Patterns for Certification Standards

Kevin Delmas, Claire Pagetti, Thomas Polacsek

Patterns for Certification Standards

Kevin Delmas, Claire Pagetti(✉), and Thomas Polacsek

ONERA, Palaiseau, France
claire.pagetti@onera.fr

Abstract. One of the absolute preconditions for a safety-critical system to enter the market is to be issued a *certificate* by the regulating authorities. To this end, the "applicant" must demonstrate the compliance of its product with the domain's standards. The high complexity of this process has led applicants to rely on *assurance cases* made for certification in the medical, nuclear, or aeronautic domains. In this paper, we propose a generic method that guides the applicant through the specification of assurance cases for a complex standard. Unlike existing works focused on a single context, our objective is to provide an approach that is both generic and domain-agnostic. In order to illustrate this new approach, we present the results of its application on a real-world case study, which pointed out new issues and led to improvements.

1 Introduction

Context. Safety-critical systems, i.e. systems with the potential to endanger a person's life, are often subject to a *certification process*. In practice, any *applicant* requesting the certification of a system is in charge of convincing a *certification authority* that their product is compliant with the regulatory requirements. When the authorities are positively convinced, they deliver a certificate that authorizes its operation. Examples of such authorities include: the European Medicines Agency (EMA) and the Food and Drug Administration (FDA), for drug evaluation; or the European Aviation Safety Agency (EASA) and the Federal Aviation Administration (FAA), for civil aviation safety.

To support applicants in this task, expert committees, composed of companies, certification authorities and academics, have defined standards, guidelines or recommendations (that will be simply referred as standards in the sequel)[1]. These standards are complex documents, which provide high-level certification objectives to be fulfilled and often require experts to understand precisely what is expected by the certification. Moreover, there are two main types of standards: those which only define objectives without imposing any method in order to give some leeway to applicants in their development and validation; and conversely those which impose some high-level process not easy to implement.

Assurance Cases for Certification. Practically, an applicant must provide all the elements concerning the design of the system and the Verification and

[1] Examples of standards are DO178, ARP4754 for aeronautics, ISO 26262 for automotive and EC 62366, EC 62304 for medical devices.

S. Dustdar et al. (Eds.): CAiSE 2020, LNCS 12127, pp. 417–432, 2020.
https://doi.org/10.1007/978-3-030-49435-3_26

Validation (V&V) operations that have been carried out. In addition, they must also *argue* why these are sufficient to address all of the certification authority's concerns. In this context, for applicants (and system designers), the problem is to argue well and, for the certification authority, the problem is to evaluate an argument. As [4] points out for reliable systems, the system must provide a service that can legitimately be trusted, with trust being established through plausible links between the evidence provided and the fact that the system provides the expected service.

In order to cope with the complex activities associated with certification, industries are increasingly relying on *assurance cases*. An assurance case can be defined as "*an organized argument that a system is acceptable for its intended use with respect to specified concerns*" [33]. In practice, to build an assurance case, the applicant is free to organize their argumentation and to use any kind of format. However, especially in the safety world, practitioners rely on dedicated formalisms such as the *Goal Structuring Notation* (GSN) [18,26]. In addition, several works [7,27,39] suggest a pattern approach to design assurance case. In engineering, the design pattern approach is a way of describing a recurring problem and its associated solution based on best practices [2,10]. In a certification context, these assurance case patterns consist of a generic assurance case that lists, for a given claim, the associated evidences and the justification of why the claim could be concluded. Those patterns are then instantiated for a particular product and usage domain.

Towards a Generic Method to Build Assurance Cases. Even though the literature provides assurance case notations and consensus on the necessity of patterns approach, there is almost no work, apart from [13,42], on how to make a pattern. In fact, designing assurance case patterns and instances is really challenging and requires numerous skills. So the aim of this paper is to propose a method for designing certification assurance case patterns.

Through various projects, we have already had the opportunity to design patterns in the medical field, embedded aeronautical systems and assembly line [5,7,32]. In all these projects, the design process was not clearly defined so the construction of the patterns was quite tedious and time-consuming. This is the reason why we tried to define a method that is as generic as possible. This method was designed using a trial and error approach. Of course, we did not design our process from scratch, but we gradually enriched the process and defined the practices (roles and wording) step by step.

After presenting the general context and notations in Sect. 2, we define, in Sect. 3, a method to design patterns for certification standards. In Sect. 4, we detail the lessons learned when applying the method on a specific standard. Section 5 is dedicated to related work and we conclude in Sect. 6.

