A Model for Safety Case Confidence Assessment

Jérémie Guiochet, Quynh Anh Do Hoang, Mohamed Kaâniche

A Model for Safety Case Confidence Assessment

Jérémie Guiochet[1,2], Quynh Anh Do Hoang[1,2], and Mohamed Kaaniche[1,2]

[1] LAAS-CNRS, 7 avenue du colonel Roche, 31031 Toulouse, France
[2] Université de Toulouse, France
{guiochet, qdohoang, kaaniche}@laas.fr

Abstract. Building a safety case is a common approach to make expert judgement explicit about safety of a system. The issue of confidence in such argumentation is still an open research field. Providing quantitative estimation of confidence is an interesting approach to manage complexity of arguments. This paper explores the main current approaches, and proposes a new model for quantitative confidence estimation based on Belief Theory for its definition, and on Bayesian Belief Networks for its propagation in safety case networks.

Keywords: Safety Case · Confidence · Uncertainty · Quantitative estimation · Bayesian Belief Network · Belief Theory

1 Introduction

Safety cases are used in several critical industrial sectors to justify safety of installations and operations. As defined in the standard [6]: "a Safety Case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment". An important research work has also been initiated to deliver guidelines to document safety cases. An initial work developed at York University [19], based on an adaptation of Toulmin argumentation model [25], led to the proposal of the Goal Structuring Notation (GSN). Other proposals such as CAE for Claims-Argument-Evidence [3] and KAOS (Knowledge Acquisition and autOmated Specification) [5], but they did not reach the maturity of GSN [14]. The Object Management Group (OMG) has also delivered a metamodel for the argumentation approach [22]. The goal of these approaches is to make more explicit the supporting arguments for a top-level claim.

Given a claim and a supporting argument, an important and growing issue is to understand how much confidence one could have in the claim and how the different arguments contribute to such confidence. For instance, let us consider the classical example of the claim "{System X} is safe", supported by the evidence that all specific hazards have been eliminated as presented in Figure 1. Main concepts of GSN are presented here: goals present claims forming part of the argument; Strategies describe the nature of inferences that exist between a goal and its supporting sub-goal(s); Solutions present a reference to an evidence item (results of a fault tree analysis for instance); Contexts present contextual artifacts (they could be a reference to contextual information, or statements). Other elements are used in GSN but not presented here as our proposal focuses on these main components of GSN. Each element of such an argument may

be subject of uncertainties, such as "do all the hazards have been identified?" or "is the treatment of hazard n effective?". Moreover, considering that argument structures tend to grow excessively, it may become too complex for third parties to analyse the argument. Therefore, appropriate methods to assess confidence in the argument structures and supporting evidence are required. Three main challenges are of particular interest: how confidence could be formally defined, how confidence could be quantitatively estimated, and how confidence in argument leaves could be propagated to assess the impact on the main claim confidence.

In this paper we mainly address the first and third issues by introducing a new method for defining and propagating a quantitative estimation of confidence of a safety case. After presenting related work in Section 2, we introduce our definition of confidence based on belief theory in Section 4. This definition is used in Section 5 where details about confidence propagation are given. Finally, in the conclusion we will discuss about first results and open issues in this area.

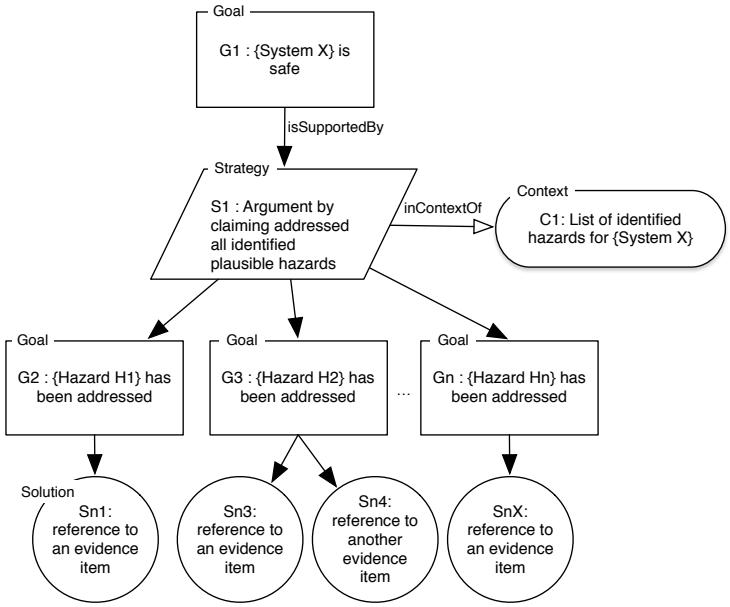


Fig. 1. GSN example adapted from Hazard Avoidance Pattern [20]

2 Related Work

The issue of confidence in argument structures has already been addressed by several works, with slightly different objectives and scopes. Table 1 presents a common framework to analyze some relevant related work considering the following dimensions:

– Argument modelling: construction of the "case" which may be based on GSN or other notations

– Argument uncertainties identification: uncertainties in inferences and arguments elements are identified
– Confidence modelling: construction of a confidence case, with explicit representation of dependencies between the uncertainties
– Confidence estimation: theoretical framework for quantitative estimation of the confidence
– Decision support: provide support based on the quantitative estimation in order to make a decision for the acceptability of the argument, or its improvement.

