White Rose Research Online

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk
Universities of Leeds, Sheffield and York

Deposited via The University of York.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/id/eprint/94449/

Version: Accepted Version

Article:
de la Vara, Jose Luis, Ruiz, Alejandra, Attwood, Katrina et al. (2016) Model-based specification of safety compliance needs for critical systems: A holistic generic metamodel. Information and Software Technology. pp. 16-30. ISSN: 0950-5849

https://doi.org/10.1016/j.infsof.2015.11.008

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

Manuscript
Click here to view linked References

Model-Based Specification of Safety Compliance Needs for Critical Systems: A Holistic Generic Metamodel

Jose Luis de la Vara[a,1], Alejandra Ruiz[b], Katrina Attwood[c], Huáscar Espinoza[b], Rajwinder Kaur Panesar-Walawege[d], Ángel López[b], Idoya del Río[b], Tim Kelly[c]
[a]Computer Science Department, Carlos III University of Madrid, Avda. Universidad 30, 28911 Leganés, Madrid, Spain
[b]ICT-European Software Institute, Tecnalia, Parque Tecnológico Ed. 700, E-48160 Derio, Spain
[c]Department of Computer Science, University of York, Heslington, York YO10 5GH, United Kingdom
[d]Meta-zen Consulting, Unit 50 - 12165, 75 Avenue, Surrey, British Columbia, V3W0W7, Canada

Abstract
Context: Many critical systems must comply with safety standards as a way of providing assurance that they do not pose undue risks to people, property, or the environment. Safety compliance is a very demanding activity, as the standards can consist of hundreds of pages and practitioners typically have to show the fulfilment of thousands of safety-related criteria. Furthermore, the text of the standards can be ambiguous, inconsistent, and hard to understand, making it difficult to determine how to effectively structure and manage safety compliance information. These issues become even more challenging when a system is intended to be reused in another application domain with different applicable standards.
Objective: This paper aims to resolve these issues by providing a metamodel for the specification of safety compliance needs for critical systems.
Method: The metamodel is holistic and generic, and abstracts common concepts for demonstrating safety compliance from different standards and application domains. Its application results in the specification of "reference assurance frameworks" for safety-critical systems, which correspond to a model of the safety criteria of a given standard. For validating the metamodel with safety standards, parts of several standards have been modelled by both academic and industry personnel, and other standards have been analysed. We further augment this with feedback from practitioners, including feedback during a workshop.
Results: The results from the validation show that the metamodel can be used to specify safety compliance needs for aerospace, automotive, avionics, defence, healthcare, machinery, maritime, oil and gas, process industry, railway, and robotics. Practitioners consider that the metamodel can meet their needs and find benefits in its use.
Conclusion: The metamodel supports the specification of safety compliance needs for most critical computer-based and software-intensive systems. The resulting models can provide an effective means of structuring and managing safety compliance information.

Keywords. Safety-critical system, safety standard, safety compliance, safety assurance, safety certification, reference assurance framework, metamodel.

1 Introduction

Most critical computer-based and software-intensive systems in domains such as aerospace, railway, and automotive are subject to some form of safety assessment by a third party (e.g. a certification authority) as a way of ensuring that they do not pose undue risks to people, property, or the environment. A common type of assessment is compliance to safety (or safety-related) standards, usually referred to as safety certification. Examples of safety standards used in industry [1,2] include IEC 61508 for electrical, electronic, and programmable electronic systems in a wide range of industries, and more specific standards such as DO-178C for avionics, the CENELEC standards for railway (e.g. EN 50128), and ISO 26262 for the automotive sector.

[1] Corresponding author. Tel.: +34 91 624 91 15; fax: +34 91 624 91 29
Email addresses: jvara@inf.uc3m.es (J.L. de la Vara), alejandra.ruiz@tecnalia.com (A. Ruiz), katrina.attwood@york.ac.uk (K. Attwood), huascar.espinoza@tecnalia.com (H.Espinoza), rajwinder.panesar@gmail.com (R.K. Panesar-Walawege), angel.lopez@tecnalia.com (A. López), idoya.delrio@tecnalia.com (I. del Rio), tim.kelly@york.ac.uk (T. Kelly)