2 Background and Motivation

2.1 Certification

An applicant must provide a *compliance demonstration* that its product is compliant with the standards where a compliance demonstration is a set of assurance

cases, each applying to a high-level objective. High-level objectives are usually defined as a sort of a reachable goal (sometimes process-oriented activities) and there is no indication on how to achieve the goal. Since nothing is imposed on the manner to develop or validate a product, applicants can rely on numerous solutions to fulfill an objective. For example, for the certification of a kettle, an objective may indicate that it is necessary to identify all scenarios where a user may be injured and show how those situations are mitigated. The ways to proceed (both for hazard identification and mitigation means validation) are not fixed by the standard. For instance, if, to reduce the risk of burns, the designer has put on a handle that remains always cold, it is up to them to demonstrate that this indeed mitigates the risk.

Any standard comes with an intrinsic complexity: high-level objectives are not always easy to understand and are very generic, rationales are not always provided, etc. Moreover, a compliance demonstration encompasses all the concerns of the certification authority, such as safety, security [3] or dependability [41]. This means that certification activities involve several people that need to have transverse and large spectrum knowledge of the product, the process and/or the V&V activities. Such a complexity can be a real obstacle, especially for small companies, to enter in safety critical markets. Thus, offering more tractable approaches is mandatory and our work is a way.

2.2 Assurance Cases

In order to help applicant organize their documentation, several works propose to structure argumentation demonstration with assurance cases and some adequate notations. We can cite for instance, on the academic side, GSN [18,26], *Claim-Argument-Evidence* [8], *Justification Diagram* [32] and, on the standardization organism side, *Structured Assurance Case Meta-model* [30].

All of these notations organize in diagrammatic form the various elements, formal and informal, that contribute to the justification of a result. These frameworks are all based on the model of the British philosopher Stephen Toulmin [36]. His purpose was to define a structure to help assess the validity of a judgement issued on the basis of justifications. In Toulmin's model, any argumentation is composed of a conclusion, namely the *claim*, and facts on which the claim is based. Basically, Toulmin has a legalistic view: to argue well amounts to stating a claim based on facts. In addition to these facts, Toulmin adds information about the reasoning process. This information clarifies why the inference is acceptable, why a set of justifications lead to a conclusion. Typically, in the legal field, this information corresponds to a reference to an article of law. Toulmin writes that this distinction "*is similar to the distinction drawn in the law courts between questions of fact and questions of law*". Toulmin called this additional information a *warrant*. Warrants are therefore what allow the passage from facts to claim, they justify the inference. Distinguishing between facts and warrants is not always easy. Warrants relate to the strength of the argumentation, they are general, whereas reasons depend more on data related to the context. To these

three concepts, Toulmin adds other notions for the qualification of the conclusion and the backing of the warrants.

All assurance case notations focus on the three concepts: claim, warrant and fact, although terminology is sometimes changed, for example *strategy* is used in place of warrant in GSN [18]. We have chosen an agnostic notation approach based on a textual syntax (kind of abstract syntax) compliant with all existing notations (kind of concrete syntax). We rename fact as *evidence* because our argumentation does not really refer to established facts but to documents, for instance calculation results, test reports or expert judgements. The notation is hierarchical since an evidence of one pattern may also be the claim of another one. A final evidence refers to a terminal element that does not become a claim for another pattern. Such a final evidence could be a document or an analysis.

```
Claim: All hazards identified
Warrant: Analysis acceptable by the
authority
Evidence:
  (E1)Means for correctness
  (E2)Means for completeness
```

Fig. 1. Pattern example for the kettle

```
Claim: All hazards identified
Warrant: Functional Hazard Analysis
Evidence:
  (E1)Correctness: external safety
experts reviews
  (E2)Completeness: former accidents
database
```

Fig. 2. Instance example for the kettle

Figure 2 is a possible assurance case, for the kettle example, that answers part of the objective on identifying the hazards. To establish the claim, the justification relies on a Functional Hazard Analysis, a classical safety technique to extract hazards. Such an analysis, to be trustworthy, requires reaching a certain correctness level, based here on a double review by a second experts' team (E1), and also on a certain level of completeness, based here on checking the list with known accidents (E2).

For Toulmin, the notion of warrant is the cornerstone of reasoning. Indeed, it gives the rational and explains why a conclusion can be assessed. Even if some practitioners tend not to use the notion of warrant, it is difficult to evaluate an argument where the warrant is not explicit, in particular for an auditor. For us, even a simple aggregation with an "*and*", like a decomposition strategy for warrant, needs to be explicit. Indeed, a simple conjunction, such as "*and*" between evidence, can hide more complex mechanisms (e.g. check that the evidences are not contradictory or check whether they are sufficient).

2.3 Patterns Notation

[21] promoted the use of a collection of assurance case patterns, with the aim of rationalizing and reusing elements from previous assurance cases. The authors of [19] provide a format, including meta-data, that allows to capture and reuse patterns. In the case of medical devices, the authors [40] explain all the advantages

of using patterns in standards; and their arguments are valid in any application domain.

