Evidence Management for Evolutionary Safety Assurance and Certification

Sunil Nair
Department of Software Engineering, Simula Research Laboratory
P.O. Box 134, 1325 Lysaker, Norway
sunil@simula.no

***Abstract*—Safety assurance and certification are amongst the most expensive and time-consuming activities in the development of safety-critical systems. Deeming a system to be safe involves gathering convincing evidence to argue the safe operation of the system, usually according to the requirements of some safety standard. To handle large collections of safety evidence effectively, practitioners need knowledge of how to classify different types of evidence, how to structure the evidence to show fulfilment of standards' requirements, and how to assess the evidence. However, the notion of evidence is vague and safety standards´ requirements can be ambiguous and difficult to understand. Major problems also arise when a system evolves, as the body of safety evidence has to be adequately maintained in order to ensure system safety and allow its demonstration. In this context, this PhD aims to propose a framework for safety evidence management in evolutionary scenarios. The thesis work will concentrate on devising a model-based and customizable infrastructure for storage, manipulation, reuse, and analysis of evolving safety evidence. The infrastructure will be developed and evaluated in the scope of OPENCOSS, a large-scale European research project.**

***Index Terms*—Safety-critical system, safety standards, safety compliance, safety certification, safety evidence, evidence evolution, evidence traceability, change impact**

I. Introduction

Most critical systems in domains such as avionics, railways, and automotive are subject to some form of safety assurance and assessment process as a way to ensure that these systems do not pose undue risks to people, property, or the environment. The most common type is safety certification [13], whose goal is to provide a formal assurance that a system is deemed safe by a licensing or regulatory body.

The assurance or certification process is usually performed based on one or more standards that apply in a given domain. Typical examples of safety standards include IEC61508 [8] for a broad class of systems, DO-178C for avionics [6], the CENELEC standards for railways [9], and ISO26262 for the automotive sector [11].

Such standards for safety critical software or systems usually mandate or recommend a number of development and assessment techniques usually in the form of requirements that are to be met to minimise the risk of system failure. To comply with the standard and to deem the system or software to be safe, one has to provide convincing *evidence* that the relevant requirements in the standard are met. We define evidence for safety certification as *"information or artefacts that contribute to developing confidence in the safe operation of a system"*. In the context of safety certification, safety evidence also aims to show fulfilment of the requirements of a safety standard. Some generic examples of safety evidence are test results, system specifications, and personnel competence.

II. Challenges and Motivation

A clear definition of evidence does not exist and varies from domain to domain. Failing to clearly understand the evidence needs for a system's assessment process [24] can result in two main challenges. First, the supplier may fail to record critical details during system development that the certifier would need. This can be both expensive and laborious, as the supplier has to reconstruct the missing evidence artefacts after-the-fact. Second, not knowing ahead of time what the certifiers will receive as evidence may affect the planning and organisation of the certification activities. The certifier may find it hard to develop sufficient confidence in the system undergoing certification without having agreed to the evidence requirements first [7]. In addition, attention needs to be paid by the supplier to how this evidence is organized and assessed. Especially, for large-scale systems, if the evidence is not structured and assessed properly, its sheer volume and complexity can jeopardize the clarity of the safety requirements being met [26].

Furthermore, system evolution often becomes costly because it entails regenerating the entire body of evidence that was previously collected. As a result, the evidence chain should be re-examined whenever the system is modified and, if the evidence is no longer adequate, new evidence should be provided. As a result, when a system is certified, the supplier usually avoids subsequent modifications. This hinders innovation, as the use of new technologies would require re-certification.

With return of investment as a primary focus in industry when dealing with safety certification, the main motivators for this thesis are, **lack of precision and large variety of certification requirements, ambiguity of evidence definition, ambiguities in existing reuse strategies and high cost for (re) certification.**

III. Related Work

Even though related work exists ([1][19][24]), little light has been shed towards the problem of providing and understanding evidence for safety certification. There is also prior work that studies specific types of evidence [9]. Strands of work have provided classifications of artefacts that can be used as evidence [10], and classifications of evidence for specific domains and standards [12][23].

Some previous work has been done to standardise the process of evidence collection, development, evaluation and management. SAEM (Software Assurance Evidence Metamodel [20]) establishes the necessary models of evidence elements required for detailed compliance and risk analysis. ARM (Argumentation Metamodel [21]) defines a metamodel for representing structured arguments that facilitates projects by allowing them to effectively and succinctly communicate in a structured way that their systems and services are meeting their assurance requirements. An evidence-related conceptual model for IEC61508 with relationships beyond those between artefacts used as evidence was introduced in the past [23].