Demonstration of compliance with safety standards is usually costly and time-consuming [3], and can be very challenging [2,4]. Firstly, system suppliers have to collect evidence for compliance such as hazard analyses, test results, and activity records in order to show that the safety criteria of a standard have been fulfilled. In order to collect this evidence, practitioners need to determine the safety objectives to be reached and the process to be executed based on the characteristics of a particular system. As the text of the safety standards can be ambiguous, inconsistent, and hard to understand, this can become an arduous task. Secondly, practitioners usually have to manage large quantities of evidence 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 changes [5]. For example, evidence evolves when a system aims to be certified against different safety standards or reused in another application domain. These are currently important concerns in industry [6], and most practitioners have faced these situations according to [1]. Although the correspondence between safety standards has started to be studied, it is a complex task. No perfect match usually exists between the compliance needs of different 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. The industry needs means that enable evidence reuse and support evidence change impact analysis in general, and in cross-domain and cross-standard situations in particular.

All the challenges above can lead to certification risks [7], as a system supplier might not be able to develop a safe system, demonstrate compliance with a safety standard, or help a third party to gain confidence in system safety. We advocate the use of model-based approaches to tackle these challenges. Models can facilitate the understanding of safety standards [8], the identification of inconsistencies in their text [9], the determination of the evidence to collect [3], the specification of traceability requirements [10], and compliance assessment [11]. There is evidence of the use of models in industry for safety compliance purposes [1,2]. However, the current approaches are standard-specific (e.g. for IEC 61508 [8]) or address only partial safety compliance needs (e.g. process compliance [12]). Therefore, they do not provide solutions that can be directly applied in contexts of cross-domain use or where compliance with multiple standards is necessary, or that cover all safety compliance needs.

This paper aims to fill this gap by providing a generic, safety standard-independent metamodel for the holistic specification of safety compliance needs. To our knowledge, no other model or metamodel has achieved this objective, except our previous work presented in [13]. Therefore, we provide the first common, unifying model of safety compliance needs for critical systems.

We present a metamodel for reference assurance frameworks (RAF), which model the different criteria for demonstrating the compliance of a critical system with a safety standard. The metamodel includes concepts and relationships in the form of classes and associations that are common to different safety standards and to different application domains. It addresses safety compliance from several perspectives, explicitly dealing with information related to the process, data, and objectives necessary to demonstrate compliance, and their applicability. The metamodel is also part of a wider approach for compositional and evolutionary safety assurance and certification and for cross-domain reuse of assurance information. This approach has been designed in the scope of OPENCOSS (http://www.opencoss-project.eu), which is a European industry-academia project that has defined model-based safety compliance support for automotive, avionics, and railway. The specification and validation of the RAF metamodel consists of over two years of extensive and continuous work in the OPENCOSS project, including industrial case studies in the automotive, railway, and avionics domains.

This paper extends the results in [13], where we presented the initial version of the metamodel. The extension is mainly based on: (1) the introduction of new classes and associations in the metamodel and the refinement of others in order to meet further industry requirements and expectations on the specification of safety compliance needs; (2) the provision of further information about the metamodel and its usage; (3) a wider validation of the metamodel, with a higher number of standards (from four to 37 standards) and in the context of three specific industrial case studies, and; (4) feedback from practitioners, including the organization of a workshop with practitioners at which they provided feedback on the metamodel and its use. We started with a much simpler metamodel and initially validated it using fragments of four different standards. The metamodel has now evolved considerably based on feedback from industry personnel. This includes practitioners that have used RAF models (e.g. in OPENCOSS industrial case studies). The feedback was used to

enhance the metamodel. We have also taken steps to further validate the metamodel with more standards and a small workshop.

The rest of the paper is organized as follows. Section 2 presents the background of the paper. Section 3 introduces the metamodel and Section 4 presents its validation. Section 5 summarises our conclusions. Finally, Appendix A lists the safety standards analysed for validation.

2 Background

We have divided the background of the paper into two main parts: the OPENCOSS project and related work.

2.1 The OPENCOSS project

OPENCOSS is a large-scale European research project on safety assurance and certification of embedded systems. The OPENCOSS consortium comprises four academic partners and 13 companies, including safety-critical system manufacturers, component suppliers, certification authorities, safety assessors, and tool vendors. The project is also supported by a large advisory board with representatives from more than 20 international organizations.

The project has (1) devised a common certification framework that spans different vertical markets for railway, avionics, and automotive industries, and (2) developed 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.