Figure 1 shows an assurance case pattern (also referred as justification pattern) for the identification of all kettle hazards. A possible instantiation of the pattern is given Fig. 2. The pattern is generic and could be reused for other products that need a risk analysis.

2.4 Justification Pattern Elicitation Problems

Building an assurance case, pattern or instance, is not an easy task. Each pattern can be seen as a guide that lists the necessary elements to meet an objective. The design of a pattern must involve experts who will define the patterns according to their technical domain knowledge and of the established good practices, standards, quality requirements, etc. The main pitfall is the introduction of mistakes during the design of the patterns, which are meant to guarantee the validity of the reasoning.

The problem when it comes to making justification patterns is to think in terms of inference, that is, determine whether or not it is acceptable to pass from a set of justifications to a given claim and to elicitate why this inference is correct. Experts tend to cling to their technical knowledge and how different activities are organized; whereas claims often target quality and safety reached levels. *Critical Thinking* [16] and the usage of *guide words* (as done in some methodologies like HAZOP[2] [20]) may support the experts in their task.

There are many cognitive biases that influence human reasoning. Among them, there is a tendency to consider one's own subjective interpretation as the truth about reality. Research in psychology has shown that one of the implications of this cognitive bias is our inability to judge our understanding and ignorance of what we know. In other words, we think we understand and have valid explanations for phenomena that we do not really understand. On sensitive subjects, the situation is such that we can greatly overestimate the quality of our justifications and reasoning [9]. However, it is possible to compensate for this bias through dialogue. As many studies have confirmed, group reasoning in a collaborative way is more effective than individual reasoning, especially for reasoning and logic problems[3] [23,37].

Regarding legitimacy, the experts must be considered as experts in their field by the people who will use the patterns. This legitimacy can only be acquired through credentials and recognition of competence by peers. In practice, the legitimacy comes from expert's resume, from the projects he has already collaborated on. Thus, an expert is most often someone who has already participated in system certification and/or made recognized contributions (usually in industrial

[2] HAZOP for *HAZard and OPerability analysis* is an industrial risk analysis method.

[3] Moshman and Geil showed on a reasoning problem, with a cohort of 20 groups and 32 individuals, that 75% of the groups found the right answer for only 9.4% of individuals [29]. It should also be noted that groups build more sophisticated, qualitatively, arguments than an individual.

conferences). The question of legitimacy arises with regard to the certification authority. It is the authority who will ultimately decide whether a person is an expert or not.

Finally, from our experience, patterns are very well received and accepted in a group (e.g. company) if they were collaboratively designed by experts working on the side of the applicant and experts belonging to the certification authority.

3 A Method to Design Certification Pattern

Our objective is to define a method to help applicant build a repository of justification patterns dedicated to their specific standard(s). To each objective is associated a pattern. Since correctness and completeness of a pattern can be altered by process flaws and psychological biases, the method concentrates on detecting and correcting these flaws as much as possible.

3.1 Process

Our method is based on a long process to construct justification patterns via several expert meetings. The process, given in Fig. 3, is composed of four iterative steps described below. Note that for a given claim, several patterns may exist since a same claim may be justified in several ways.

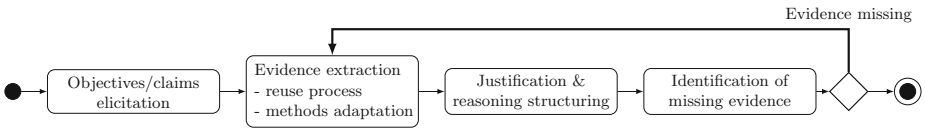

Fig. 3. A first pattern design process

Objectives/Claim Elicitation. Identify the certification objectives the product or process must comply to. Each objective is considered to be a top-level claim. As the process is iterative, some justifications (evidences) defined during an iteration may become a claim.

Evidence Extraction. There are mainly two cases for eliciting evidence: either the applicant has some experience on the claim and can rely on existing practices that have already been applied and convinced the authority. In which case, they can transform the process as a pattern and this corresponds typically to the classic design pattern approach where the pattern captures good practices and well-known solutions. Or the standard applies to a new technology or a new method, in which case experts have to find a fully new solution which can rely on methods coming from any other relevant domain. The result of this activity is an unorganized set of evidences (new claims or final evidences).

Justification and Reasoning Structuring. The activity consists in taking all identified evidences and articulating the inference, or different inferences, that lead(s) to the claim. This step defines the structure of the pattern and the associated warrants.

