertainty, improved the precision and the validity of the evaluation, and reduced the blindness and the subjectivity of evaluation of confidence in safety case.

Sharp tools make good work. For this reason the next step is to develop the tool, to support the algorithm of evaluating confidence in safety case based on D-S theory.

ACKNOWLEDGMENTS

This work has been partially Project supported by the National Defense Pre-Research Foundation of China (Grant No. 513190801).

REFERENCES

[1] Liu, C. Sha, X.; Yan, F.; Tang, T.,A scenario-based safety argumentation for CBTC safety case architecture, WIT Transactions on the Built Environment, v 114, p 839-850, 2010.

[2] Feather, Martin S, Building a safety case for a safety-critical NASA space vehicle software system, the 4th IEEE International Conference on Space Mission Challenges for Information Technology, p10-17, 2011.

[3] Bardy. Mariana. Silveira, Paula Dias, Use of safety case to accomplish with Brazilian regulations for drilling units, Proceedings of the Annual Offshore Technology Conference, v 2, p 804-812, 2011.

[4] Denney, Ewen; Pai,Ganesh; Habli,Ibrahim, Perspectives on software safety case development for unmanned aircraft, Proceedings of the International Conference on Dependable Systems and Networks, 2012.

[5] T. P. Kelly, Arguing Safety – A Systematic Approach to Safety Case Management, DPhil Thesis, YCST-99-05, Department of Computer Science, University of York, 1998.

[6] American Nuclear Society, "Risk-Informed and Performance-Based Regulations for Nuclear Power Plants," Position Statement 46, June 2004.

[7] Shafer, G. A Mathematical Theory of Evidence. Princeton University Press, 1976.