SafetyMet: A Metamodel for Safety Standards

Jose Luis de la Vara and Rajwinder Kaur Panesar-Walawege

Certus Centre for Software V&V, Simula Research Laboratory
P.O.Box 134, 1325 Lysaker, Norway
{jdelavara, rpanesar}@simula.no

Abstract. In domains such as automotive, avionics, and railway, critical systems must comply with safety standards to allow their operation in a given context. Safety compliance can be an extremely demanding activity as practitioners have to show fulfilment of the safety criteria specified in the standards and thus that a system can be deemed safe. This is usually both costly and time consuming, and becomes even more challenging when, for instance, a system changes or aims to be reused in another project or domain. This paper presents SafetyMet, a metamodel for safety standards targeted at facilitating safety compliance. The metamodel consists of entities and relationships that abstract concepts common to different safety standards from different domains. Its use can help practitioners to show how they have followed the recommendations of a standard, and particularly in evolutionary or cross-domain scenarios. We discuss the benefits of the use of the metamodel, its limitations, and open issues in order to clearly present the aspects of safety compliance that are facilitated and those that are not addressed.

Keywords: safety standard, metamodel, safety compliance, safety assurance, safety certification, SafetyMet, OPENCOSS.

1 Introduction

Safety-critical systems are those whose failure can cause injury or death to people or harm to the environment in which they operate. These systems are subject to rigorous safety assurance and assessment processes, which are usually based on some safety standards upon which the system is to be certified [34]. System suppliers have to show that a system (and/or its lifecycle) has fulfilled the requirements of the safety standard so that the system can be deemed safe for operation in a given context.

Examples of safety standards include IEC61508 [24] for systems that combine electrical, electronic, and programmable electronic systems, DO-178C [45] for the avionics domain, the CENELEC standards (e.g., EN50128 [8]) for the railway domain, and ISO26262 [26] for the automotive industry. Companies can also adopt recommended practices (e.g., [14]) or defined company-specific practices as a part of their own, internal safety procedures.

Demonstration of safety compliance is usually costly and time-consuming [16], and can be very challenging [33, 34]. Firstly, system suppliers have to collect evidence of compliance such as hazard specifications, test results, and activity records. This can be hindered because of difficulties in understanding safety

standards, in determining the evidence, or in gaining confidence in evidence adequacy. Secondly, practitioners usually have to manage large quantities of evidence and structure it to show how a system complies with a standard. If the evidence is not structured properly, its sheer volume and complexity can jeopardize safety certification.

Demonstration of compliance with safety standards becomes even more difficult when a system evolves [13]. For example, recertification of a system requires a completely new set of evidence since changes to the system will have invalidated previously existing evidence. There can be re-use of evidence only if it is possible to accurately assess how the changes have impacted the existing evidence. Consequently, industry needs approaches that enable evidence reuse and support evidence change impact analysis.

If aiming to reuse an already-compliant system in another domain, practitioners have to demonstrate compliance with other standards. This is currently an important concern in industry [4]. Although correspondence between regulations has been addressed in other fields (e.g., [19]), the situation in safety compliance is more complex. No perfect match usually exists between safety standards, and system suppliers usually have their own interpretations and thus usage of a standard. As a result, compliance with a new standard is never straightforward, and means to facilitate this activity are necessary.

All the challenges above can lead to certification risks [3]. In other words, a system supplier might not be able to develop a safe system, show system safety, or make a third party gain confidence in system safety.

To tackle these issues we propose the use of model-based technologies. Several proponents of these technologies have argued their suitability for mitigating the complexity of and thus facilitating safety compliance (e.g., [41]). However, the current model-based approaches for safety compliance have been targeted at specific standards or domains, thus they do not provide generic solutions that can be applied in contexts of cross-domain use or where multiple standards are required in the same domain.

This paper aims to fill this gap by presenting SafetyMet, a metamodel for safety standards. This metamodel aims to support practitioners when having to deal with safety compliance, especially in situations in which a system evolves or must comply with several standards. The metamodel is part of our contribution to OPENCOSS (`http://www.opencoss-project.eu/`), a European research project whose goal is to devise a common certification framework for the automotive, avionics, and railway domains. The metamodel has been developed in close collaboration with industry.

SafetyMet is a generic metamodel that includes concepts and relationships common to different safety standards and to different domains. It addresses safety compliance from several perspectives, explicitly dealing with information related to the process, data, and objectives that are necessary to demonstrate compliance. The metamodel is a part of an overall approach for model-based safety compliance that encompasses both standard-specific and project-specific aspects.

Apart from supporting demonstration of safety compliance in general, use of the metamodel can help practitioners to structure and reuse evidence, assess its adequacy, and deal with evidence traceability and change. Nevertheless, some compliance needs such as human aspects are out of the scope of SafetyMet and its application.

The rest of the paper is organised as follows. Section 2 introduces the background of the paper. Section 3 presents SafetyMet, whereas Section 4 discusses its benefits and limitations. Finally, Section 5 summarises our conclusions and future work.

2 Background

This section introduces the OPENCOSS project and reviews related work.

2.1 OPENCOSS

OPENCOSS is a large-scale FP7 European project that aims to (1) devise a common certification framework that spans different vertical markets for railway, avionics, and automotive industries, and (2) establish an open-source safety certification infrastructure. The ultimate goal of the project is to bring about substantial reductions in recurring safety certification costs and at the same time reduce certification risks through the introduction of more systematic safety assurance practices. The project deals with: (1) creation of a common certification conceptual framework; (2) compositional certification; (3) evolutionary chain of evidence; (4) transparent certification process, and; (5) compliance-aware development process.