Identification of Lack of Evidence or End of the Process. When structuring the pattern, the experts may observe that some elements are missing in their reasoning, meaning that evidences are missing. The most common problem is to *forget some final evidences or intermediate claims* to sustain the objective. Thus, between two meetings, the experts must individually think on the patterns they have designed together, looking for mistakes, problems and missing elements possibly introduced during justification structuring. Alternating group and individual works is very important[4]. Indeed, collaborative reasoning facilitates individual cognitive progress, but it is also important for experts to take stock: team influences more individuals than individual influences team [22]. Any doubt should be discussed and traced at the next meeting, not to ask the same question several times. A lack of evidence can be a clue of some missing process, method or practices that, at first glance, seems not to sustain the objective but after deeper inspection provides some lack of evidences.

3.2 Organization

Designing patterns is both an individual and a collective task. To this end, meetings are organized. The purpose of these meetings is to engage in the construction of a common reference framework and to compare points of view. From there, a *justification pattern design team* (denoted *design team* in the remainder of the paper) will be able to collectively elicit justification patterns. The team should be small, three to five persons. Small teams encourage *dialogical* interaction (conversation between two people). To tackle the problem of deducting reasoning, psychological studies have shown that dialogical and small groups are very effective [22,23,37]. During the constitution of the design team, one must take into account the psychological biases of system experts. Especially for experts involved in the design of a system whose compliance to the certification objectives depends on the designed patterns. These experts are susceptible to confirmation bias (as identified in [24]) and thus may try to build assurance cases enforcing the compliance of their own system (a typical case of such a bias is illustrated in the accident report [12]).

During meetings, the experts must have all the necessary information: the standard, all the technical documentation, the past experiences. To create the patterns, the team must be able to share a common medium and "*draw*" patterns together (e.g. white board with markers). In order for the experts to work

[4] In a sense, we are quite close to the Delphi method [28] here since, between two meetings, the experts think alone, in isolation, about what has been collectively produced, the synthesis, and give their feedback at the next meeting. However, unlike the Delphi method, in our method much of the work is done during group meetings.

individually between meetings, it is also important to have minutes of meeting that include the patterns and detailed explanations of the elements of the patterns.

We recommend to have a design team composed of one *facilitator* managing the meetings and recording the patterns and *experts* designing the pattern.

Facilitator Role. The facilitator should help determine whether or not it is acceptable to pass from a set of justifications to a given claim. The study of such reasoning has expanded in North America since the 1970s, particularly since the publication of *Logical Self-defense* [16]. In this book, the authors attempt to define a systematic approach to studying informal argumentation. Thus, in recent years, all research that relates to non-formal reasoning has been called *Informal Logic*, *Critical Thinking* and *Argumentation*. To support the experts in their task of eliciting and explaining the inference, the facilitator must be very familiar with Critical Thinking. There is no need for the facilitator to be an expert in the areas covered by the standard, but they will still need to know the vocabulary and the context in order to communicate easily with the experts. Indeed, a minimum of technical knowledge is required for the experts to express their ideas without always having to explain technical issues. The facilitator is thus paramount in identifying a misuse of the pattern formalism that can lead to the following threats to pattern validity: introduction of *unnecessary evidence*, the *lack of evidence* and *fallacious inference*. If several members of the team are familiar with the Critical Thinking, we recommend alternating the role between meetings.

Expert Role. An expert must be a specialist in the field covered by the standard and, more precisely, a specialist in the V&V methods used to define the pattern. Indeed, the justifications and warrant of a pattern are generally related to V&V operations and results. To ensure the acceptance of the patterns, the expert must have credentials recognized by their peers and by the certification authority. Involving recognized experts prevents the design of incorrect patterns due to a *poor knowledge* of the application domain in which the pattern is intended to be used. An expert could be a well-known practitioner, a researcher or a member of the certification authority. Note that, it is better to have both practitioners and members of the authority in the team. Indeed the heterogeneity of the experts can address two threats by helping to identify *missing patterns* and avoiding a *non-holistic view*. A non-holistic view is when the pattern does not treat the whole problem but only adopts the point of view of the applicant or of the certification authority.

3.3 Wording

The way the design team brainstorms has a major impact on the avoidance of common mistakes. Hence, we define *guide words* and *avoid words* to promote an argumentation thinking mindset rather than a temporal thinking one and to ensure that warrants are not forgotten.

Temporal Thinking. One of the major difficulties when developing a pattern is to elicit an inference and not a process. Again, experts know how the system has been designed and they are tempted to graft the development process to the justification pattern. Writing a sequence of actions can lead to simply paraphrasing a process and thus concealing the underlying rationale justifying the claim. The claim is no longer the result of an argument, but of a series of activities and this does not sustain the claim. This threat of *temporal thinking* can be mitigated if the meeting participants avoid using all vocabulary relating to time. In other words, experts should try not to use the words: follow, after, before, then, etc. Instead, the facilitator should question the experts and direct them towards reformulation using the wording: "*the conclusion of*", "*needs*", "*is based on*", etc.