For the common certification conceptual framework, the main objective is to create a language that can be used across different domains to describe safety-related information, standards, and projects. Such a language will facilitate the analysis and the comparison of safety standards, and the reuse of safety-related information across projects, including projects under different safety standards or in different application domain.

Fig. 1 outlines the model-based approach defined in OPENCOSS for safety assurance and certification. The approach is based on a set of metamodels targeted at different safety assurance and certification needs, to which models of safety assurance and certification must conform. The set of metamodels corresponds to the common certification conceptual framework. The RAF metamodel is part of this framework and addresses the specification of the safety compliance needs that have or might have to be considered in an assurance project. These needs can be from either specific standards, recommended practices, or company-specific practices. As can be observed, the development of the RAF metamodel is only one of the activities of OPENCOSS. The project deals with many other aspects (e.g. modelling of assurance project information and the development of an approach for cross-domain reuse of this information).

In practice, there are two main sources of information for safety compliance: the standard to be complied with and the product for which compliance is sought. Therefore, the metamodels produced during the OPENCOSS project include the concepts and relationships necessary for modelling and managing project-specific information. This assurance information needs to be recorded regardless of which safety standard is being followed. OPENCOSS has defined metamodels for modelling the process executed to create a product, the evidence of safety and of compliance, and the arguments that will be used to justify key safety-related decisions taken during the project. The specific safety criteria of a standard with which an assurance project has to show compliance are represented by means of a baseline. This baseline is usually a subset of all the safety criteria present in a standard, and can be tailored to project-specific characteristics. For example, the safety criteria will vary if a system is developed using model-based technologies or automatic code generation.

Two other metamodels are proposed. The vocabulary metamodel is a means to define and record the terms and concepts used to characterize reusable assurance assets such as evidence, argumentation, and process data. Finally, there is a metamodel for mappings. Mappings can be specified between vocabulary terms (e.g. from different application domains), between the assurance information gathered during a project and its baseline for indicating compliance, and between safety standards (i.e. RAF models) for indicating how the standards relate and if equivalences exist between them. In general, the mappings aim to allow engineers and managers to make informed decisions about the appropriateness and implications of reusing assurance information across projects, safety standards, and application domains.

Further information about the OPENCOSS approach for safety assurance and certification can be found in [14].

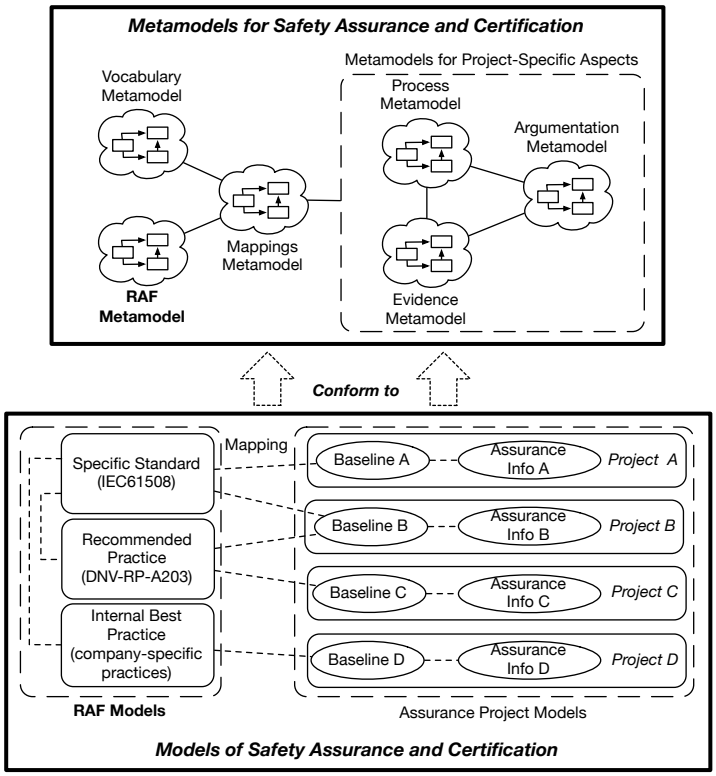

Fig. 1. Overview of the OPENCOSS approach for safety assurance and certification

2.2 Related work

As discussed in [13], compliance has received great attention in the requirements engineering and business process management communities, including model-based compliance. Models can also be used for safety-critical system specification.