SafetyMet can be regarded as a part of the common certification framework. More details about the framework and the role and usage of SafetyMet are presented below. It must also be mentioned that this paper presents our current vision of the framework, thus it might not reflect the final vision of the entire OPENCOSS consortium.

2.2 Related Work

Related work can be divided into three main streams: models for compliance or assurance in general, models for safety assurance, and models for safety compliance. When mentioning models in this section, we refer to both models and metamodels, understood as sets of concepts and the relationships between them, independently of the graphical or textual languages used for their representation.

Models for compliance or assurance in general have been proposed in order to facilitate demonstration of fulfilment or alignment with different requirements or criteria. This topic has received great attention in the requirements engineering and business process management communities. Systematic reviews on compliance from a requirements engineering and business process perspective can be found in [17, 48].

The requirements engineering community has provided insights into issues such as regulatory compliance in practice [36], correspondence between regulations [19], regulation formalization [47], argumentation [25], and component selection [35]. Examples of aspects related to business process compliance that have been addressed are compliance patterns [43], compliance management [1], and compliance with reference models [28], context [12], contracts [20], and control objectives [46].

Most of the models proposed (e.g., [15, 18]) are generic. An especially relevant example is the just published first version of SACM (Structure Assurance Case

Metamodel; [39]). It is an OMG specification and includes an argumentation and an evidence metamodel. Other models have been developed for compliance with non-safety-specific standards (e.g., CMMI [32]).

Apart from not targeting system evolution, the main weaknesses of these models is that they do not support safety standards-specific needs such as having to show alignment with the many varied criteria of the standards (activities, artefacts, techniques, requirements, criticality levels, etc.).

Models for safety assurance can be regarded as a refinement of the models presented above. They aim at supporting analysis of safety-related system aspects such as traceability between requirements and design [37], process assurance [23], or dependability [5]. Broader traceability models for safety-critical systems can also be found in the literature (e.g., [9, 27, 52]). In the context of graphical modelling of safety argumentation, metamodels for GSN (Goal Structuring Notation) (e.g., [11]) and a model of evidence for safety cases [51] have been proposed.

In general, these models can be regarded as closer to the domain of project-specific aspects than to the domain of safety standards. For example, they do not include means to explicitly model and analyse the requirements of a safety standard and thus to show how they have been fulfilled by means of the execution of some activity or the creation of some artefact.

During the past few years, several **models for safety compliance** have been presented in order to support demonstration of fulfilment of the criteria of a safety standard. This has been usually presented in the scope of some specific standard. Examples of safety standards for which models have been proposed include ISO26262 [29], IEC61508 [30, 42], and DO-178B [54]. A model that combines ISO26262 and SPICE can be found in [2]. In some cases, these models have focused in specific parts of the standards such as quality-related aspects [31], faults [49], and testing [50]. These models are not generic but standard-specific, thus they cannot be directly applied when, for instance, aiming at demonstrating compliance with another standard. These models can be regarded as SafetyMet instances.

Other related works are those that have proposed models for impact analysis (e.g., [7]) or for system evolution (e.g., [53]). However, they have not explicitly addressed how these aspects are related to safety compliance.

In summary, since the models reviewed have purposes different to SafetyMet, they do not fit its needs. In this sense, SafetyMet aims to extend the state art by providing a metamodel that (1) supports safety compliance in a generic way that can be adapted to different regulatory contexts, and (2) facilitates evidence change management and cross-standard/domain compliance. Consequently, the metamodel aims to generalize and widen the scope of past proposals (e.g., [42]).

3 Metamodel for Safety Standards

This section introduces SafetyMet, the metamodel that we propose for safety compliance. The metamodel includes a number of key relationships that exist between the different pieces of information that are managed for safety compliance. Showing these relationships is a prerequisite to demonstrating compliance [40].

For the purpose of compliance, there are two main sources of information: the standard to be complied with and the product for which compliance is sought. Related to the product we have information regarding the process used in its construction, the evidence that contributes to gaining confidence in system safety, and the argumentation to justify system safety. Argumentation can be presented implicitly (e.g., [42]) or explicitly (e.g., [21]). These three aspects must match the process, data, and objectives prescribed by the safety standard. In addition, it is necessary to understand the vocabulary (i.e., terms) used in the standard and usually map it to the vocabulary that exists in the domain in which the product is being developed.

Based on these relationships and the need to abstract the relevant information from the vast amount of data that is created during system lifecycle, we advocate for the creation of models that represent both the compliance and product-specific information. The models must also be structured in a specific manner in order to perform useful analyses with them. To this end, we propose the use of metamodels to which all the models must conform [6].

The following subsections present more details about the context and purpose of SafetyMet, its concepts and relationships, and how it has been validated.

3.1 Scope and Purpose

In general, safety compliance is not based on just one standard. Minimally there are at least the safety standard mandated by a particular industry and then the internal working procedures of the specific system supplier. These procedures are a mix of internal best practices and geared towards aiding compliance to the applicable safety standard. In other cases a system is to be certified to multiple standards used in different parts of the world, and finally there may be the case of using components (or systems) that have been certified in one domain in another. Hence a component certified to one standard may have to be re-certified to another. There exist also other specific needs when a system evolves [13], such as managing evidence change impact. We propose SafetyMet in order to aid compliance in these various scenarios.

The metamodel captures the abstract notions that can be used to describe the information that needs to be collected to show compliance to safety standards and manage system change. Specifically, SafetyMet corresponds to a unified metamodel that will aid in the creation of models for compliance.

SafetyMet is an element of a set of metamodels and corresponds to a metamodel for safety standards (Fig. 1). The models resulting from these metamodels will capture the information necessary for showing compliance in specific projects (safety compliance models). The rationale for developing such models is to create a consistent interpretation of the standard being used and link this to the product being certified. The need for a consistent interpretation stems from the fact that safety standards are textual documents amenable to subjective interpretation. By creating a model we do not avoid subjectivity but aid in a shared, consistent interpretation.

