Using Model-Driven Engineering for Managing Safety Evidence: Challenges, Vision and Experience

Rajwinder Kaur Panesar-Walawege[1,2], Mehrdad Sabetzadeh[1], Lionel Briand[1,2]
[1]*Simula Research Laboratory, Lysaker, Norway*
[2]*University of Oslo, Norway*
Email: {rpanesar,mehrdad,briand}@simula.no

***Abstract*—Certification is a major prerequisite for most safety-critical systems before they can be put into operation. During certification, system suppliers often have to present a coherent body of evidence demonstrating that the developed systems are safe for operation. Regardless of the certification approach taken (process-based or product-based), collection of proper evidence at the proper stage of development is critical for successful certification. Currently, system suppliers and certification bodies alike are facing various challenges in relation to safety evidence collection. Notably, they find it hard to interpret the evidence requirements imposed by the safety standards within the domain of application; little support exists for recording, querying, and reporting evidence in a structured manner; and there is a general absence of guidelines on how the collected evidence supports the safety objectives.**

This paper states our position on how safety evidence should be characterized and managed. Specifically, we propose the application of Model-Driven Engineering as an enabler for performing the various tasks related to safety evidence management. We outline our current work on the specification of safety evidence requirements, upfront planning of evidence collection activities, tailoring of evidence information to domain-specific needs, and storage of evidence information. Based on this work, we identify a number of challenges that need further investigation and provide a future research agenda for managing safety evidence for software safety certification.

***Keywords*-UML; Profile; safety; certification;**

I. Introduction

As we create increasingly complex control systems incorporating both software and hardware, it is becoming crucial for these systems to be certified as safe for operation. A system is considered safe when it can perform its intended function without posing undue harm to the environment within which it operates. It is becoming the norm for safety critical systems to be certified by third-party certification bodies.

A key requirement of safety certification is the provision of evidence that a system complies with the applicable safety standards. The two main aspects under consideration here are: the standards involved, and the evidence that shows the compliance of the system with the specified standards. The standards prescribe the procedures for compliance and the system supplier creates, *during* the development of the system, the necessary evidence to meet the compliance requirements.

The compliance procedures may be process-based or product-based. In a process-based certification procedure, the safety of the system is assured by following prescribed activities that employ specific techniques to ensure a certain level of safety; whereas in product-based certification, a well reasoned argument that is supported by product-based evidence is required. This argumentation and evidence is usually structured into what is called a safety case [1]. Whatever the advantages or drawbacks of the two approaches, the ideal case is to have strong evidence created via a structured development process that backs the safety arguments of the product being certified. Thus we maintain that both process-based and product-based certification procedures are important for assuring the safety of a system and the commonalty between the two is the requisite compliance evidence.

In this paper, we present our experience with certification in the Maritime and Energy (M&E) industry. One of the main standards for certification in M&E is the IEC61508 standard [2] for functional safety of electrical/electronic/programmable electronic systems. Functional safety is paramount in M&E as their safety-critical systems are increasingly reliant on software. M&E now utilize various Integrated Software-Dependent Systems[1] (ISDSs) in such areas as fire and gas detection, drilling and production, vessel propulsion, steering and navigation. Hence the suppliers of these systems are increasingly required to have them certified by recognized certification bodies. In M&E, certification is important not only to assure reduction in risks but also to assure continued business. The challenge is less about whether to use process-based or product-based certification, and more about how to provide a consistent understanding of the information in the IEC61508 certification standard and how to manage the certification in a systematic and timely manner.

In this paper, we discuss the challenges with using the current certification standards in Section II. We then propose our vision on how to tackle these challenges in Section III. Section IV highlights the current work we have performed in taking this vision forward. Further work that still needs to be addressed is covered in Section V. We conclude our discussion in Section VI.

II. Challenges in Safety Evidence Management

The use of recognized standards for certifying complex control systems is the norm for providing assurance to the

[1]Integrated systems for controlling, monitoring and maintaining safety that may be connected via communication networks.

public that the system will be safe during its operation. Without standards upon which to base the certification requirements, the process would become ad hoc. Standards provide a means of accumulating and sharing best practices and providing a structure to the certification process. However, the use of standards does pose some challenges to system suppliers and certifiers alike.