Warrantless Approach. Experts may be familiar with formal logic and tend to build a proof tree instead of a pattern representing informal argumentation. This formal thinking usually leads to *logical* warrants, a symptomatic case is logical decomposition (the claim is the conjunction of the evidence). Of course, if one is able to express the argumentation in a formal way then this formal proof should be a final evidence and does not need to be represented as an argumentation pattern. Nevertheless, the facilitator must seek carefully this kind of warrants since it may conceal the actual warrant that allows the passage from evidence to claim. In the context of argumentation, the experts should avoid warrants containing only logical connectors: "*and*", "*or*", "*entails*", etc.

4 Case Study

We have applied our method on the CAST-32A [6], that serves as a guideline to certify multi-core processor-based systems in avionics. All embedded platforms until now relied on mono-processor hardware or very specific dual-core. In the coming years, only multi-core processor hardware will be available on the market and the airframers will have no choice but to embed these new architectures. Since the CAST-32A is a new guideline, there is currently no process to refer to and applicants must create their argumentation from scratch. This is a perfect opportunity to apply our method.

4.1 Application of the Method

The *Design team* was composed of: 1. a senior expert on multi-core processor architectures, predictable programming and the mainstream aeronautics validation and verification process; 2. a junior safety expert of the safety assessment of technical systems; 3. a facilitator with a solid experience in justification pattern design and familiar with the overall V&V process used in aeronautics.

During the project, the justification pattern design team had a meeting once every two weeks, and each member individually took some time to ponder on the work that was done.

By the end, the design team defined 15 patterns[5] that address 5 high-level objectives of the guideline (some objectives, such as those that are purely organizational, have not been addressed in the context of this project).

4.2 Justification Pattern for RU3

Let us describe one of the objectives, namely RU3 (for *resource usage 3*) and part of the associated patterns. This objective concerns interference situations, which are feared situations where software can encounter strong slowdowns.

Objective RU3. *The applicant has identified the interference channels that could permit interference to affect the software applications hosted on the multicore processor cores, and has verified the applicant's chosen means of mitigation of the interference.*

`Claim:` RU3
`Warrant:` `(W1)` Check completeness of interference and mitigation
`Evidence:`
`(E1)` Identification and classification of interferences
`(E2)` Verified mitigation means

Fig. 4. Pattern for RU3

`Claim:` E1
`Warrant:` `(W2)` Platform stressing strategy
`Backing:` Architecture mastering
`Evidence:`
`(E3)` Interference identification
`(E4)` Effect classification
`Given:` Configuration, temporal constraints

Fig. 5. Pattern for E1

Fig. 4 shows its transcription as a pattern. Evidence (E1) states that the existing interferences have been identified and classified. Focusing on (E1), Fig. 5, it has been achieved because there was a stressing benchmark analysis that has collected the effects of each interference (strategy (W2)). Those effects can be expressed in different units (e.g. delay, bandwidth). Evidence (E3) points to a report that summarizes which interferences have been identified, how they have been identified, and why the identification is sound and complete. Evidence (E4) points to a safety report that details the acceptable effects on the hosted applications. From this information, the applicant has defined adequate means of mitigation to prevent, for instance, unacceptable effects. Evidence (E2) collects all those means of mitigation, how they mitigate each unacceptable interference and how they were verified. The applicant can argue the compliance with RU3 because an expert, who masters the architecture, has reviewed and double-checked that each interference has been correctly mitigated (W1).

[5] Available at https://w3.onera.fr/phylog/patterns.

4.3 Lessons Learned

The Facilitator Supports the Elicitation of Patterns. Both experts clearly reported that the facilitator helped them understand the argumentation approach. When designing the first patterns, experts tended to not know how to express the warrant, to skip it, and to describe a process rather than an argument. Interestingly, the further the project progressed, the more the experts understood how to operate. However, although the experts became familiar with the approach, a facilitator was always needed. By being outside of the context, facilitators rephrase the discussions and question the foundations of what may seem obvious to experts (by using, for example, the Douglas Walton's critical questions [11]). In the future, it would be preferable to define more precisely the skills of the facilitator as well as the way in which meetings should be conducted. To do this, we can take inspiration from, for example, [28].

Wording Importance. The wording was really necessary to prevent the experts falling in false reasoning. It helped counter the tendency to express what needs to be done rather than what leads to a justification.

Process/Patterns Evaluation. To evaluate the process, we must turn to an evaluation of the produced patterns. At the end, the design team presented the justification patterns in a workshop, the participants of which were: two contributors to the CAST-32A, five well-known experts from the aeronautics industry and three certification authority members.