Table 1. Different approaches for managing confidence in safety case

	Argument modelling	**Argument uncertainties identification**	**Confidence modelling**	**Confidence estimation**	**Decision support**
[21]			Bayesian network	Probability law	
[26]	Argumentation Metamodel (ARM) based case	Based on Toulmin model	Bayesian network (with Hitchcock criteria)	Probability law (with basic logical gates)	
[7]	GSN		Bayesian network	Probability law and tool support with AgenaRisk	
[4]	Trust case based on Toulmin model			Dempster-Shafer Theory	Decision level associated to confidence level
[2]	GSN			Dempster-Shafer Theory	Decision based on the confidence value
[1]	GSN	Common Characteristic Map (CCM)	Confidence case based on GSN		
[13]	GSN	Based on Assurance Claim Points (ACP)	Confidence case in GSN	Baconian probability	
[16]	GSN	Based on Assurance Claim Points (ACP)	Assurance case in GSN		

Qualitative Approaches

In [16], the inventors of GSN address the confidence issue, by proposing to split a traditional safety case in two pieces. The first is the safety argument, showing all evidences, and the second is a confidence argument that addresses confidence in evidences, contexts, and individual inferences. This confidence argument is also represented with GSN. It starts by adding to the safety case some possible uncertainty sources, which are called Assurance Claim Points (ACP), that are attached to inferences (the arrows connecting claims), contexts (explanatory information), or solutions. Then, for each ACP, an argumentation mainly focuses on demonstrating that the ACP is trustworthy and appropriate, which is built using GSN. Another proposal [1], is based on the ACP but only focuses on Context and Solution elements. The authors propose to use a map (Common Characteristic Map) as a check list to identify sources of uncertainties, with recursive dependencies. For instance, if a safety case includes a solution which is a "Process result", they propose the generic uncertainties related to "the use of a language", "the use

of a tool", "the use of a mechanism", "the involved artifacts", etc. All those characteristics are then refined, with possible recursive dependencies.

The proposed approach in [12] is quite similar, adapting the defeater concept from Defeasible Reasoning theory introduced by [24]. These defeaters that could be compared to previous ACP, or weaknesses in the argumentation, are then analyzed to be reduced one by one.

Both previous proposals focus on the identification of the weaknesses in an argumentation, and present methods for a well structured approach. Nevertheless, such approaches may lead to complex confidence cases. Although controversial, we believe that quantitative estimation approaches may help to analyze the safety case confidence. For instance, it can support sensitivity analyses to identify the weak elements of an argumentation.

Quantitative Approaches

This group of approaches tries to apply mathematical formalism to capture lack of confidence in argument elements. Apart from some proposals based on simple mathematical models as in [13] where the number of uncertainties is estimated, two main ways of approaching the problem can be identified:

- Bayesian Belief Networks (BBNs): in this case the uncertainty is interpreted as a probability. BBNs are then applied to deduce the confidence in a goal from credibility of its backing arguments. Some authors directly use BBNs for modeling arguments and confidence. For instance, in [18], they only use BBNs and commercial tools to calculate "trustworthy", which is actually a conditional probability. With a similar approach, authors of [21] particularly focus on the diversification in argumentation, calculating how a "multilegged" argument (a claim is supported by two evidences) impacts the probability (interpreted as a confidence level) of achieving the main claim. However, they directly use BBNs, without any safety case. On the contrary, [26] propose to apply to each claim of a Toulmin model argument, a Bayesien network pattern showing relationships between uncertainties in the argumentation based on Hitchock criteria [17]. However, confidence propagation is not clearly analyzed and justified. In [7], the authors present an interesting approach to build a BBN from the safety case, and use the work of [11], to define a distribution of confidence for each argument element, but they do not propose transformation rules between safety case in GSN and the confidence BBN. The confidence propagation formulas are also not justified.
- Dempster–Shafer (D-S) theory of evidence. These approaches are based on the belief theory developed by P. Dempster in 1967, and extended by G. Shafer in 1976. A common justification for its use, is that probability theory does not make difference between epistemic and aleatory uncertainties [10]. In the D-S approach, belief, disbelief and epistemic uncertainty are explicitly quantified. An important work by [4] is based on this theory. The authors, propose to build "Trust cases" based on Toulmin concepts, and to directly associate levels for belief and uncertainties, linked with a decision to accept or not an argument element. In this case, they do not build a confidence case, but directly propose a method and a tool for decision support.