Regarding the actual product being certified, the metamodels will also include the concepts and relationships necessary for modelling and managing project-specific information. This information needs to be recorded regardless of the safety standards being followed (e.g., confidence in evidence). There are metamodels for modelling:

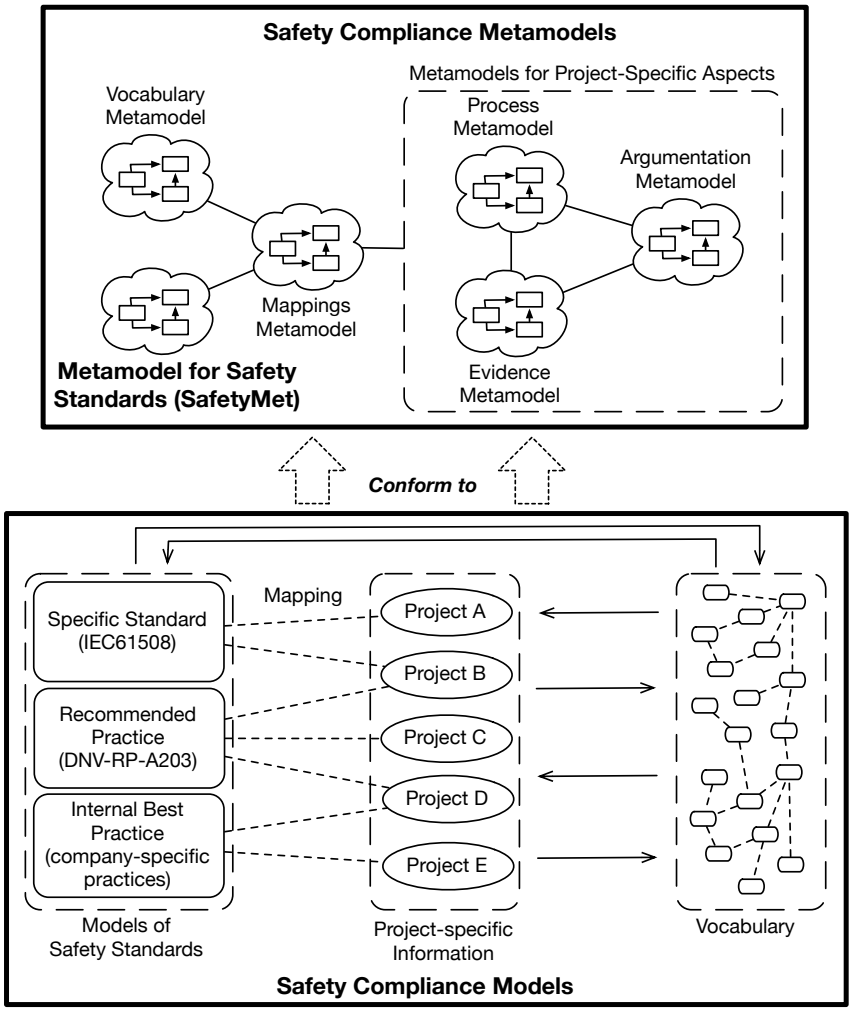

Fig. 1. Overall approach for safety compliance

- The actual process used to create a product, which is important as assurance artefacts are produced as a result of process activities and it must be shown that the activities materialise the process mandated by safety standards;
- The argumentation that will be used to justify key safety-related decisions taken during the project and must be in line with the objectives of safety standards, and;
- The specific information that needs to be kept about the concrete artefacts that will be used as evidence of compliance and that thus must materialise those types of artefacts prescribed by safety standards.

Two other metamodels are proposed, which may be considered the 'glue' that connects the others. The vocabulary metamodel is a means to define and record the terms and concepts used to characterize reusable assets such as evidence, argumentation, and process assets. When multiple standards are used for compliance

purposes (e.g., certification of a system for another domain), mappings will be created between the vocabulary terms of one standard and those of another. The mappings will then allow engineers to use this information in order to make informed decisions about the appropriateness and implications of reusing a given asset that was created for compliance to a particular safety standard in the context of another standard.

Finally, there is a metamodel for mappings. We have already mentioned mappings in the context of the vocabulary used in one standard to the vocabulary used in another standard. Another use of mappings will be for associating the assurance information gathered during a project to the safety criteria of a standard. This is a means of showing compliance to the standard. We discuss the mappings further when describing the actual models created using the metamodels proposed. Mappings between models of safety standards can also exist.

It must be noted that although we refer to them as a set of metamodels, a single metamodel aimed at supporting several aspects of safety compliance will be created. Relationships will exist between the concepts of the metamodels, such as the evidence (evidence metamodel) used for argumentation (argumentation metamodel) or the mapping (mappings metamodels) of project artefacts (evidence metamodel) to the types of artefacts of some safety standards (metamodel for safety standards).

The metamodels will be used to create the actual models that will be used for showing compliance. This is depicted in the bottom part of Fig. 1. The metamodel for safety standards is used to create the models of the relevant safety standards and the project-specific models are created using the process, argumentation, and evidence metamodels. As these models are being created, the vocabulary metamodel is used to capture the relevant vocabulary terms, such as the vocabulary used in the standards as well as that used in the project.

Mappings from the project assets to the assets mandated by the standard need to be created in order to demonstrate compliance. Doing so, we can show clearly how a particular asset created during a project complies with a particular standard. When a project needs to comply with multiple standards, then the vocabulary can aid in mapping the assurance assets created in the project for compliance with one standard to those required by another standard. In this case not all assets may be reusable, some new assets may need to be created, and some assets might have to be modified [13].