The overall feedback was very positive. For industrial experts, the patterns are very useful and help clarify some implicit / ambiguous textual rationales. Moreover, because they give concrete evidence, they simplify discussion between stakeholders. Industrial experts also gave some suggestions to prepare certification audits with the patterns. For CAST-32A contributors, the patterns were compliant with the writers' perspective. They confirmed that patterns highlight some elements that were only in the writers' minds. In fact, the design team has extracted the implicit structure of the sentences, the main elements expected to be supplied and made explicit the reasoning of the writers. For certification authority members, patterns provide a framework for legible and clear presentation of justifications and their rationale.

Of course, the patterns were not free of defects (some evidences were missing and some warrants were not explicit enough). In addition, it appeared that an additional pattern would be useful for easing the discussion and moving around the other patterns. The conclusion we can draw from this evaluation is that there is one step missing from our process. We could add an expert committee assessment to our process. In this new process, the assessment committee would become the validation team. At the end, this team would be involved in a validation activity and would address the following challenges:

– *fallacious reasoning:* find conditions where the warrants do not sustain the claim. Those conditions can either be considered as rebuttal and must be integrated into the patterns, or disclose a flaw to be corrected;

- *lack of evidence:* find conditions where the evidences are not sufficient to sustain the claim. In that situation, the design team should identify them out of the processes, methods and practices;
- *missing patterns:* find another way to establish the claim. This may look challenging since this requires designing a new pattern but it can be addressed by trying some slight modifications of the existing patterns and assessing the validity of this new version.

5 Related Work

If there are many notations to structure an assurance case, there are fewer works addressing the justification patterns elicitation. In [42], the authors focus on security requirements and propose a tool to manage these requirements. In addition, they are interested in capturing the rationality of these requirements by using Toulmin's scheme. While they give some key elements to produce such models, they do not go into the details (role, wording, etc.) of the elicitation method. In another field, [13] are interested in safety arguments and provide a guide on how to build a GSN diagram properly, but no elicitation method is proposed. In the avionic context, the authors of [43,44] propose a UML profile, namely SafeUML, dedicated to safety requirements for an aeronautics guideline. This profile defines a set of stereotypes to model specific concepts associated to safety. The purpose of their approach is to facilitate communication between safety experts, software developers and certification authorities. Regarding the links with our approach, the different certification objectives are seen as requirements in SafeUML. Tractability between requirements and design choices is achieved by a stereotype "*rationale*" which has a text field to give an explanation. So, the use of our patterns could easily be added to SafeUML. Indeed, their application, linked to the rationale, would model more precisely this explanation of why a design meets a certification objective.

This idea of having a modeling framework to organize the certification elements is not new. It was particularly highlighted by [1,25]. Among the works on compliance to a regulation, we can mention, for example, the SafetyMet metamodel safety oriented [38] or the UML stereotype developed by [31]. In the second case, with the UML stereotype-based approach, the authors give a generic approach to model a safety certification standard and make the link between the concepts of the system designer and those of the standard. Their method consists in supporting modeling a safety standard in their UML profile, then to make the link, according to precise rules materialized by OCL constraints, between the domain model and the certification model. This work, as identified by [1], models the *structure* of the standard to provide an organization of the elements provided by the applicant to satisfy the standard. However this work does not clarify the *intent* of the objectives of standard, this task being assigned here to the experts who will model the safety standard.

Still in the field of modeling, [14] propose to add an argumentative dimension to a combine model of i* and Nomòs [35] with the *Acceptability Evaluation*

framework [17]. The purpose here is to capture expert discussions to determine whether the requirements in systems are compliant with a standard or whether there are irregularities. Unlike us, the authors focus here on an argumentation with contradictory points of view and the certification of a specific system, not to eliciting requirements from the standard.

Seeking to capture variability in regulatory texts, [34] propose a formalism to model conditions and exceptions in a regulation. In addition, their framework also allows them to express alternatives that are compliant with the standard. We could imagine a link between their approach and ours. Indeed, sometimes, for one certification objective, several justification patterns could be applicable. Depending on the chosen pattern, it is necessary to guarantee new sub-objectives which are the evidences of the pattern. Representing these alternatives and all the possible solutions could be a significant help for system designers.

Finally, close to our work, [15] use a Goal-Oriented approach to refine guideline objectives. This method allows clarify law and certification terms, that are subject to interpretation. However, unlike us, they do not attempt to highlight the rationality that allows us to conclude from sub-objectives to the main claim. Clearly explaining this, in particular by means of a warrant, is crucial for the certification authority side that is rarely taken into account as identified by [1].

6 Conclusion

This paper introduced a method to guide the design justification patterns by experts. The method has been applied to a new position paper written for multi-core processor and allowed design several patterns accepted by end users.