As presented later, they do not explicitly take into account confidence in the inferences of the argument. Authors of [2], directly reuse the previous work, with a limited version, only considering that for each argument element it exists a level for "sufficiency".

In summary, defining and measuring confidence in assurance claims is an important and open issue. A framework for determining confidence is needed, and this paper presents some initial steps to fulfill this objective.

3 Proposed Approach Overview

Our objective is to propose a method to identify weaknesses in safety case, in order to improve it. Referring to Table 1, our contribution focuses on the following steps presented Figure 2:

- Argument modelling: the safety case is built using GSN
- Confidence modelling: we propose to annotate the GSN models and transform them into a confidence network
- Confidence estimation: confidence in the network leaves are estimated and propagation formulas are used
- Sensitivity analysis: impact of confidence variations is analyzed to identify weaknesses of the safety case.

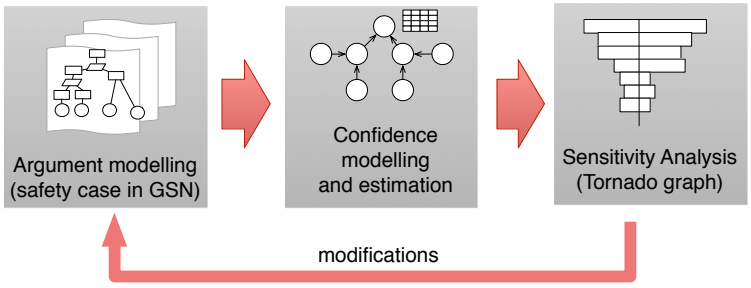


Fig. 2. Overview of the proposed method

4 Measuring Confidence

Confidence may be used as a common concept for different theories, including probability, and D-S. As in [1, 4], we define confidence using the D-S approach. In this theory, a belief function is defined from the powerset $\mathcal{P}(\Omega)$ of possible events into $[0; 1]$. For instance, let ω be the state of an indicator light that can have two values on and off, then $\Omega = \{on, off\}$ and $\mathcal{P}(\Omega) = \{\{on\}, \{off\}, \{on, off\}, \varnothing\}$. In this example the belief function Bel, is defined as the mass m of belief such as $Bel(\{on\})$ represents the credibility of the light to be ON. As an example, a possible estimation would be $Bel(\{on\}) = m(\{on\}) = 0.2$, $Bel(\{off\}) = m(\{off\}) = 0.5$ et

$m(\{on, off\}) = m(\Omega) = 0.3$. When events are Boolean, like in this example, we can sum-up the D-S concepts with the Figure 3 (Plausibility is another D-S concept which will not be included in this paper).

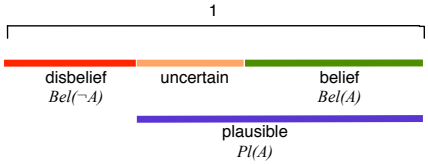


Fig. 3. D-S theory concepts, with a Boolean set

We will consider in a safety case that all elements leaves are observed, and that they cannot be false. Hence, for an element A, $Bel(\overline{A}) = 0$. This led us to define confidence and uncertainty as the belief functions:

$$\begin{cases} m(A) = Bel(A) = g(A) \in [0,1] & : \quad confidence \\ m(A, \overline{A}) = 1 - g(A) \in [0,1] & : \quad uncertainty \\ m(\overline{A}) = 0 \end{cases} \tag{1}$$

In the context of safety case, we consider two types of uncertainty sources, which are similar to those presented in [16] named "appropriateness" and "trustworthiness". For instance, in the very simple safety case presented in Figure 4, two sources of uncertainties may be identified:

- uncertainty in the fact that B is appropriate for the inference "A is Supported by B"
- uncertainty in the solution B itself : are the tests trustworthy?

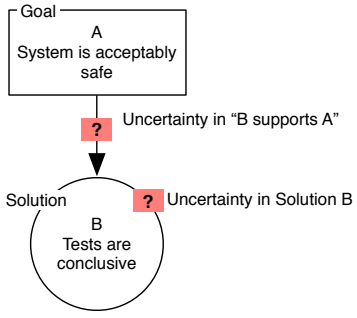


Fig. 4. Uncertainty points in a simple inference

5 Propagating Confidence

5.1 Argument Types

The very basic inference is the simplest one, "A is Supported by B". Nevertheless, most of arguments are more complex than direct one-to-one inference. For instance, let us consider the example presented with the main claim "A: System is fit for use", supported by both "B: Tests are conclusive" and "C: Formal verification has been performed". In that case, we can expect that both evidences independently increase the level of confidence in A. This concept is presented as "alternative argument" in [4]: even if there is no confidence in B, the fact that C also independently supports A will preserve some level of confidence.