This overall approach for safety compliance aims to enable reuse of certification assets. As further discussed below, the models of safety standards and the vocabulary will be used from one project to another and will be valuable assurance assets in a company. The use of mapping provides a clear traceable link between the assets of a project and the standard to be complied with. This is a link very difficult to show and maintain using textual documents but can be more easily managed using models.

3.2 SafetyMet

The metamodel is shown in Fig. 2 in the form of an Ecore diagram [22]. We have modelled it this way in order to quickly generate model editors for validation purposes. The metaclasses of which SafetyMet consists are defined as follows.

- *Safety Standard* is used to hold information about the safety regulation(s) modelled.

- *Criticality Level* corresponds to the categories of criticality that a safety standard defines and that indicate the relative level of risk reduction being provided (e.g., *SIL 1, 2, 3,* and *4* in IEC61508).
- *Applicability Level* represents the categories of applicability that a safety standard defines (e.g., a given technique is *mandated* in EN50128).
- *Activity Type* is targeted at modelling the activities (i.e., the units of behaviour [42]) that a safety standard defines for system lifecycle and must be executed to demonstrate compliance. An activity type can be decomposed in others.
- *Role* represents the types of agents [42] that execute activity types, either explicitly defined in a safety standard or required to be defined by the supplier.
- *Artefact Type* represents types of units of data that a safety standard prescribes to be created and maintained during system lifecycle. Artefact types are materialised in projects by means of concrete artefacts [38]. This means that these artefacts have the same or a similar structure (syntax) and/or purpose (semantics) [9]. Artefact types can be required or produced by activity types, and some can determine the criticality level in a project (e.g., risks [14]).
- *Artefact Type Property* is used to model the characteristics [38] of an artefact type.
- *Artefact Relationship Type* aims to model the existence of a relationship between two artefact types (source and target of the artefact type relationship) [38, 44]. An artefact relationship type is materialised by relating two artefacts of a project, and characterizes those artefact relationships that have the same or similar structure (syntax) and/or purpose (semantics) [9]. Such a relationship can be recorded in an artefact if the relationship itself is used as evidence (e.g., DO-178C explicitly requests the provision of traceability information). An artefact type relationship can be created as a result of executing some activity type.
- *Technique* corresponds to specific ways to create an artefact type and that can be utilised in some activity type. Specific techniques are defined in many standards.
- *Requirement* represents the criteria (e.g., objectives) that a safety standard defines (or prescribes) to comply with it. Requirements are fulfilled by executing activity types, and are the aim of artefact types (i.e., the reason why they are necessary).
- *Requirement Decomposition* corresponds to the contribution of several requirements to the fulfilment of another requirement.
- *Criticality Applicability* represents the assignation, in a safety standard, of an applicability level for a given criticality level to its requirements or techniques.

Two enumerations have also been included, one for specifying how a requirement can be decomposed (*Decomposition Type*) and another for specifying the *Change Effect* of the target of an artefact type relationship on the source.

Although at first sight some relationships might seem redundant (e.g., *Activity Type* utilizes *Technique* and *Artefact Type* results from *Technique*), they all are necessary in order to allow different and alternative ways to model a safety standard. For example, an activity type might produce several artefact types, and several activity types might produce an artefact type. Therefore, it might be necessary to link *Technique* with both *Activity Type* and *Artefact Type* in order to be able to determine what technique is used in a specific activity type to produce a given artefact type.

Further details about the classes, their attributes, their relationships, and their constraints are not provided due to page limitations.