Repeatability and reproducibility are the main limitations of our approach. For the moment, even if the method results from a long standing experience, we have only used it on the CAST-32A. In the future, to consolidate the method, we will ask a new team to define patterns for the same standard and compare the results. As there are many ways to develop an argument, we will have to define the notion of equivalence between two patterns. A second axis of consolidation is to define patterns for another standard with the same team.

Future work will also need to address more deeper the problems of biases (anchoring, availability, bandwagon effect, halo effect, overconfidence, etc.) that may arise and their mitigation. To do this, we will have to rely on methods and works on expert knowledge elicitation.

Eventually, the current method does not characterize the assurance level provided by a given pattern nor an assessment of its cost. Our future works need to provide guidelines to document such impact to support the trade-off analysis of the applicant when several patterns are applicable. The question of how to instantiate a pattern is also an important issue and we will provide guidelines to help applicants on this matter as well as a method to conduct efficient certification audits with justification patterns and instances.

References

1. Akhigbe, O., Amyot, D., Richards, G.: A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance. Requirements Eng. **24**(4), 459–481 (2018). https://doi.org/10.1007/s00766-018-0294-1
2. Alexander, C., Ishikawa, S., Silverstein, M.: A Pattern Language: Towns, Buildings Construction. Oxford University Press, Oxford (1977)
3. Alexander, R., Hawkins, R., Kelly, T.: Security assurance cases: motivation and the state of the art (2011)
4. Avizienis, A., Laprie, J., Randell, B., Landwehr, C.E.: Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable Sec. Comput. **1**(1), 11–33 (2004)
5. Bieber, P., et al.: MIMOSA: towards a model driven certification process. In: Proceedings of European Congress Embedded Real Time Software And Systems (2016)
6. Certification Authorities Software Team: Multi-core Processors - Position Paper. Technical report CAST 32-A, Federal Aviation Administration (2016)
7. Duffau, C., Polacsek, T., Blay-Fornarino, M.: Support of justification elicitation: two industrial reports. In: Krogstie, J., Reijers, H.A. (eds.) CAiSE 2018. LNCS, vol. 10816, pp. 71–86. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-91563-0_5
8. Emmet, L., Cleland, G.: Graphical notations, narratives and persuasion: a pliant systems approach to hypertext tool design. In: Proceedings of Hypertext and Hypermedia, HYPERTEXT 2002 (2002)
9. Fisher, M., Keil, F.C.: The illusion of argument justification. J. Exumlperimental Psychol. Gen. **143**(1), 425 (2014)
10. Gamma, E., Helm, R., Johnson, R., Vlissides, J.: Design Patterns: Elements of Reusable Object-oriented Software. Addison-Wesley Longman Publishing, Boston (1995)
11. Godden, D.M., Walton, D.: Argument from expert opinion as legal evidence: critical questions and admissibility criteria of expert testimony in the American legal system. Ratio Juris **19**(3), 261–286 (2006)
12. Haddon-Cave, C.: The Nimrod Review: an independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006, report, vol. 1025. Derecho International (2009)
13. Hawkins, R., Kelly, T., Knight, J., Graydon, P.: A new approach to creating clear safety arguments. In: Dale, C., Anderson, T. (eds.) Advances in Systems Safety. Springer, London (2011). https://doi.org/10.1007/978-0-85729-133-2_1
14. Ingolfo, S., Siena, A., Mylopoulos, J., Susi, A., Perini, A.: Arguing regulatory compliance of software requirements. Data Knowl. Eng. **87**, 279–296 (2013)
15. Ishikawa, F., Inoue, R., Honiden, S.: Modeling, analyzing and weaving legal interpretations in goal-oriented requirements engineering. In: Proceedings of International Workshop on Requirements Engineering and Law (2009)
16. Johnson, R.H., Blair, J.A.: Logical Self-Defense (Key Titles in Rhetoric, Argumentation, and Debate Series), 1st edn. International Debate Education Association, Brussels (2006)
17. Jureta, I., Mylopoulos, J., Faulkner, S.: Analysis of multi-party agreement in requirements validation. In: Proceedings of International Requirements Engineering Conference - RE 2009 (2009)
18. Kelly, T., Weaver, R.: The goal structuring notation - a safety argument notation. In: DNS 2004 Workshop on Assurance Cases (2004)