Creating common interpretations. Suppliers need to recognize that it is not sufficient to build safe systems, they will also need to demonstrate that a system is safe and in order to do so they need to collect the requisite evidence whilst building the system and not after the fact. Collating evidence once the system has been built can be a very expensive undertaking that may still not yield the required results. This means there should be a consistent understanding and an agreed-upon interpretation of the standard used, and all parties involved should know what evidence is to be collected and maintained in readiness for certification. This common understanding also needs to extend to the certification body – it would hardly be useful for the supplier and the certifier to have different interpretations of the standard being used. These different interpretations occur due to the standards being rather large documents expressed textually in a language not easily understood by everyone in the organization. Thus, they are amenable to subjective interpretation. This is an issue well recognized in the literature, Redmill [3] addresses it in the context of IEC61508 standard, Feldt et. al [4] discuss it regarding standards used in the space industry and most recently Sannier et. al [5] find the same problem in the nuclear energy industry. There is a need to have a common and formal interpretation of the requirements of a standard on which certification can be based.

Specializing standards to industrial contexts. A standard may need to be adapted to its context of use. It is common to have a generic standard that captures the common requirements across different sectors of industry and then derive sector-specific standards to capture the differences. We call this practice *specialization*. IEC61508 is one such standard that has been adapted to number of different sectors. In the process industry, this standard is adapted as IEC61511 [6], in railways as EN 50128 [7], in the petroleum industry as OLF070 [8], and in the automotive industry as the forthcoming ISO 26262 [9].

To effectively use derived standards, it is important to know which requirements of the generic standard map on to the sector-specific standard. This specification of the relationship between two standards can also be necessary between two standards within the same industry sector. Sometimes standards within a sector evolve, leading to different systems being specified to different versions of the same standard. In this case we again have a parent standard and another that is derived from it, and we still have the issue of systematically specifying the relationship between the two. Feldt et. al. [4] cite the lack of agreed-upon relationships between generic and derived standards as one of the main reasons behind certification delays within the space industry. Whatever the case, there has been little work to date on systematizing the specification of the relationship between generic and derived standards. Furthermore, Nordland [10] notes the lack of a well-formulated process for showing that a derived standard is consistent with a generic one. This too is directly attributable to the lack of precise and explicitly-defined relationships between the standards.

Aligning Standards to organizational practices. When a standard is being used within an organization it will need to be aligned to the practices of the organization. In this manner, the organization can check which of its existing practices comply with the standard and which new practices need to be introduced and tailored. Thus, there is a need to assist system suppliers in relating the concepts of their application domain to the evidence requirements of the applicable standards. This observation is based on the fact that the majority of the evidence artifacts that the suppliers create and manage are based on the concepts for the application domain, as opposed to the concepts of the certification standards. The certification body also needs to interpret the standard in the context of the application domain in order to understand how the evidence relates to the standard before it can check whether sufficient evidence exists to satisfy all the requirements of the standard. This highlights the need for a systematic procedure for creating the necessary evidence and presenting it in a form that will allow the certification body to assess it in terms of both the application domain and the relevant standard.

Planning for certification. Inherent in the three challenges above is the need to ensure that the supplier and the certifier are both using the same interpretation of the standard and that both have an upfront agreement concerning the evidence artifacts that will be created during the system development. If no such agreement exists, then it is possible that the supplier may create evidence artifacts that do not match the certifiers' interpretation of the standard, or the supplier may be missing certain artifacts that the certifier deems necessary. This mismatch can be a costly affair for the supplier who will need to remedy the situation after the system has already been developed. Thus, there needs to be a systematic procedure for ensuring an upfront agreement regarding the specifics of the evidence artifacts.

Managing safety evidence electronically. The final form in which the evidence is presented for certification needs to be highly structured in order to ensure that it is readable and assessable. In general, there is a large amount of evidence that is gathered and all of it needs to be structured such that each piece of evidence and how it relates to other artifacts is clear to the certifier. Traditionally, this has been very difficult to achieve via the paper-based documents that form the basis of the certification evidence. Thus, there is a case for managing this evidence electronically [11] in order to

ease navigation of the information and to allow for diversity of presentation, delivery and re-use.

Promoting re-use. The type of systems that are usually certified are characterized as belonging to product families that have many variants of a base system. Thus any proposed solution for managing certification evidence should take advantage of the re-use that is possible in these types of systems to create a systematic and cost-effective solution.

Certifying system to multiple safety standards. Control systems are often subject to certification based on multiple standards. This may occur due to the use of the system in diverse geographical locations or merely due to the diversity of the components that make up the system. The different standards that may be relevant can often have overlapping requirements and thus there is a need to effectively manage both the distinctions and the overlaps in a systematic manner.