An another form of inference, is presented in the GSN «Hazard Avoidance Pattern» proposed in [20], presented Figure 1. In that case, the main Goal "System is Safe", depends on all the sub goals together (we do not consider "Strategy" as a node, because it is only a descriptive element). Each of the premises covers a part of the goal. [4] propose to name such an argument a "complementary argument".

Figure 5 present those two types of arguments, with the inference "A supported by B and C". We also illustrate the fact that in both types of argument, the sub nodes may have a different weight in the overall confidence in the claim A. Other types of arguments may be included, as introduced in [2, 4], but they are not included in this paper.

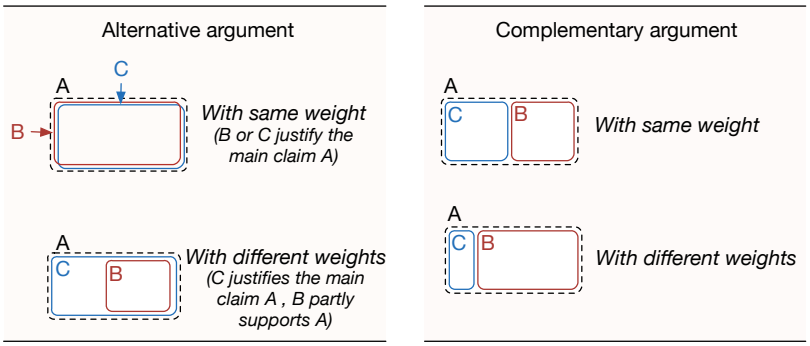
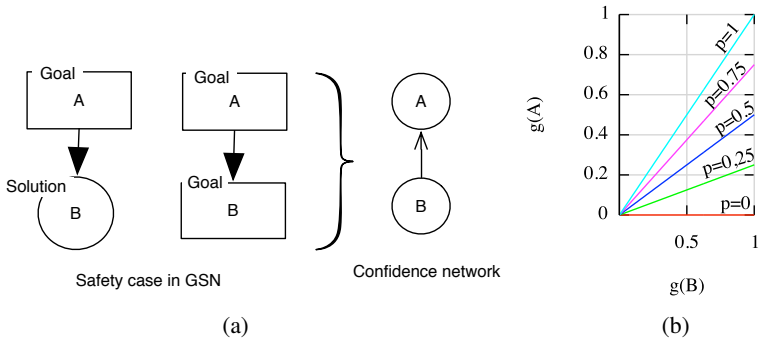


Fig. 5. Alternative and complementary arguments

5.2 Simple Argument

The basic inference, "A is supported by B" can apply to the cases (a) a goal is refined into a subgoal and (b) a goal is supported by an evidence, as presented in Figure 6. In this case, the confidence network is represented like a BBN, using two nodes and one edge. We propose to use the following table to describe the confidence propagation:

g(B)	0	1
g(A)	0	p



(a) (b)

Fig. 6. (a) GSN Simple argument transformation into confidence network and (b) $g(A)$ in function of $g(B)$, for $p \in [0; 1]$

In this table, the confidence in A is estimated when there is no confidence in B (i.e. when $g(B) = 0$), then $g(A) = 0$, and when there is a maximum confidence in $g(B)$. In this case, the confidence in A depends on a factor p, which represents the confidence in the inference "A is supported by B". The final confidence is obtained using this table as a probability table: $g(A) = p * g(B)$. The result is a linear dependency $g(A)$, illustrated in Figure 6 considering different values for p and g(B).

5.3 Alternative Arguments

As presented Figure 5, several arguments may support a claim with an independent influence. It is important to note that in this Figure, we do not represent the confidence, but the way each argument supports the main claim. In this case, the confidence in A, may be increased by the confidence in both B and C. Such approach could be applied to Solutions or sub-goals as presented Figure 7. The Strategy node is not part of the confidence network, as it only gives explanations on the choices made for argumentation.