Although the above mentioned strands of work can be considered to have provided more insights into evidence requirements for compliance purposes, they still lack details about effective management of safety evidence requirements and relationships in evolutionary context. Past work has been either too generic or too specific allowing very little space for real life implementation. None of the above has targeted at developing a *unified* classification of evidence [16], leading to two main gaps: first, the term evidence has largely remained a *vague* notion due to the lack of a general classification; and second, there has been little opportunity for cross-comparison of evidence requirements in different domains, standards, and systems due to the absence of a higher-level conceptual framework. The lack of clear definition of evidence and knowledge about the purpose of each evidence item has eventually shed very little light on how to effectively reuse evidence items. Moreover, past models of evidence requirements have not included the evolutionary context of the system and the evidence items.

Despite the limitations identified, above work are considered complementary to the work proposed in this thesis. Our aim is to develop a more general view on safety evidence requirements with evolution of the system in focus.

IV. Research Questions

The overall objective of the thesis is to provide better practices and tools for safety evidence management and traceability for certification and assurance processes. The following are the research questions (RQs) formulated for this thesis:

RQ1. *What types of information/artefacts contribute as evidence for demonstrating compliance?* - This RQ aims at identifying and classifying the different types of evidence information used for demonstrating compliance. Such a classification would serve, as a body of knowledge to better understand the evidence requirements.

RQ2. *What kind of relationship links exists among the various evidence types envisaged by different safety standards?* – This RQ aims at establishing traceability links between various evidence artefacts. Such a traceability schema would allow knowing which evidence type is related to others and would be helpful during reuse of evidence information.

RQ3. *What safety requirements do the types of evidence meet?* – The aim of this RQ is to identify the various safety claims that can be made with the different types of evidence identified in the previous RQ. This ontology of safety properties and evidence types would allow clarifying the notion of an evidence item and its purpose of existence.

RQ4. *How can we maintain the links between evidence items as the underlying system evolves?* – The aim of this RQ is to analyse how change impact propagates among the linked evidence items when an evidence item is modified. The analysis will help in deciding beforehand, if a particular change needs to be made by presenting an overall picture of items that would be affected as a result.

V. Proposed Solution and Research Methods

This thesis aims to provide methods and supporting tools for understanding evidence requirements and managing them, placing particular focus on situations in which the evidence changes.

The thesis will develop an *Infrastructure for Evolutionary Evidential Management* (IEEM), which will require devising new evidence management techniques and implementing prototype tools that will help maintain and analyse evidence information. The IEEM will incorporate different types of evidence used for compliance purposes, the assertion that could be made about them in relation to the safety properties, tool support automatically capturing evidence trace information and tool support for change-impact analysis. The tools would be based on model-driven engineering techniques, which can help in creating formalized interpretations of standards [23] being complied too and will serve as a primary vehicle for tackling the challenges presented above.

To achieve the proposed solution, a number of research methods will be employed. First, a systematic literature review on the state of the art of evidence provision and management will be conducted. Next, a survey on the state of the practice of evidence provision and management will be conducted. The results of the review and survey will be compared to identify potential gaps and needs. A taxonomy for evidence types and ontology of assertions will be build based on the review and survey and validated through experiments. Investigation of existing traceability techniques for safety certification and tool support for evidence traceability will be performed to build the evidence traceability model. Tool support for the model will be then developed based on these studies. Investigation of existing impact analysis techniques will be performed. Tool support for the same will be developed. Finally, an initial framework for IEEM will be build based on the research insights obtained from the above studies and validated with case studies from the OPENCOSS project.

VI. Progress

This section gives an overview of the work performed so far in relation to the addressing the RQs. The RQs being addressed in each study is denoted in brackets in the title.

A. State of the Art (RQ1)

As mentioned above, there exists no past work on a *unified* classification of evidence types. To assimilate the existing knowledge in the academic literature about safety evidence, concentrating on the information that constitutes evidence, structuring of evidence, and evidence assessment, a *Systematic Literature Review* (SLR) was performed [14]. An extended SLR [16] drew on 216 peer-reviewed publications. As part of our work, we classified into a hierarchical taxonomy the various notions of evidence that we gleaned from the literature. The taxonomy, which includes 49 evidence types, is the most comprehensive classification of safety evidence built to date.

B. State of the Practice (RQ1)

A survey was performed to identify state of the practice in evidence management [16]. 53 participants from 11 different domains and 16 countries participated in the survey. The survey was a way to evaluate the results obtained from the state of the art study. Some commonalities and difference in the literature and practice are reported. The results of the survey indicate that much manual work is still performed when having to check (1) completeness of the body of evidence and (2) evidence change impact analysis. This is a major motivation for the prototype tool to be developed as part of this thesis.