In the remainder of the paper, we will discuss our vision for tackling the above challenges and subsequently some concrete steps we have taken to realize the vision.

III. Vision and Foundations

Having identified the challenges faced by our industry partners during certification we found there were a number of goals that any potential solution would need to fulfill:

1) Provide ways of extracting a common understanding of the requirements presented in a textual certification standard.
   a) Extract the most important concepts.
   b) Extract any inherent relationships amongst these concepts.
   c) Capture this information in a structured and systematic way such that it is can be amenable to specialization in different contexts.
2) Capture all requisite information electronically.
3) Provide some guidance for collecting safety certification information in a precise and structured manner.

Given these goals, we need a means to deals with different levels of abstraction in the information that needs to be represented: going from generic standards to specialized standards, from product family to a specific variant of a system and a way to explicitly define the relationships between the two. If we combine this with the need to structure the information systematically and electronically, we can come to the conclusion that the use of models would be an ideal way to cover all the goals.

Briefly, our position is that models, and not documents, should serve as the main sources of development information - documents, when needed, should be generated from models. For the purpose of safety certification, models are beneficial in many important respects. Most notably: (1) Models can be employed to clarify the expectations of safety standards and recommended practices, and develop concrete guidelines for system suppliers; (2) Models expressed in

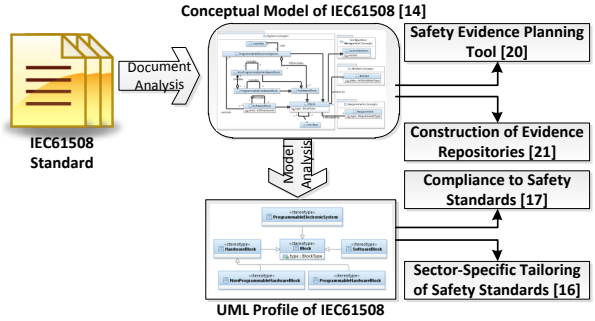

Figure 1. Our current work using MDE techniques

standard notations avoid the ambiguity and redundancy problems associated with text-based documentation; (3) Models provide an ideal vehicle for preserving traceability and the chain of evidence between hazards, requirements, design elements, implementation, and test cases; (4) Models can represent different levels of abstraction and an explicit mapping between the different levels; (5) Models present opportunities for partial or full automation of many laborious safety analysis tasks (e.g., impact analysis, completeness and consistency checking, etc).

We thus maintain that model-driven engineering techniques can be leveraged to create formalized interpretations of standards, and can serve as a primary vehicle for tackling the challenges presented in Section II. Specifically, we have chosen UML [12] as the modelling language of choice as it is standardized and has a well-defined syntax and semantics that will give a degree of formalization to the interpretation of the standard. We use UML profiles for tailoring standards compliance evidence according to domain-specific needs. Additionally, constraints can be defined in a UML profile by using the Object Constraint Language (OCL) [13] to ensure the inclusion of compliance information in the models to which a profile is applied. We use this mechanism to provide guidance for collecting safety certification evidence. The models allow for creating electronically managed evidence that can be queried and transformed to whatever form is required by the certification body. Finally, the use of models will allow for a higher degree of re-use as we will show in Section IV.

IV. Current Work

The basis of our work is an explicit interpretation of textual standards. We need to ground our approach on a particular standard for illustration. We have chosen IEC61508 which is the most comprehensive safety standard we know of. It is a de-jour standard for many systems. It is generic and applies to multiple domains (e.g., railways, maritime, energy, process industries). Given the significance of IEC61508, we believe that the successful application of our approach to it, is a good indication of the generalizability of our work. In Figure 1, we show the areas of safety certification that we have tackled.

A. Creating common interpretations.

In order to create an explicit interpretation of the IEC61508 standard that promotes a common understanding of the standard, we have created a conceptual model that formalizes the evidence requirements of the standard [14]. The process of creating a conceptual model of the evidence requirements of a given standard involves a careful analysis of the text of the standard. It requires skills in modelling, systems development and knowledge of the process of certification beyond merely reading the standard. To some extent, this can be viewed as a process of qualitative data analysis, where the data is the text of the standard and it is being analyzed to identify from it, all the salient concepts and their relationships.