We chose for this argument type to use a *leaky noisy-or* as defined in probability theory [8]. It was originally introduced in [23], and it is based on a logical OR between parent nodes (Y_i) and a child node(X), but it includes the fact that the relationship between parents and the child node are not necessary deterministic. The $leaky$ effect corresponds to the fact that even when both parents (B and C) have 0-value probability, there is still a "leaky" probability for the child node. For probabilities, the mathematical function is, with Y_v the set of Y_i in state $\{True\}$:

$$P(X = \{True\}|Y_i) = 1 - (1 - l) * \prod_{Y_i \in Y_v} (1 - p_i) \tag{2}$$

with $p_i = P(X|Y_i, \{\overline{Y_i}\}_{j \neq i})$. In its application to confidence, we do not consider the leaky effect, it is indeed obvious that if there is no confidence in B and C ($g(B) = g(C) = 0$), then the confidence in A is zero, i.e. $g(A) = 0$. Consequently, we obtain the following equation:

$$g(X|Y_i) = 1 - \prod_{Y_i \in Y_v} (1 - p_i) \tag{3}$$

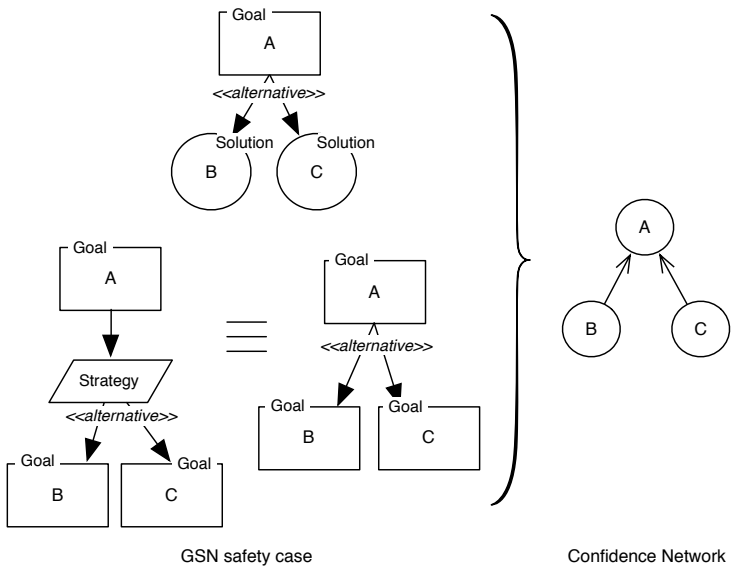


Fig. 7. Alternative argumentation transformation into confidence network

According to 3, the resulting table for two parents is:

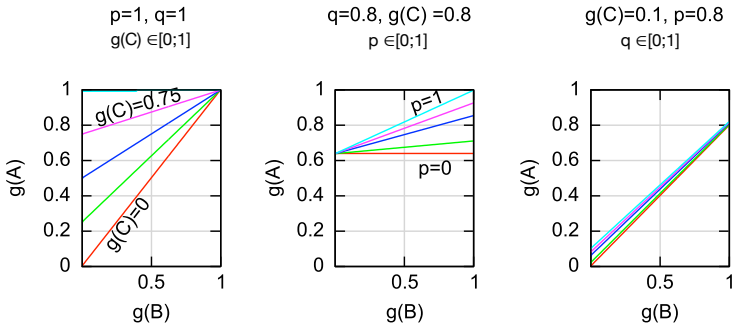
g(B)	0		1	
g(C)	0	1	0	1
g(A)	0	q	p	1-(1-p)(1-q)

This leads to the confidence formula $g(A) = p*g(B)+q*g(C)-g(B)*g(C)*p*q$. p and q respectively represent the confidence in A in case one only has confidence in B or C. Figure 8 illustrates the evolution of confidence g(A) for different situations:

- Figure (a) where $p = q = 1$ illustrates that increasing the confidence in $g(B)$ alone or $g(C)$ alone, automatically increases $g(A)$. For instance, for $g(C) = 0.75$ and $g(B) = 0.5$, the resulting confidence is 0.875. Confidence of 1 for A, occurs only if $g(B)$ or $g(C)$ reaches 1.
- Figure (b) shows influence of p on $g(A)$. For a low confidence p in the inference "A is supported by B", the confidence in A only depends on confidence in C ($g(A)$ is constant for $p = 0$).
- Figure (c) shows that for a low value of $g(C)$ (0.1), the variation of q, which is the confidence in the inference "A supported by C", has no effect on $g(A)$.

5.4 Complementary Arguments

Complementary arguments are used when a set of solutions or subgoals are required simultaneously for supporting the main goal. However, a weight for each element is assigned to rate its relative importance. For instance, in the "Hazard Avoidance Pattern", some hazards may have a less impact on the overall safety, and the lack of confidence in



(a) (b) (c)

Fig. 8. Alternative argument: g(A), in function of g(B), g(C), p and q

their treatment, may induce less reduction in the main confidence, than for other more severe hazards. Several models are used in the literature for such arguments, such as simple And-gate [26], weighted mean [7], or Noisy-And [18]. In our case, after several simulations, we decided to define our own Noisy-And, to obtain the trends that are relevant for complementary argumentation. In this case, we based our calculation on the uncertainty as defined in equation 1 and using the leaky noisy-or defined in equation 2, but taking for the leak $v = 1 - l$. We then obtain the following confidence table:

$m(B,\overline{B})$	0		1	
$m(C,\overline{C})$	0	1	0	1
$m(A,\overline{A})$	$1-v$	$1-v.(1-q)$	$1-v.(1-p)$	$1-v.(1-p).(1-q)$

To calculate the confidence table, we apply the relation $g(X) = 1 - m(X,\overline{X})$, and we also decided to fix $g(A) = 0$ when $g(B) = g(A) = 0$ (which should be obtain for whatever weight of B and C). We thus obtain the following table:

$g(B)$	1		0	
$g(C)$	1	0	1	0
$g(A)$	v	$v.(1-q)$	$v.(1-p)$	0

One main difference with other research works, lies in the interpretation of the parameters. In our case, p and q represent the weight of B and C to decrease confidence (increase uncertainty). In the context of confidence calculation, we also propose to introduce a relation between leak value v, p,and q such as: $v = (p+q)/2$. Indeed, when p and q are lower than 1, it means that the confidence in the inference is less than one. The generalization of this constraint to a complementary argument with n parents is:

$$v = \frac{1}{n}\sum_{i=1}^{n} p_i \tag{4}$$

The values in the confidence table are:

$$g(X|\overline{Y_1},...,\overline{Y_k}) = v.\prod_{i=1}^{k}(1-pi)$$

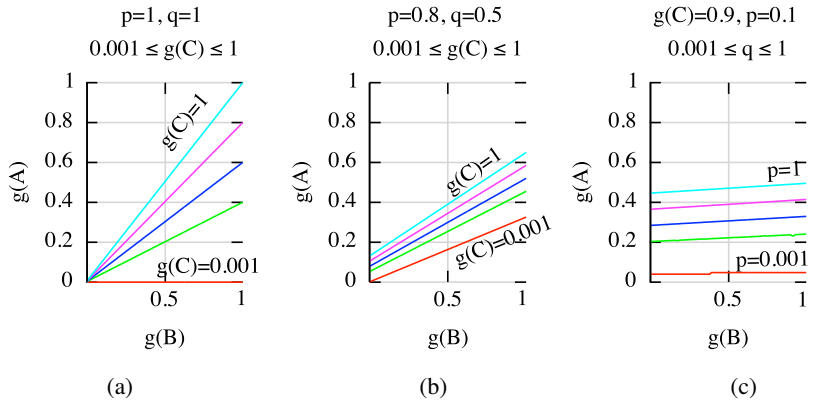


Fig. 9. Complementary argument: g(A) in function of g(B), p and q

where p_i represent the weight of Y_i in the argument. We consider in the following discussion that having a value of 0, for any confidence is not considered, has such an element (no confidence at all), will be removed from a safety argument. Figure 9 presents the result for 2 parents, B, and C, and one child, A. In (a) and (b) we illustrate that when q decreases (q=1, q=0.5) then the influence of $g(C)$ decreases. On the figure, the lines for different values of $g(C)$ are close depending only on $g(B)$ (with a value of 0.5, not presented here due to limitation space). We also illustrate in (b), that when p and q are less than 1, we obtain a residual confidence when $g(B) = 0$ and $g(C) > 0$. This is actually an expected result, because, when the weights are less than one, this means that the argument is not a perfect AND gate. In (c), p is low (0.1), which is interpreted as a low influence of $g(B)$, and characterized by the fact that all lines are nearly horizontals (i.e. with no influence of $g(B)$). A complete analysis of limits, which is not presented here, has demonstrated that the variations of $g(A)$ are compliant with a complementary argument [9].

5.5 Mixed Arguments

The previous arguments could be used also to integrate the confidence in the GSN "Context" element. Indeed, a context is actually a complementary element for the considered argument. Figure 10 presents a complementary argument, where a context has also been defined. In this case, the resulting network, is a node A, with three parents (B, C, D), and a noisy-and table for node A. When an alternative argument is used between B and C, then, an intermediate node I_BC is included, with an alternative table for B and C. The confidence table in A is a noisy-and between D and I_BC.