C. Evidence Evolution Scenarios (RQ4)

Possible scenarios in which safety evidence can evolve with the help of the industrial partners from the OPENCOSS project were identified. A possible solution based on the use of model-driven engineering was drafted and published [4]. In addition to the ideas about the application of model-driven engineering for management of evolutionary chains of evidence, the paper sets the background on which the solution is based and that makes us believe that the solution is necessary and feasible.

D. Evidence Traceability (RQ2)

To better understand the traceability research trends and advancements, a review on past traceability research was performed [15], specifically at RE conference as it is the arena best known for traceability related research. Based on this study, the motivation for safety evidence traceability, its challenges, and its open issues were identified. Furthermore safety evidence traces that must be created and maintained were identified. As a result, we have created SafeTIM [18], a traceability information model for safety evidence that can help both researchers and practitioners to better understand the importance of safety evidence traceability, thereby improving project management and reducing cost.

E. Evidence Metamodel (RQ2 & RQ4)

In our approach to better elaborate the concept of evidence, we present how an artefact can be used as safety evidence [5]. A conceptual model of safety evidence that is part of a larger safety compliance framework was proposed. We identified the set of concepts and relationships that characterize artefacts and those that characterize the pieces of safety evidence, and make clear distinctions between the two notions. The model can help practitioners to better deal with activities related to safety evidence management such as evidence traceability, change impact analysis, specification of confidence in evidence, and evidence reuse.

F. Tool Review (RQ2 & RQ4)

As part of the OPENCOSS deliverable [22], several tools for evidence management were reviewed. A final set of 71 tools that might be relevant for evidence management in OPENCOSS was identified. As a result of the review, two major research areas for improvement were identified: (1) Advanced traceability management, (2) Advanced impact analysis

VII. Planned Work

The work performed so far helped us to understand the current trends in evidence management and highlighted the gaps and needs. The future work is aimed towards satisfying these needs.

A. Evidence Assertions (RQ3)

An evidence assertion is a minimal proposition that describes straightforward factual information concerning an item of evidence [26]. Such assertions are usually claims about what an item of safety evidence can satisfy. Evidence assertion would enable to clarify the role of a particular piece of evidence as early as possible and helps in managing them effectively. As part of the thesis, a classification of evidence types and evidence assertion will be developed to understand the purpose of each evidence type and its role. This knowledge would help in bringing a shared common understanding about evidence and will enable reuse.

B. Tool Support (RQ2 & RQ4)

As part of the on-going work, the Evidence Metamodel and SafeTIM will be evaluated with real industrial data from OPENCOSS. Based on the evaluation of the models and the tool review, I aim to develop a prototype tool to support evidence traceability. This tool will try to automatically capture and maintain evidence traces using techniques such as information retrieval. Some potential challenges will be to identify the right level of granularity of evidence/artefacts specification for adequately tracing them, and traces suggestion [1]. Once the required level of granularity is identified, I aim to perform an evidence change-impact analysis. This will be incorporated in the prototype tool that will help the practitioner to identify the impact of change of one piece of evidence on the other pieces of evidence. I also aim to present some guidance on how to handle the changes.

VIII. Evaluation

Different means of evaluation will be employed at different phases of the thesis. Iterative validation activities will be

conducted all throughout the project timeline that will enable us to verify the implementation and adaptation of specific facets of the thesis. The results obtained will allow us to redefine the proposed solution for traceability and impact analysis. To achieve this, the conceptual work proposed in the thesis will be evaluated by *peer-review* in conferences, journals and workshops. I aim to run *experiments* iteratively to identify the understandability of the evidence types and the assertions made regarding them. To evaluate the final outcome of the thesis (IEEM and the prototype tools), *case studies* will be conducted with industrial partners from OPENCOSS, to assess the applicability and adoption of the proposed solution. The benefits of the proposed solutions will be measured by comparing the results before and after the adoption of IEEM and the tools. Further empirical validation such as conducting *surveys* with domain experts who would validate the usefulness of IEEM will also be done.

IX. Contributions and Conclusion

Understanding the notion of safety evidence, managing and presenting them clearly are an important but complex activity during the safety assurance and certification process. A better knowledge of what evidence is required for certification, what relationships exist between them and how can this information be managed, analysed and reused can help reduce certification costs and further make certification results more credible.

With this in mind, this thesis aims to provide an *Infrastructure for Evolutionary Evidential Management* (IEEM), that proposes better practices for understanding the notion of evidence requirements, capturing traceability among the evidence items, enabling better change impact analysis and facilitate reuse of evidence information. The thesis aims to clarify the notion of evidence by providing a taxonomy of evidence types. To further elaborate on the concept of evidence, the thesis provides the safety properties met by each evidence type. The tool support developed as part of IEEM, try to automatically capture the links between evidence items. As a result, this will allow us to perform change-impact analysis to identify the change propagation. The IEEM along with the tool support can significantly reduce cost and effort involved in safety certification.