This retrieved information from the text is used to identify all the important concepts in the standard and as a means of explicitly showing the relationships that exist between the salient concepts. Lewis [15] expresses the need for presenting certification information as an information model. He highlights the need for creating a formal structure and the need to present the relationships that exist between atomic items of information, resulting in a *web of information* that supports certification.

In order to represent these relationships as required by a particular standard, we create a conceptual model that allows us to represent the main factors that need to be considered for certification and the relationships amongst them [14]. The fundamental elements that we need to represent are 1) concepts, 2) attributes, 3) inter-concept relationships and 4) constraints. Additionally, as standards can be quite large, it is useful to have a means to divide the concepts into useful groupings. The conceptual model has an analogous glossary to provide descriptions of the identified concepts and their relationships. The UML [12] class diagram notation can be used to conveniently express the conceptual model. Concepts are represented as classes and concept attributes as class attributes. Relationships are represented by associations. Generalization associations are used to derive more specific concepts from abstract ones. When an attribute assumes a value from a predefined set of possible values, we use enumerations. Finally, we use the package notation to make groupings of concepts and thus better manage the model complexity.

At the most basic level, the conceptual model we have developed helps improve understanding and communication of the IEC61508 standard. Interpreting a standard like IEC61508 is a difficult task for system suppliers, and inevitably their interpretation may vary, sometimes significantly, from that of the certifier. Suppliers are frequently not clear as to what documents and information, and at what level of detail, they are expected to provide in support of safety. Furthermore, they are unsure of how these documents should be linked to hazards, requirements, activities, and so on. A concise but precise graphical representation of the core concepts in the standard such as the one we have developed is a valuable and appealing aid for understanding and using the standard. In particular, the representation can be used by the certifiers to convey their expectations and to clarify the information requirements for demonstrating compliance. Towards this end, we have used the conceptual model as the basis for creating a UML profile of the IEC61508 standard. This profile is used to *specialize* generic evidence requirements according to sector-specific needs (e.g., in the railways, avionics, and maritime and energy sectors) and to support compliance to safety standards.

B. Specializing standards to industrial contexts.

For sector-specific tailoring [16], we capture the relationship between the evidence requirements of a generic standard and those of a sector-specific derivation. Briefly, our approach works by building conceptual models for the evidence requirements of both the generic and sector-specific standards. The conceptual model of the generic standard is turned into a UML profile, and this profile is used for stereotyping the elements in the conceptual model of the sector-specific standard. We use OCL constraints attached to the stereotypes of the profile for validating the sector-specific conceptual model to ensure that it is consistent with the generic standard. Our approach offers two main advantages: First, it provides a systematic and explicit way to keep track of the relationships between a generic and a derived standard in terms of their evidence requirements. The concepts of the generic standard can be incorporated into the sector-specific standard whilst making a clear distinction between the two. And second, it enables the definition of consistency constraints to ensure that evidence requirements are being specialized properly in the derived standard. The consistency constraints can be automatically verified and used for providing guidance to the users about how to resolve any inconsistencies.

C. Aligning Standards to organizational practices

In order to support compliance to safety standards we need to establish a relationship between the concepts in the standard to the concepts in the application domain [17]. This is done by creating a domain model containing concepts that represent the physical and abstract components of a *family* (class) of systems in a particular application area (e.g., subsea control systems), the environment in which this family of systems function, and the key artifacts built throughout development. An example of a product family [18] is a Fire and Gas Protection system that will consist of sensors being used to detect fire or combustible gas, a controller that does processing based upon the input from the sensors and then deploys certain actuators such as sprinklers or dampers. This is a generic description of a class of systems – each variant of the system will have very specific types of sensors and

actuators with specific actions that should take place upon the detection of fire or gas.

Following the norm in MDE, we assume domain models are represented as UML class diagrams [19]. This domain model is then *elaborated* using the UML profile of the relevant standard, which has been augmented with constraints to aid system suppliers in systematically relating the concepts in the standard to the concepts in the application domain. During elaboration the stereotypes of the profile are applied to the appropriate domain model elements, and the domain model is refined so that it satisfies the OCL constraints of the stereotypes. These refinements could include the addition of new domain model elements or making changes to the existing ones (e.g., adding new attributes, revising multiplicities). Elaboration makes it possible to establish a concrete link between the evidence requirements of a given standard and a domain model. Finally, for certifying a specific system (variant) of a product family, an instantiation of the UML class diagram representing the elaborated domain model is created. In other words, an object diagram of the domain model is built to represent the specific properties of a system variant. This will represent the safety evidence to be collected to demonstrate compliance of a specific variant of the system.