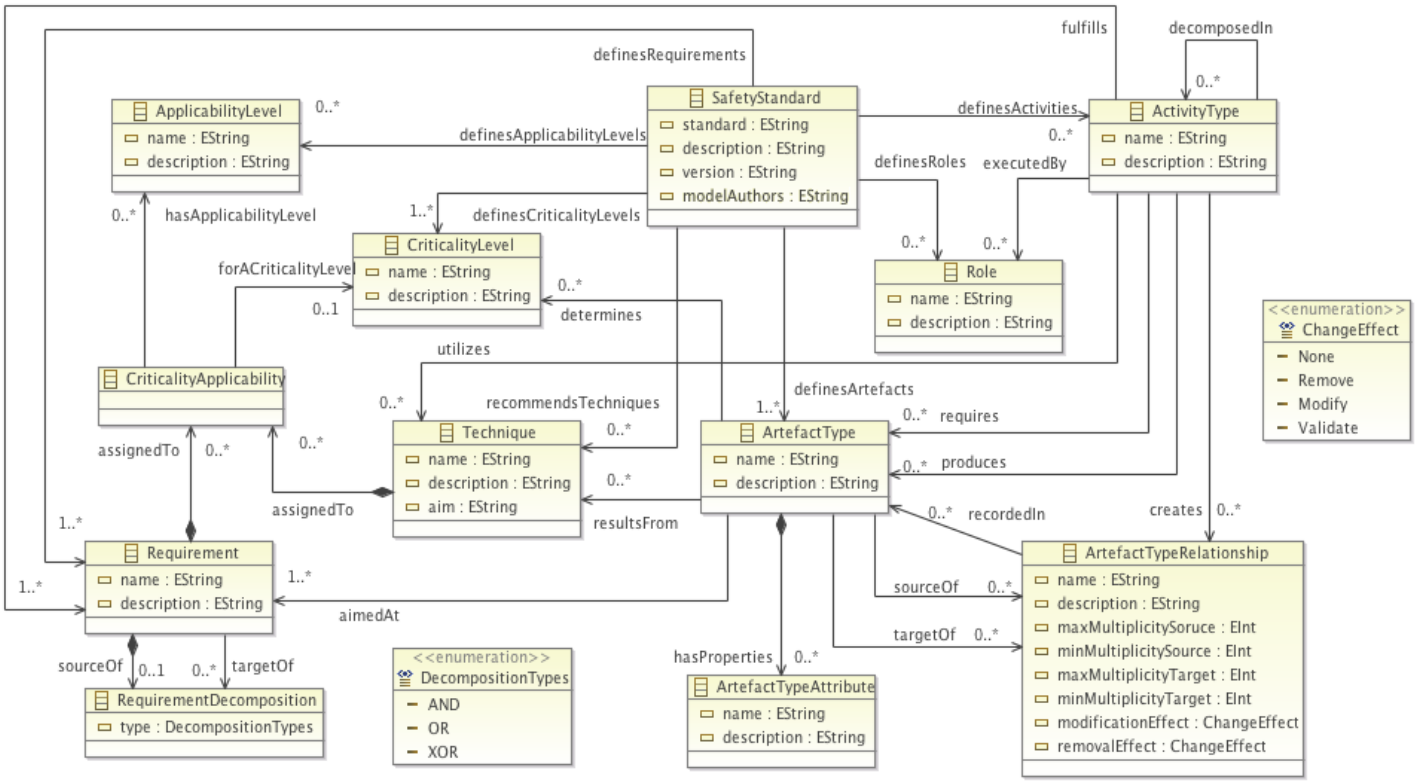

Fig. 2. Metamodel for safety standards

As can be noted, SafetyMet includes concepts related to process (e.g., *Activity Type*), data (e.g., *Artefact Type*), and objectives (e.g., *Requirement*) for safety compliance. In essence, the metamodel is targeted at modelling those elements of a safety standard with which correspondence must be shown in a project in order to demonstrate safety compliance. These elements are also necessary to compare and map safety standards. In this sense, it is very important to know the objectives of activity and artefact types when comparing standards.

SafetyMet also aims to be generic and flexible, in order to allow different ways to model a standard. For example, the metamodel does not assume the existence of a given number of levels (i.e., decompositions) of requirements and activities types, and provides modellers with freedom to determine the granularity of artefact types. Nonetheless, and especially for the latter aspect, we plan to provide guidelines.

Some aspects of SafetyMet to be further studied and developed in the future are:

- Specification of more attributes for the classes
- Further support for change impact analysis by specifying more change effects
- Provision of a set relationships between types of artefacts (i.e., inclusion of classes that specialise *ArtefactTypeRelationship*, as proposed in works such as [44])
- Inclusion of more links between requirements and between activity types

Decisions upon these aspects will be made once the metamodel is further validated.

3.3 Preliminary Validation

We have initially validated SafetyMet by analysing its support for the necessary compliance information of several specific software safety standards and thus by modelling them. More concretely, we have validated SafetyMet with: DO-178C [45] (although not specifically and explicitly targeted at safety, it is used for this purpose [33]); EN50128 [8]; ISO26262 [26] (Part 6), and; IEC61508 [24] (Part 3). This set of standards corresponds to both objective-based and process-based safety standards.

In Table 1 we show examples of how SafetyMet classes correspond to specific information from the standards. More details and examples are not shown due to page limitations. Although all the standards do not include explicit information about some elements (e.g., *Role*), this information is usually required. For other concepts, the standards might not explicitly include such pieces of information, but it can be specified as a result of their interpretation. For example, DO-178C objectives correspond to *Requirement* in SafetyMet, and their analysis can lead to the specification of other requirements that decompose the objectives. We have not included this information in Table 1 to keep it as small as possible.

We have also validated SafetyMet by analysing if it could be used to create the models for safety compliance reviewed in Section 2.2. We have determined that it is possible, despite the fact that no model includes all the information that can be specified with SafetyMet. SafetyMet can be regarded as a metamodel for all these models, addressing modelling of process, data, and objectives for safety compliance.

An instance of SafetyMet must be regarded as an interpretation of how a project can comply with a safety standard and of how evidence traceability and change will be managed. For the latter two aspects, this is the reason why, for instance, Artefact Type Relationship has attributes related to multiplicity and change effect.

Table 1. Examples of SafetyMet elements from several safety standards

	Safety Standard			
SafetyMet Element	**DO-178C**	**EN50128**	**ISO26262**	**IEC61508**
Criticality Level	Software Level A, B, C, D, E	SIL 0,1, 2, 3, 4	ASIL A, B, C, D	SIL 1, 2, 3, 4
Applicability Level	Satisfied, Satisfied With independence	M, HR, R, NR, -	+, ++, o	R, HR, NR, -
Activity Type	Software Development Processes	Component Design	Software Unit Design and Implementation	Software Design and Development
Role	(Specified by the supplier)	Designer	Designer	(Specified by the supplier)
Artefact Type	Input: Software Requirements Data; Output: Design Description	Input: Software Design Specification; Output: Software Component Design Specification	Input: Softw. Architectural Design Specification; Output: Software Unit Design Specification	Input: Softw. Architecture Design Description; Output: Software System Design Specification
Artefact Type Property	Approval Status	Author	Version	Date of Revision
Artefact Type Relationship	Design Description *satisfies* Software Requirements Data	Software Component Design Specification *links to* Software Component Test Specification	Software Unit Design Specification *links to* Software Requirements and *specifies* Software Unit Implementation	Software System Design Specification *derived from* Softw. Architecture Design and Hardware Architecture Design Descriptions
Technique	(Specified by the supplier)	Modelling	Semi-formal notations	Semi-formal methods
Requirement	(A-4.8) Software architecture is compatible with high-level requirements.	(7.4.4.1) For each component, a Software Component Design Specification shall be written, under the responsibility of the Designer, on the basis of the Software Design Specification.	(8.4.3) The specification of the software units shall describe the functional behaviour and the internal design to the level of detail necessary for their implementation.	(7.4.5.3) The software should be produced to achieve modularity, testability, and the capacity for safe modification.
Criticality Applicability	Software Level A, Satisfied with Independence	SIL 2, HR	ASIL D, ++	SIL2, HR

4 Discussion

In this section we discuss the benefits, limitations, and open issues of the application of SafetyMet.