5.6 Sensitivity Analysis

We propose to perform a sensitivity analysis using a tornado graph. It is a simple statistical tool, which shows the positive or negative influence of basic elements on main function. Basically, considering a function $f(x_1, ...x_n)$, where values $X_1, ..., X_n$ of the 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

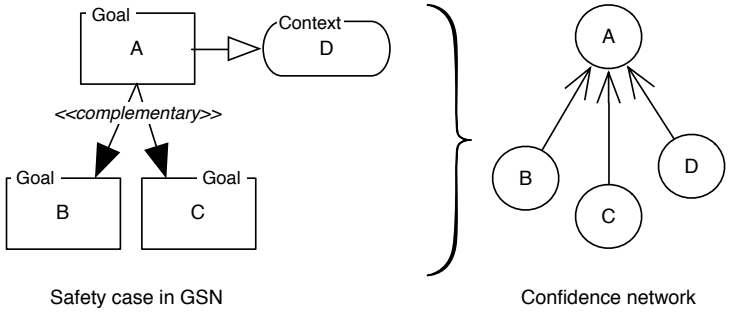


Fig. 10. Mixed argumentation 1

$f(X_1, ..., X_{i-1}, X_{max}, X_{i+1}, ...X_n)$, where X_{min} and X_{max} the maximum and minimum admissible values of variables x_i. Hence for each x_i, we get an interval of possible variations of function f. The tornado graph is a visual presentation with ordered intervals. In our case, we estimate the intervals of $g()$ with $X_{min} = 0$ and $X_{max} = 1$.

If we take the example of alternative argument, with arbitrary values $q = 0.7$ and $p = 0.9$, we get the following table:

g(B)	0		1	
g(C)	0	1	0	1
g(A)	0	0.7	0.9	0.97

If we choose the values of $g(B) = 0.8$ and $g(C) = 0.7$, the confidence table leads to the value $g(A) = 0.8572$, also computed with the tool AgenaRisk[3], presented Figure 11. In this example, to determine the sensitivity to $g(B)$, we keep all the values

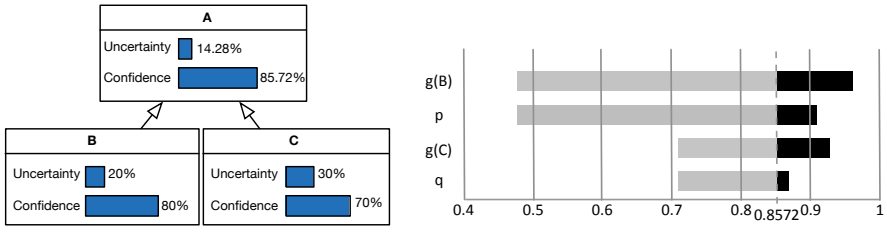


Fig. 11. (a) Example of an alternative argument with the tool Agenarisk and (b) Corresponding Tornado graph

for p, q, and $g(C)$, and only calculate the values $g(A)$ for $g(B) = 0$ and $g(B) = 1$ (we obtain the values 0.49 and 0.949).

The same approach is used for other variables p, q, and $g(C)$. The result is presented Figure 11 (b). In this tornado graph, g(B) appears to be the most influent parameter to decrease or increase the confidence in A. The left part is between 0.49 and 0.872, which

[3] http://www.agenarisk.com

means that if g(B) is equal to its lower limit, then the confidence in A could be reduced to 0.49. On the opposite, with a maximum value of g(B), then confidence in A could reach 0.949.

Such an analysis leads to identify some sensitive points in a confidence network. This could be used to increase the confidence focusing first on the most positive sensitive points, or to focus on the elements where confidence should never be decreased (to consolidate the safety case confidence). Nevertheless, two main limits appear: it is not possible to identify combination of confidence variations, and such a diagram does not identify which variables are the easiest to increase. For instance, even if $g(C)$ appears to be less influent, it may be easier to increase its confidence than the one in $g(B)$. Our approach does not focus on those aspects, but they are important points to study.

6 Conclusion

This paper proposed a new approach for the definition and estimation of confidence in a safety case. We argue that it is important to have a separation between the safety case and the confidence case. Our aim is to analyze uncertainties that may be present in a safety case, using a sensitivity analysis. Our approach is based on the Dempster-Shafer theory for the definitions of confidence and uncertainty. But the constraint $m(X, \overline{X}) = 0$, brings the main benefit of letting use mathematical tools, such as BBN. Hence, we proposed for most common safety case models in GSN, some transformation rules into a confidence network. We particularly introduce the use of noisy-or for alternative arguments, and an adapted version of noisy-and for complementary arguments. An experiment on a real case study of a rehabilitation robot [15] has been carried out [9]. A confidence graph of 65 nodes has been identified with only two alternative arguments (all the others were complementary). The complete analysis is still under development but, we were able to compute the complete graph and get a tornado graph in few minutes with the AgenaRisk tool with consistent results. In this paper, we only focus on the feasibility of a quantitative estimation of confidence, and its propagation in a confidence network. But this is obviously completely dependent on the determination of the confidence values themselves. As already mentioned, this important issue is not addressed in this paper, but is part of our future work.