D. Planning for certification.

The conceptual model is also used in planning for certification. Once there is an agreed upon interpretation of the standard, the certifier and supplier can use this to create an upfront plan as to what evidence the supplier will create and present for the certification process. We have created EvidenceAgreement [20], a web-based safety evidence planning tool for assisting suppliers and certifiers in developing an agreement about the evidence necessary to demonstrate compliance to a safety standard. The agreement process revolves around the notion of a questionnaire: the questions are regarding what evidence to collect and the answers are the agreed upon specifics of the evidence to collect. The tool takes the conceptual model as input and assists system suppliers and the certifiers in reaching a documented and consistent agreement about the safety evidence that needs to be collected.

E. Managing safety evidence electronically.

The conceptual model can be used directly to keep track of safety information by instantiating the conceptual model in a UML modeling environment. However if the suppliers do not wish to work directly with a modelling tool, e.g., due to scalability reasons, then the conceptual model can be the basis of an automatically constructed evidence repository. We have created such a repository infrastructure, named CRESCO [21]. CRESCO is a flexible tool infrastructure for creating repositories to store, query, and manipulate standards compliance evidence. Additionally, CRESCO generates a web-based user interface for interacting with these repositories. Our work was prompted by an observed need that little infrastructure support has been developed to date to support management of safety evidence based on a specific standard. This issue has also been noted in the literature as an important gap in the safety certification process [15], [3]. CRESCO is a general tool and can be used in conjunction with different standards.

F. Promoting re-use

Within all this work, we have always been conscious of creating solutions that can build upon each other and incorporate a lot of re-use. In all this work, the creation of the conceptual model and the corresponding UML profile needs to be created once per standard, the domain model needs to be created once per product family and the instantiation is performed for each variant that is subject to certification. We have also chosen to illustrate our approach by working with IEC61508. Given the prolific use of IEC61508 and that our profile closely reflects its concepts makes our work reusable - the profile and its OCL constraints can be reused for all the domains that use the standard directly as well as those using its specializations. These collectively cover a significant fraction of the safety certification activities in the current practice.

Regarding the challenges of using textual standards for expressing certification requirements, we have created potential solutions and demonstrated their applicability for the first six challenges expressed in Section II. We believe that the creation of UML profiles of the certification standards will also help in the final challenge of certification to multiple standards. We are now in the process of working on this issue. We discuss this and other future work directions in Section V.

V. Future Research Agenda

At present, we are working on extending the process presented in [17] for the certification of a single system to multiple standards and how to deal with overlapping standard requirements. Each standard will represent different concerns, however there is likely to be some overlap in the concepts of standards that are for certifying systems in the same domain. If we choose to express each standard as a UML profile that is applied to a domain model of the system to be certified then we need to ensure that a consistent vocabulary is used such that the same terms are not used to express different concepts or the same concept is not expressed multiple times with different vocabulary. Hence, to successfully employ multiple UML profiles we will need to look for formal ways to represent the concepts in the standards such that their underlying semantics can be captured and reconciled in some automatic way.

Our current work has focused on creating models, specifically from a certification point of view. This means that we do not expect that the supplier is using model-driven

development for the actual system development. The models we create are for certification, irrespective of which development methodology is used. However, if a model-driven development approach is used for system development as well, then it should be possible to leverage those models for the purpose of certification. We would like to investigate how the conceptual model and profile of a certification standard can be used along with development models to improve the process of certification. This may have an impact on how the system is designed as the developers need to be more aware of certification requirements.

A common thread when presenting the evidence for certification is to link it to corresponding argumentation. The norm is to have safety claims and argumentation backed by evidence of how these claims are fulfilled. Recently, the OMG has put forward a proposal, called the Software Assurance Evidence Metamodel (SAEM) [22], for managing safety assurance evidence. The SAEM is a standard-independent metamodel and directed towards linking the certification evidence to safety claims and the evaluation of these claims subject to the evidence. The approach that we propose uses a UML profile for characterizing the evidence of a specific standard. To perform the same task, the SAEM model will still require a definition of the specific evidence needed by a particular standard (perhaps based on a conceptual model as we have proposed). On the other hand, a profile of the SAEM could be incorporated into our approach and cover both the evidence requirements for compliance to a particular standard, as well as the evaluation of the evidence to ensure that it is sufficient to substantiate the safety claims. Together this could be a means to further the field of model-based certification.