4.1 Application and Benefits of SafetyMet

Several benefits of SafetyMet have been outlined throughout the previous sections, such as the creation of a shared, common, and consistent interpretation of safety standards. We now present further details about the most novel and salient benefits, which come from three usage aspects of the safety compliance metamodels in general and of SafetyMet in particular: the mapping between safety standard models and project information, the reuse of safety standards models, and the relationship with the vocabulary. Other benefits of applying model-driven engineering for safety compliance such as the generation of electronic evidence repositories or the provisions of support for compliance planning have been discussed in [41]. For compliance with several standards, one model for all the standards or one model for each standard can be created, and thus associated to a project.

4.1.1 Mapping Between Safety Standard Models and Project Information

Fig. 3 shows how SafetyMet elements (bottom part of the figure) can be mapped to elements of project-specific metamodels (top part). In this example, *ArtefactType* is mapped to *Artefact*.

The possibility of establishing this mapping between these two elements provides a specific way of structuring the artefacts of a project according to how a safety standard requires them. At the same time, this allows identification of missing artefacts or artefact relationships. For example, if two artefact types are related in a safety standard model and it is specified that the artefact type relationship must exist for one of the artefacts types, it may be possible to detect that some artefact relationship is missing in a project.

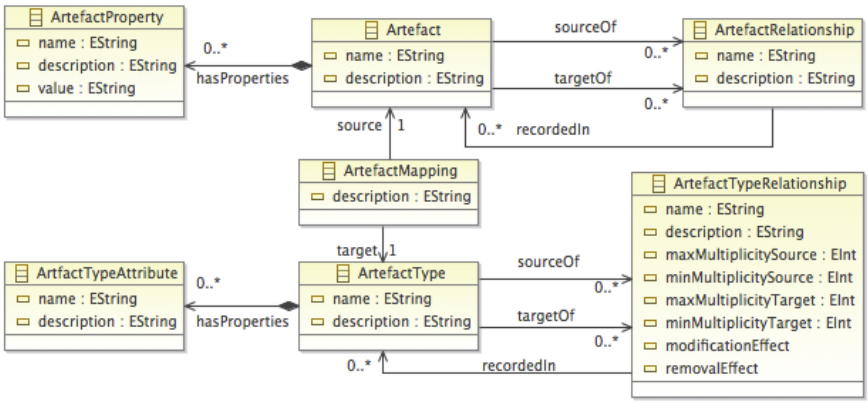

Fig. 3. Example of mapping with SafetyMet

In summary, a safety standard model provides what is usually referred to in the literature as conceptual schema [38] or traceability information model [10]. This can help practitioners to know if, for instance and in relation to the artefacts of a project, the set of artefacts is complete and consistent, thus allowing safety compliance according to a given safety standard model.

Another benefit from this usage is evidence reuse between projects. Once an artefact has been mapped to an artefact type, such a mapping and thus the use of the artefact as evidence of compliance with the corresponding safety standard can be reused. Finally, evidence change impact analysis can also be facilitated. By specifying change-related information in artefact type relationships, such information can be used to analyse change impact in the related artefacts (i.e., evidence).

4.1.2 Reuse of Safety Standards Models

Although project-specific information usually varies among projects, safety standard models can be reused in several projects. Therefore, all the benefits indicated in the previous section can apply to any project targeted at compliance with a given safety standard (i.e., its model). An existing safety standard model could also be used as the source for creating another model, thus reducing the effort for this task.

Furthermore, if mappings are specified between safety standards and thus between their models, it can be possible to determine how project assets mapped to a given safety standard model correspond to the elements of another safety standard model.

4.1.3 Relationship with the Vocabulary

In relation to the vocabulary, it is possible to both store information (i.e., terms) from a safety standard model in the vocabulary and also name the elements of a safety standard model according to the information stored in the vocabulary. Consequently, SafetyMet, in conjunction with the vocabulary, allows term reuse.

Another advantage of this reuse is related to terminology alignment. Once the terms of a safety standard have been stored in the vocabulary, they can be reused. Therefore, it is possible to guarantee that the terminology used in another safety standard model is aligned with that previously stored.

Finally, if mappings between the terminologies of different safety standard exist, and in line with the discussion in the previous section, terminology and the related compliance assets can be reused for compliance with several safety standards.

4.2 Limitations of SafetyMet and Its Application

Despite the argued benefits of SafetyMet, we also acknowledge that it has some limitations. Compliance with safety standards is a very complex activity, thus a metamodel alone cannot address all its needs and possible challenges. In this sense, OPENCOSS aims to mitigate many challenges in safety compliance by proposing new, systematic ways to address system assurance and certification. Nonetheless, some aspects are out of the scope of the project (e.g., analysis of the correctness of a fault tree), and some aspects cannot be fully addressed by means of new technology because of their nature (e.g., aspects in which a human has to make some judgement).

Two main areas have been identified in relation to the limitations of SafetyMet: certification risks and human aspects of safety compliance. Limitations arising from the validation performed so far (e.g., model creation for a limited set of standards) are not discussed but are regarded as aspects to be addressed in future work.