In this section, we review related work that has proposed model-based approaches for the specification of safety compliance needs (i.e. of criteria whose fulfilment must be shown for safety assurance and certification according to some safety standard). This work can be divided into three main streams: safety regulation modelling, safety standard-specific modelling, and safety standard-independent modelling. When mentioning models in this section, we refer to both models and metamodels, understood as sets of concepts and the relationships between them, and independently of the graphical or textual languages used for their representation. Overall, we have found that there is no holistic and generic means for the modelling of safety compliance needs.

By **safety regulation modelling**, we refer to modelling the content (i.e., text) of standards in order to perform some analysis for identifying, for instance, issues such as conflicts and inconsistencies. Regulation modelling is an area in which very little has been done so far for safety standards. We are only aware of three research efforts, one for railway [15] and two for the nuclear domain [9,16]. These publications have not addressed the need for deriving a RAF from the text of safety standards. It is not enough to analyse the different parts of the text, but it is also necessary to determine how a project or product can comply with a safety standard.

Safety standard-specific modelling corresponds to those model-based approaches that focus on some safety standard. Models have been proposed for DO-178B (e.g. [17]), IEC 61508 (e.g. [8]), ISO 13482 [18], and ISO 26262 (e.g. [19]). The models have addressed specific aspects of the standards, such as their processes [20-22], artefact traceability [23,24], system specification [17,18,25], system architecture [26,27], quality-related aspects [28], faults [29], and testing [30]. The models in [8,25] address both process and system specification. Models for more than one safety standard can also be found. Process assurance with ISO 26262 and Automotive SPICE is addressed in [31], the representation of the safety case process with EN 50126, EN 50128, and EN 50129 in [32], and the specification of safety-related design aspects for IEC 61508, ISO 12100, or ISO 26262

in [33]. Panesar-Walawege et al. [34] have presented an approach for the specification of IEC 61508-based sector-specific models, and Papadopoulos and McDermid [35] have proposed a common process for system development, assessment, and certification after analysing ten safety standards (ARP4754, ARP4761, DO-178, DO-254, EN 50126, EN 50128, EN 50129, EN 50159, IEC 61508, and MISRA). A similar process model is presented in [36]. In the medical domain, there are some efforts trying to define common software process [37] and traceability [38] models from different standards and regulations.

The main weakness of these models is that they cannot be directly applied for demonstrating compliance with other safety standards. For example, the IEC 61508 model proposed in [8] does not support demonstration of compliance with DO-178. These models could also be represented with the RAF metamodel and thus can be regarded as RAF models. Therefore, the RAF metamodel increases the level of abstraction of these approaches for the specification of safety compliance needs.

Finally, **safety standard-independent modelling** explicitly aims to support the specification of safety compliance needs in a generic way, so that the approaches can be instantiated for any safety standard. Whereas safety standard-specific models are mostly characterised by the adoption of concepts and relationships from concrete safety standards, safety standard-independent models are characterised by the use of concepts and relationships that correspond to notions from several safety standard. In other words, the latter are mainly based on concept generalization and abstraction from standards. For example, they would use “artefact” as a generalization and abstraction of requirements specification, design specification, test case specification, and source code. The former are mainly based on concept set extension. For example, they would directly include requirements specification, design specification, test case specification, and source code as concepts. Therefore, the RAF metamodel corresponds to safety standard-independent modelling.

The approaches that have addressed this type of modelling focus on specific safety compliance needs such as the requirements to fulfil [39], the artefacts to manage [40], artefact traceability [41], and the process to follow [12,42-44]. Safety cases have also been used for the analysis of safety standards in order to determine the safety arguments in the standards and thus how safety is or should be justified [45-50]. All these models have not addressed most of the relationships to consider between objectives, data, processes, and applicability information of standards for the specification of safety compliance needs. Therefore, although they are suitable for their purposes, these solutions are partial for the challenges addressed in this paper.

3 Metamodel for reference assurance frameworks

This section introduces the metamodel that we propose for the specification of safety compliance needs in the form of RAFs. The metamodel includes key concepts and the relationships between them for demonstrating safety compliance. It captures abstract notions that can be used to describe the information that needs to be collected to show compliance with safety standards and to manage system change. Specifically, the RAF metamodel corresponds to a unified means for the creation of models for safety assurance and certification.