References

1. Anaheed, A., BaekGyu, K., Insup, L., Oleg, S.: A systematic approach to justifying sufficient confidence in software safety arguments. In: Frank, O., Peter, D. (eds.) Computer Safety, Reliability, and Security Lecture Notes in Computer Science. vol. 7612, pp. 305–316. Springer Berlin Heidelberg (2012)
2. Anaheed, A., Jian, C., Oleg, S., Insup, L.: Assessing the overall sufficiency of safety arguments. In: 21st Safety-critical Systems Symposium (SSS'13), Bristol, United Kingdom (2013)
3. Bishop, P., Bloomfield, R., Guerra, S.: The future of goal-based assurance cases. In: DSN Workshop on Assurance Cases : Best Practices, Possibles Obstacles, and Future Opportunities. Florence, Italy (July 2004)
4. Cyra, L., Górski, J.: Support for argument structures review and assessment. Reliability Engineering and System Safety 96(1), 26–37 (2011)

5. Dardenne, A., Fickas, S., van Lamsweerde, A.: Goal-directed requirements acquisition. In: Science of Computer Programming. vol. 20, pp. 3–50 (1993)
6. DefStan 00-56: Defence standard 00-56 issue 3: Safety management requirements for defence systems. UK Ministry of Defence (2004)
7. Denney, E., Habli, I., Pai, G.: Towards measurements of confidence in safety cases. In: Proceedings of the 5th International Symposium on Empirical Software Engineering and Measurement (ESEM'11). Banff, Canada (September 2011)
8. Díez, F.J., Druzdzel, M.J.: Canonical probabilistic models for knowledge engineering. Tech. rep., Research Center on Intelligent Decision-Support Systems. UNED. Madrid, Spain (2007)
9. Do Hoang, Q.: Analyse et justification de la sécurité de systèmes robotiques en interaction physique avec l'humain (in French). Ph.D. thesis, INP Toulouse, LAAS-CNRS (2015)
10. Felipe, A., Mohamed, S., Walter, S., Siqi, Q.: On the distinction between aleatory and epistemic uncertainty and its implications on reliability and risk analysis. In: European Safety and Reliability Conference, ESREL 2013 (2013)
11. Fenton, N., Neil, M.: Risk Assessment and Decision Analysis with Bayesian Networks. CRC Press, Taylor and francis Group (2012)
12. Goodenough, J., Weinstock, C., Klein, A.: Eliminative induction: A basis for arguing system confidence. In: 35th International Conference on Software Engineering (ICSE2013). pp. 1161–1164 (May 2013)
13. Goodenough, J.B., Weinstock, C.B., Klein, A.Z.: Toward a theory of assurance case confidence. Tech. rep., Software Engineering Institute, Carnagie Mellon University (2012)
14. GSN-Standard: GSN COMMUNITY STANDARD VERSION 1. http://www.goalstructuringnotation.info [Online; accessed Decembre 18th 2014] (2011)
15. Guiochet, J., Do Hoang, Q.A., Kaaniche, M., Powell, D.: Model-based safety analysis of human-robot interactions: The MIRAS walking assistance robot. In: Rehabilitation Robotics (ICORR), 2013 IEEE International Conference on. pp. 1–7 (2013)
16. Hawkins, R., Kelly, T., Knight, J., Graydon, P.: A new approach to creating clear safety arguments. In: Proceedings of 19th Safety Critical Systems Symposium. Southampton, UK (February 2011)
17. Hitchcock, D.: Good reasoning on the toulmin model. Argumentation 19(3), 373–391 (2005)
18. Hobbs, C., Lloyd, M.: The application of bayesian belief networks to assurance case preparation. In: Proceedings of the 20th Safety-Critical Systems Symposium, Bristol, UK. pp. 159–176. Springer London (2012)
19. Kelly, T.P.: Arguing Safety – A Systematic Approach to Managing Safety Cases. Ph.D. thesis, University of York (1998)
20. Kelly, T., McDermid, J.: Safety case construction and reuse using patterns. In: 16th International Conference on Computer Safety and Reliability (SAFECOMP97) (1997)
21. Littlewood, B., Wright, D.: The use of multilegged arguments to increase confidence in safety claims for software-based systems: A study based on a BBN analysis of an idealized example. IEEE Trans. Software Eng. 33(5), 347–365 (2007)
22. OMG-ARM: Structured assurance case metamodel (SACM), version 1. Object Management Group (2013)
23. Pearl, J.: Probabilistic reasoning in intelligent systems: networks of plausible inference. Morgan Kaufmann Publishers Inc. San Francisco, USA (1988)
24. Pollock, J.: Defeasible reasoning. Reasoning: Studies of Human Inference and Its Foundations pp. 451–469 (2008)
25. Toulmin, S.: The uses of argument. Cambridge University Press (1958)
26. Zhao, X., Zhang, D., Lu, M., Zeng, F.: A new approach to assessment of confidence in assurance cases. In: SAFECOMP Workshops. pp. 79–91 (2012)