4.2.1 Certification Risks

Application of SafetyMet does not guarantee that certification risks will not arise in a project. In essence, there is no way to completely avoid these risks by means of model-based approaches, despite the fact that they can support and facilitate safety assurance and certification.

Although a project conforms to a safety standard model it is still possible that:

- Someone does not develop a safe system (e.g., because a hazard was missed).
- System safety cannot be demonstrated (e.g., someone might present inconsistent evidence, such test cases linked to requirements that the cases do not test).
- A third party does not agree upon the demonstration of safety compliance (e.g., there are aspects related to argumentation are out of the scope of SafetyMet).

4.2.2 Human Aspects of Safety Compliance

When dealing with safety compliance, many aspects cannot be fully supported by models and tools, automated, or automatically verified. Humans play a major role in safety compliance, and they will always be responsible for deciding upon safety.

Although this limitation cannot be avoided, we think that SafetyMet can help both suppliers and assessors in making informed decisions about system safety. It can help them to find the information that they need to gain confidence in system safety by providing traceability between the criteria of a safety standard and the assets managed in a project. SafetyMet can also support, for instance, verification of the existence of traceability between requirements and test results.

4.3 Open Issues

Last but not least, we have identified the following open issues regarding SafetyMet.

What sort of tool support and user interaction should be created to facilitate the use of SafetyMet? The practitioners who are expected to use SafetyMet (e.g., safety engineers and assurance managers) might not be familiar with the creation of graphical models and hence alternative representations may need to be investigated. Another aspect to study regarding tool support is how to present the large amount of information necessary to model a safety standard.

To what extent can the generation of safety standard models be automated? Given the size of safety standards, creation of the models can be very time-consuming. Therefore, the advantages and suitability of automatically generating the models from the textual standards could be studied.

Is there a correspondence between SafetyMet and the results of the OMG Software Assurance Task Force? The OMG has been working on the development of several specifications related to SafetyMet (e.g., SACM [39]). It is necessary to analyse in depth how SafetyMet relates to them in order to allow their integration.

How can SafetyMet be promoted in industry? A challenge for SafetyMet (and its tool support) is that it needs to be accepted by practitioners as a suitable way to deal with safety compliance. Further validation with industry and probably adjustments according to its needs will be necessary.

Which concepts should be in SafetyMet and which should be in the vocabulary of the overall safety compliance approach? An aspect about which we are not completely sure yet is the extent to which some safety standard-related information should be considered in SafetyMet or regarded as elements of the vocabulary. For example, some safety standards define enumerations for the values of the attributes of its artefact types. This has to be discussed with practitioners.

5 Conclusion

This paper has presented SafetyMet, a metamodel for safety standards. SafetyMet is part of an overall approach for safety compliance in evolutionary situations. The approach distinguishes between safety compliance metamodels and safety compliance models, as well as between safety standard-related information and project-specific information. The correspondence between these two aspects is not always clear, direct, or straightforward, and mappings must be defined.

SafetyMet includes the concepts necessary for enabling the demonstration of safety compliance in general, and in scenarios in which a system evolves or must be certified to different standards in particular. The metamodel aims to be generic and to allow flexibility in its use. It allows modelling of information related to process, data, and objectives for safety compliance. All these aspects can be necessary when having to demonstrate compliance with safety standards, and omission of the information can result in certification risks.

Industry can benefit from the application of SafetyMet by creating models of safety standards, mapping these models to project-specific models, reusing safety standard models, and relating the models and the vocabulary of the overall approach for safety compliance. Nonetheless, practitioners must be aware of the limitations of applying the metamodel. Certification risks cannot be completely avoided, and some decisions on safety compliance have to be made by humans. In this sense, SafetyMet can support and facilitate but not guarantee safety assurance and certification. In addition, there exist several open issues regarding SafetyMet and its use that must be studied.

As future work, we plan to address the open issues discussed above and to continue working on the specification and link of the rest of the safety compliance metamodels. SafetyMet also needs to be further validated, especially beyond the text of safety standards. Data from industrial projects will be used for this purpose.

Acknowledgments. The research leading to this paper 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. We also thank the OPENCOSS partners who have provided input and feedback on the metamodel, especially Katrina Attwood, Philippa Conmy, Huascar Espinoza, Tim Kelly, Jerome Lambourg, Sunil Nair, and Alejandra Ruiz.