VI. Conclusion

In this paper, we have discussed the challenges that are faced by system suppliers and certifier when having to certify systems to safety standards. These challenges are based on our experience in working in and with industry. System supplier are required to prepare for certification based on the relevant industry standards that are textually expressed and are subjectively interpreted. The suppliers run the risk of not collecting the requisite information during the development of the system and having to do so after the fact, leading to large cost overruns and delays in deployment of systems. On the other hand, certifiers may receive a large collection of documents from the supplier with the hope that the certifier will find the required safety information (based on *their* interpretation of the standard). This results in the certifier having to invest a significant amount of time and effort sifting through the provided documents, and in many cases not finding what they were looking for. What is required is a structured and systematic procedure for certification where both parties can proceed in a timely manner, being aware of what information to collect and how to navigate easily through it.

We propose that models can be used to tackle the issues that we have identified. They can be used to clarify the expectations of standards and present opportunities for automation of the certification process. To this end, we gave an overview of our current work to show the potential of using model-driven engineering techniques for safety certification. We have illustrated our work using IEC61508, one of the most commonly used standards in industry in order to show the applicability of our approach.

References

[1] "Defence standard 00-56, safety management requirements for defence systems (DS 00-56)." 2004.

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

[3] F. Redmill, "Installing IEC 61508 and supporting its users – nine necessities." in *5th Australian Workshop on Safety Critical Systems and Software*, 2000.

[4] R. Feldt, R. Torkar, E. Ahmad, and B. Raza, "Challenges with software verification and validation activities in the space industry," in *ICST'10*, 2010, pp. 225–234.

[5] N. Sannier, B. Baudry, and T. Nguyen, "Formalizing standards and regulations variability in longlife projects. a challenge for model-driven engineering." in *MoDRE workshop*, 2011, pp. 225–234.

[6] "Functional safety - safety instrumented systems for the process industry sector (IEC 61511)." 2003.

[7] "EN50128 - Railway Applications - software for railway control and protection systems," 1999.

[8] "Application of IEC61508 and IEC61511 in the Norwegian Petroleum Industry," 2004.

[9] "ISO26262 Road vehicles – Functional safety," 2009, ISO draft standard.

[10] O. Nordland, "A critical look at the cenelec railway application standards," http://home.c2i.net/odd_nordland/~SINTEF/tekster/A_critical_look_at_rail_standards.htm, 2003.

[11] T. Cockram and B. Lockwood, "Electronic safety cases: Challenges and opportunities," in *Current Issues in Safety-Critical Systems, in proceedings of Safety Critical Systems Symposium*. Springer, 2003.

[12] "UML 2.0 Superstructure Specification," August 2005.

[13] "OMG Object Constraint Language," http://www.omg.org/spec/OCL/2.0/, OMG, 2006.

[14] R. K. Panesar-Walawege, M. Sabetzadeh, L. Briand, and T. Coq, "Characterizing the chain of evidence for software safety cases: A conceptual model based on the IEC 61508 standard," in *ICST*, 2010.

[15] R. Lewis, "Safety case development as an information modelling problem," in *Safety-Critical Systems: Problems, Process and Practice*. Springer, 2009, pp. 183–193.

[16] R. K. Panesar-Walawege, M. Sabetzadeh, and L. Briand, "Using UML profiles for sector-specific tailoring of safety evidence information," in *ER2011*, 2011, to appear.

[17] ——, "A model-driven engineering approach to support the verification of compliance to safety standards," in *ISSRE2011*, 2011, to appear.

[18] K. Pohl, G. Böckle, and F. van der Linden, *Software product line engineering - foundations, principles, and techniques*. Springer, 2005.

[19] C. Larman, *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development (3rd Edition)*. Prentice Hall, Oct. 2004.

[20] D. Falessi, L. Briand, M. Sabetzadeh, E. Turella, T. Coq, and R. K. Panesar-Walawege, "Planning for safety evidence collection: A tool-supported approach based on modeling of standards compliance information," *IEEE Software*, vol. 99, no. PrePrints, 2011.

[21] R. K. Panesar-Walawege, T. S. Knutsen, M. Sabetzadeh, and L. Briand, "Cresco: Construction of evidence repositories for managing standards compliance," in *ER2011*, 2011, to appear.

[22] "Software Assurance Evidence Metamodel (SAEM)," http://www.omg.org/spec/SAEM/, OMG, 2010.