Acknowledgment

The research leading to this thesis has received funding from the FP7 programme under the grant agreement n° 289011 (OPENCOSS) and from the Research Council of Norway under the project Certus SFI.

References

[1] W. Afzal, R. Torkar, R. Feldt, “A systematic review of search-based testing for non-functional system properties”, Info. Softw. Technol. 51(6): 957-976, 2009.

[2] CENELEC ENV 50129 - Railway applications - Safety related electronic systems for signalling, European Committee for Electrotechnical Standardisation (1998)

[3] J. Cleland-Huang, O. Gotel, A. Zisman (eds.), “Software and Systems Traceability”. Springer (2012)

[4] J. L. de la Vara, et al., “Towards a Model-Based Evolutionary Chain of Evidence for Compliance with Safety Standards”, Computer Safety, Reliability, and Security Workshop (SASSUR) SAFECOMP (2012)

[5] J. de la Vara, S. Nair, R. P. Walawege, “On the Use of Artefacts as Safety Evidence: A Conceptual Model, Technical Report” (2013)

[6] DO-178C/ED-12C, Software Considerations in Airborne Systems and Equipment Certification. (2012)

[7] D. Falessi, et al., “Planning for Safety Evidence Collection: A Tool-Supported Approach Based on Modeling of Standards Compliance Information”. IEEE Softw. 29(3): 64-70, 2012

[8] Functional safety of electrical / electronic / programmable electronic safety-related systems (IEC 61508), (2005).

[9] A. Galloway et al. "Proof vs testing in the context of safety standards." Digital Avionics Systems Conference, 2005. DASC 2005. The 24th. Vol. 2. IEEE, 2005.

[10] I.M. Habli, “Model-based assurance of safety-critical product lines”, PhD thesis, University of York, 2009.

[11] ISO/DIS - 26262-8 Draft International Standard Road vehicles — Functional safety (2009).

[12] M. Johansson, R. Nevalainen.: “Additional requirements for process assessment in safety–critical software and systems domain”, J. Softw. Maint. Evol.: Res. Pract.. doi: 10.1002/smr.499, 2010.

[13] A. Kornecki, Z. Janusz, "Certification of software for real-time safety-critical systems: state of the art." Innovations in Systems and Software Engineering 5.2 (2009): 149-161.

[14] S. Nair, J. de la Vara, M. Sabetzadeh, L. Briand, “Classification, Structuring, and Assessment of Evidence For Safety: A Systematic Literature Review”. In Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST), (2013)

[15] S. Nair, J. de la Vara, S. Sen, “A Review of Traceability Research at the Requirements Engineering Conference”. 21st IEEE International Requirements Engineering Conference (2013)

[16] S. Nair, J. de la Vara, M. Sabetzadeh, L. Briand, “An Extended Systematic Literature Review on Classification, Structuring and Assessment of Evidence for Safety Compliance, Technical Report”. (2013)

[17] S. Nair J. de la Vara, M. Sabetazdeh, D. Falessi, “The State of the Practice on Evidence Management for Compliance with Safety Standards, Technical Report”. (2013)

[18] S. Nair, J. de la Vara, A. Melzi, G. Tagliaferri, L. de-la-Beaujardiere, and F. Belmonte, “Safety Evidence Traceability: Problem Analysis and Model, nical Report”. (2013)

[19] J. Nicolás, T. Ambrosio. "On the generation of requirements specifications from software engineering models: A systematic literature review." Information and Software Technology 51.9 (2009): 1291-1307.

[20] OMG: Structured Assurance Evidence Metamodel (SAEM) (2010)

[21] OMG:Argumentation Metamodel (ARM) (2010)

[22] OPENCOSS D6.1 - Baseline for the evidence management needs (2012)

[23] R. Panesar-Walawege, M. Sabetzadeh, and L. Briand, “Supporting the Verification of Compliance to Safety Standards via Model-Driven Engineering: Approach, Tool-Support and Empirical Validation”, In the Journal of Information and Software Technology. (accepted paper) (2013)

[24] A. Singhal, A. Singhal, “A systematic review of software reliability studies”, Softw. Eng.: Inte. J. 1(1), 2011.

[25] M. J. Squair, "Issues in the application of software safety standards." Proceedings of the 10th Australian workshop on Safety critical systems and software-Volume 55. Australian Computer Society, Inc., 2006.

[26] L. Sun.: Establishing Confidence in Safety Assessment Evidence. PhD thesis, University of York. (2012)

[27] S. P. Wilson, K.P. Tim, and M. A. John A, "Safety case development: Current practice, future prospects." Safety and Reliability of Software Based Systems. Springer London, 1997. 135-156.