References

1. Abdullah, N.S., Sadiq, S.W., Indulska, M.: A Compliance Management Ontology: Developing Shared Understanding through Models. In: CAiSE 2012
2. Adedjouma, M.: Requirements engineering process according to automotive standards in a model-driven framework. PhD thesis, University of Paris Sud XI (2012)
3. Alexander, R., Kelly, T., Gorry, B.: Safety Lifecycle Activities for Autonomous Systems Development. In: 5th SEAS DTC Technical Conference (2010)
4. Baufreton, P., et al.: Multi-domain comparison of safety standards. In: ERTS 2010
5. Bernardi, S., et al. A dependability profile within MARTE. SoSyM 10(3): 313-336 (2011)
6. Bézivin, J.: On the unification power of models. SoSyM 4(2): 171-188 (2005)
7. Briand, L.C., et al.: Automated impact analysis of UML models. Journal of Systems and Software 79(3): 339-352 (2006)
8. CENELEC: Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems - EN 50128 (2011)
9. Cleland-Huang, J., et al. (eds.): Software and Systems Traceability. Springer (2012)
10. Cleland-Huang, J., et al.: Trace Queries for Safety Requirements. In: REFSQ 2012
11. Denney, E., Pai, G., Pohl, J.: AdvoCATE. In: SAFECOMP Workshops 2012
12. de la Vara, J.L., et al.: COMPRO: A Methodological Approach for Business Process Contextualisation. In: CoopIS 2010
13. de la Vara, J.L., et al.: Towards a Model-Based Evolutionary Chain of Evidence for Compliance with Safety Standards. In: SAFECOMP Workshops 2012
14. DNV: Qualification of New Technology - DNV-RP-A203 (2012)
15. Emmerich, W., et al: Managing Standards Compliance. IEEE TSE 25(6): 826-851 (1999)
16. Falessi, D., et al.: Planning for safety evidence collection. IEEE Softw 29(3): 64-70 (2012)
17. Ghanavati, S., Amyot, D., Peyton, L.: A systematic review of goal-oriented requirements management frameworks for business process compliance. In: RELAW 2011
18. Giblin, C., et al.: Regulations Expressed As Logical Models (REALM). In: JURIX 2005
19. Gordon, D.G., Breaux, T.D.: Reconciling multi-jurisdictional requirements. In: RE 2012
20. Governatori, G., Milosevic, Z., Sadiq, S.W.: Compliance checking between business processes and business contracts. In: EDOC 2006
21. Graydon, P.J., et al.: Arguing Conformance. IEEE Software 29(3): 50-57 (2012)
22. Gronback, R.C.: Eclipse Modeling Project. Addison-Wesley (2009)
23. Habli, I., Kelly, T.: A Model-Driven Approach to Assuring Process. In: ISSRE 2008
24. IEC: Functional safety of electrical / electronic / programmable electronic safety-related systems (IEC 61508) (2005)
25. Ingolfo, S., et al.: Arguing regulatory compliance of software requirements. Data & Knowledge Engineering (accepted paper) (2012)
26. ISO: International Standard Road vehicles — Functional safety - ISO/DIS 26262 (2011)
27. Katta, V., Stålhane, T.: A Conceptual Model of Traceability for Safety Systems. In: CSDM 2011
28. Koschmider, A., de la Vara, J.L., Sánchez, J.: Measuring the Progress of Reference Model-Based Business Process Modeling. In: BPSC 2010
29. Krammer, M., Armengaud, E., Bourroihh, Q.: Method Library Framework for Safety Standard Compliant Process Tailoring. In: SEAA 2011

30. Kuschnerus, D., et al.: A UML Profile for the Development of IEC 61508 Compliant Embedded Software. In: ERTS 2012
31. Mayr, A., Plösch, R., Saft, M.: Towards an Operational Safety Standard for Software: Modelling IEC 61508 Part 3. In: ECBS 2011
32. Musat, D., et al.: MATURE: A Model Driven bAsed Tool to Automatically Generate a langUage That suppoRts CMMI Process Areas specification. In: EuroSPI 2010
33. Nair, S., et al.: The State of the Practice on Evidence Management for Compliance with Safety Standards. Simula Research Laboratory, Technical Report (2013)
34. Nair, S., et al.: Classification, Structuring, and Assessment of Evidence For Safety: A Systematic Literature Review. In: ICST 2013
35. Ncube, C., Maiden. N.A.M.: PORE: Procurement-Oriented Requirements Eng. Method for the Component-Based Systems Engineering Development Paradigm. In: CBSE 1999
36. Nekvi, M.R.I., et al.: Impediments to Requirements-Compliance. In: REFSQ 2012
37. Nejati, S., et al.: A SysML-Based Approach to Traceability Management and Design Slicing of Safety Certification. Information & Software Technology 54(6): 569-590 (2012)
38. Olivé, A.: Conceptual Modeling of Information Systems. Springer (2007)
39. OMG: Structured Assurance Case Metamodel (SACM) – Version 1.0 (online) http://www.omg.org/spec/SACM/ (2013) (Accessed Mar 3, 2013)
40. Panesar-Walawege, R. K., et al.: Characterizing the Chain of Evidence for Software Safety Cases: A Conceptual Model Based on the IEC 61508 Standard. In: ICST 2010.
41. Panesar-Walawege, R.K., et al.: Using Model-Driven Engineering for Managing Safety Evidence: Challenges, Vision and Experience. In: WOSOCER 2011
42. Panesar-Walawege, R.K., et al.: Supporting the verification of compliance to safety standards via model-driven engineering. Info. Softw. Technol. (accepted paper) (2013)
43. Papazoglou, M.P.: Making Business Processes Compliant to Standards & Regulations. In: EDOC 2011
44. Pohl, K.: Requirements Engineering. Springer (2010)
45. RTCA: DO-178C - Software Considerations in Airborne Systems and Equipment (2012)
46. Sadiq, S.W., Governatori, G., Namiri, K.: Modeling Control Objectives for Business Process Compliance. In: BPM 2007
47. Sannier, N., Baudry, B.: Toward multilevel textual requirements traceability using model-driven engineering and information retrieval. In: MoDRE 2012
48. Shamsaei, A., Amyot, D., Pourshahid, A.: A Systematic Review of Compliance Measurement Based on Goals and Indicators. In: CAiSE Workshops 2011
49. Sojer, D., Knoll, A., Buckl, C.: Synthesis of Diagnostic Techniques Based on an IEC 61508-aware Metamodel. In: SIES 2011
50. Stallbaum, H., Rzepka, M.: Toward DO-178B-compliant Test Models. In: MoDeVVa 2010
51. Sun, L., Kelly, T.: Elaborating the Concept of Evidence in Safety Cases. In: SSS 2013
52. Taromirad, M., Paige, R.: Agile Requirements Traceability Using Domain-Specific Modelling Languages. In: XM 2012
53. Wenzel, S.: Unique identification of elements in evolving software models. SoSyM (accepted paper) (2013)
54. Zoughbi, G., Briand, L., Labiche, Y.: Modeling safety and airworthiness (RTCA DO-178B) information. SoSyM 10(3): 337-367 (2011)