19. Kelly, T.P., McDermid, J.A.: Safety case construction and reuse using patterns. In: Daniel, P. (ed.) Safe Comp 97. Springer, London (1997). https://doi.org/10.1007/978-1-4471-0997-6_5
20. Kletz, T.: Hazop & Hazan - Identifying and Assessing Process Industry Hazards. Institution of Chemical Engineers, New York (1999)
21. Knight, J.: Advances in software technology since 1992. In: National Software and Airborne Electronic Hardware Conference, ser. FAA (2008)
22. Laughlin, P.R.: Collective induction: twelve postulates. Organ. Behav. Hum. Decis. Process. **80**(1), 50–69 (1999)
23. Laughlin, P.R., Hatch, E.C., Silver, J.S., Boh, L.: Groups perform better than the best individuals on letters-to-numbers problems: effects of group size. J. Pers. Soc. Psychol. **90**(4), 644 (2006)
24. Leveson, N.G.: The use of safety cases in certification and regulation (2011)
25. Lewis, R.: Safety case development as an information modelling problem. In: Dale, C., Anderson, T. (eds.) Safety-Critical Systems: Problems Process and Practice. Springer, London (2009). https://doi.org/10.1007/978-1-84882-349-5_12
26. McDermid, J.A.: Support for safety cases and safety arguments using SAM. Reliab. Eng. Syst Saf. **43**(2), 111–127 (1994)
27. Méry, D., Schätz, B., Wassyng, A.: The pacemaker challenge: developing certifiable medical devices (dagstuhl seminar 14062). In: Dagstuhl Reports. vol. 4, no. 2 (2014)
28. Meyer, M.A., Booker, J.M.: Eliciting and Analyzing Expert Judgment: A Practical Guide. SIAM, Philadelphia (2001)
29. Moshman, D., Geil, M.: Collaborative reasoning: evidence for collective rationality. Think. Reason. **4**(3), 231–248 (1998)
30. OMG: Structured assurance case meta-model (SACM). Technical report Object Management Group (2013)
31. Panesar-Walawege, R.K., Sabetzadeh, M., Briand, L.: A model-driven engineering approach to support the verification of compliance to safety standards. In: Proceedings of International Symposium on Software Reliability Engineering (2011)
32. Polacsek, T.: Validation, accreditation or certification: a new kind of diagram to provide confidence. In: Proceedings of International Conference on Research Challenges in Information Science, RCIS (2016)
33. Rinehart, D.J., Knight, J.C., Rowanhill, J.: Current practices in constructing and evaluating assurance cases with applications to aviation. Technical report NASA (2015)
34. Siena, A., Jureta, I., Ingolfo, S., Susi, A., Perini, A., Mylopoulos, J.: Capturing variability of law with *Nómos* 2. In: Atzeni, P., Cheung, D., Ram, S. (eds.) ER 2012. LNCS, vol. 7532, pp. 383–396. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34002-4_30
35. Siena, A., Mylopoulos, J., Perini, A., Susi, A.: Designing law-compliant software requirements. In: Laender, A.H.F., Castano, S., Dayal, U., Casati, F., de Oliveira, J.P.M. (eds.) ER 2009. LNCS, vol. 5829, pp. 472–486. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04840-1_35
36. Toulmin, S.E.: The Uses of Argument, 1st edn. Cambridge University Press, Cambridge (1958). Updated Edition (2003)
37. Trognon, A., Batt, M., Laux, J.: Why is dialogical solving of a logical problem more effective than individual solving?: a formal and experimental study of an abstract version of Wason's task. Lang. Dialogue **1**(1), 44–78 (2011)

38. de la Vara, J.L., Panesar-Walawege, R.K.: SafetyMet: a metamodel for safety standards. In: Moreira, A., Schätz, B., Gray, J., Vallecillo, A., Clarke, P. (eds.) MODELS 2013. LNCS, vol. 8107, pp. 69–86. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41533-3_5
39. Wassyng, A., Joannou, P., Lawford, M., Thomas, M., Singh, N.K.: New standards for trustworthy cyber-physical systems. In: Omanovsky, A., Ishikawa, F. (eds.) Trustworthy Cyber-Physical Systems Engineering, pp. 337–368. Addison-Wesley Longman Publishing, New York (2016). Chap 13
40. Wassyng, A., et al.: Can product-specific assurance case templates be used as medical device standards? IEEE Des. Test **32**(5), 45–55 (2015)
41. Weinstock, C.B., Goodenough, J.B., Hudak, J.J.: Dependability cases. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, Technical report (2004)
42. Yu, Y., Franqueira, V.N., Tun, T.T., Wieringa, R.J., Nuseibeh, B.: Automated analysis of security requirements through risk-based argumentation. J. Syst. Softw. **106**, 102–116 (2015)
43. Zoughbi, G., Briand, L., Labiche, Y.: A UML profile for developing airworthiness-compliant (RTCA DO-178B), safety-critical software. In: Engels, G., Opdyke, B., Schmidt, D.C., Weil, F. (eds.) MODELS 2007. LNCS, vol. 4735, pp. 574–588. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-75209-7_39
44. Zoughbi, G., Briand, L., Labiche, Y.: Modeling safety and airworthiness (RTCA DO-178B) information: conceptual model and UML profile. Softw. Syst. Model. **10**(3), 337–367 (2011). https://doi.org/10.1007/s10270-010-0164-x