In general, safety compliance is not based on just one standard. Minimally there is at least the safety standard(s) 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 are geared towards aiding compliance with the applicable safety standard. In other cases, a system is to be certified to multiple standards being used in different parts of the world, and finally there may be the case of using components (or sub-systems) that have been certified in one domain, in another. Hence a component certified to one standard or set of standards may have to be re-certified to another. There exist also other specific needs when a system evolves [5], such as managing evidence change impact. We propose the RAF metamodel in order to aid compliance in these various scenarios.

The main rationale for developing RAF models is to create a consistent interpretation of the standard being used and link the interpretation 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 developing and communicating a shared, consistent interpretation. The RAF metamodel also provides a common means for comparing safety standards, based on a common terminology (i.e. the classes and associations of the metamodel), and can in turn facilitate safety assurance reuse across safety standards and application domains.

The proceeding subsections present the classes and associations of the RAF metamodel and its usage scenarios, and discuss some aspects of the metamodel. The examples provided focus on DO-178C, EN 50128, IEC 61508, and ISO 26262.

3.1 Classes and associations

Fig. 2 shows the RAF metamodel. For clarity, we have decomposed the metamodel into four interrelated parts: specialization hierarchy, main components of a RAF, reference assurable elements associations, and RAF applicability information. We do not show the attributes of the classes in all the parts in order to keep the figure as small and simple as possible.

A *Reference Element* (Fig. 2 (a)) has an ID, a name, a description, and a reference. The reference is for specifying from where an element is modelled (e.g. a clause of a safety standard). Some reference elements are also reference assurable elements, which represent the main safety concerns that need to be modelled for a critical system's lifecycle:

- *Reference Requirement*: conditions (e.g. an objective) that might have to be fulfilled (e.g. the software shall be produced to achieve modularity, testability, and the capability for safe modification, in IEC 61508)
- *Reference Activity*: unit of behaviour that might have to be executed (e.g. Software development processes in DO-178C).
- *Reference Role*: type of agents that might have to be involved (e.g. Designer in EN 50128).
- *Reference Artefact*: unit of data that might have to be managed (e.g. Safety plan in ISO 26262).
- *Reference Technique*: specific way to execute a reference activity or create a reference artefact (e.g. Formal methods in IEC 61508).
- *Reference Artefact Relationship*: relationship between two reference artefacts that might have to be recorded (e.g. satisfies in DO-178 - Design description satisfies Software requirements data).
- *Reference Artefact Attribute*: characteristic of a reference artefact that might have to be recorded (e.g. the expected result of a test case in EN 50128).

We deliberately indicate that the above needs *might* have to be addressed, as whether or not they are finally addressed will depend on project-specific aspects. For example, a company might only deal with software testing of safety-critical systems, thus it would not have to show compliance with the safety criteria of other software development activities. This is further explained in Section 3.2 (Usage scenarios).

Reference Assurance Framework corresponds to a composition of the safety criteria with which a critical system's lifecycle might have to show compliance (Fig. 2 (b)). Intuitively, a RAF represents a safety standard, and more concretely its safety compliance needs. In addition to reference requirements, activities, roles, techniques, and artefacts, a RAF can consist of *Reference Criticality Kind* (category of risk-reduction criteria) and *Reference Applicability Kind* (category of relevance or appropriateness for reference assurable elements). For example, SIL (Safety Integrity Level) is probably the most well-known reference criticality kind. It is used in IEC 61508 and other related standards (e.g. EN 50128). These standards also commonly provide some form of recommendation of use (reference applicability kind) for reference techniques.

Reference assurable elements are related to one another in several ways (Fig. 2 (c)). Reference requirements, which can be decomposed into sub-requirements, can be assigned to some *Constrained Reference Assurable Element*. In other words, reference activities, artefacts, roles, and techniques can be responsible for the fulfilment of reference requirements. Reference roles can participate in reference activities, and be responsible for some reference artefact. Reference techniques can be used for both reference activities and reference artefacts, and be specialised into other techniques. For example, Modelling is specialised in EN 50128 into Data modelling and Sequence diagrams, among other techniques. Reference activities can have input and output reference artefacts, and output reference artefact relationships. A reference activity can further be decomposed into sub-activities, and have predecessor and successor reference activities. Reference artefacts can have reference artefact attributes, can be the source or the target of artefact reference relationships, and can record these relationships. Finally, information about the multiplicity and change effects of the source and the target of a reference artefact relationship can be specified.

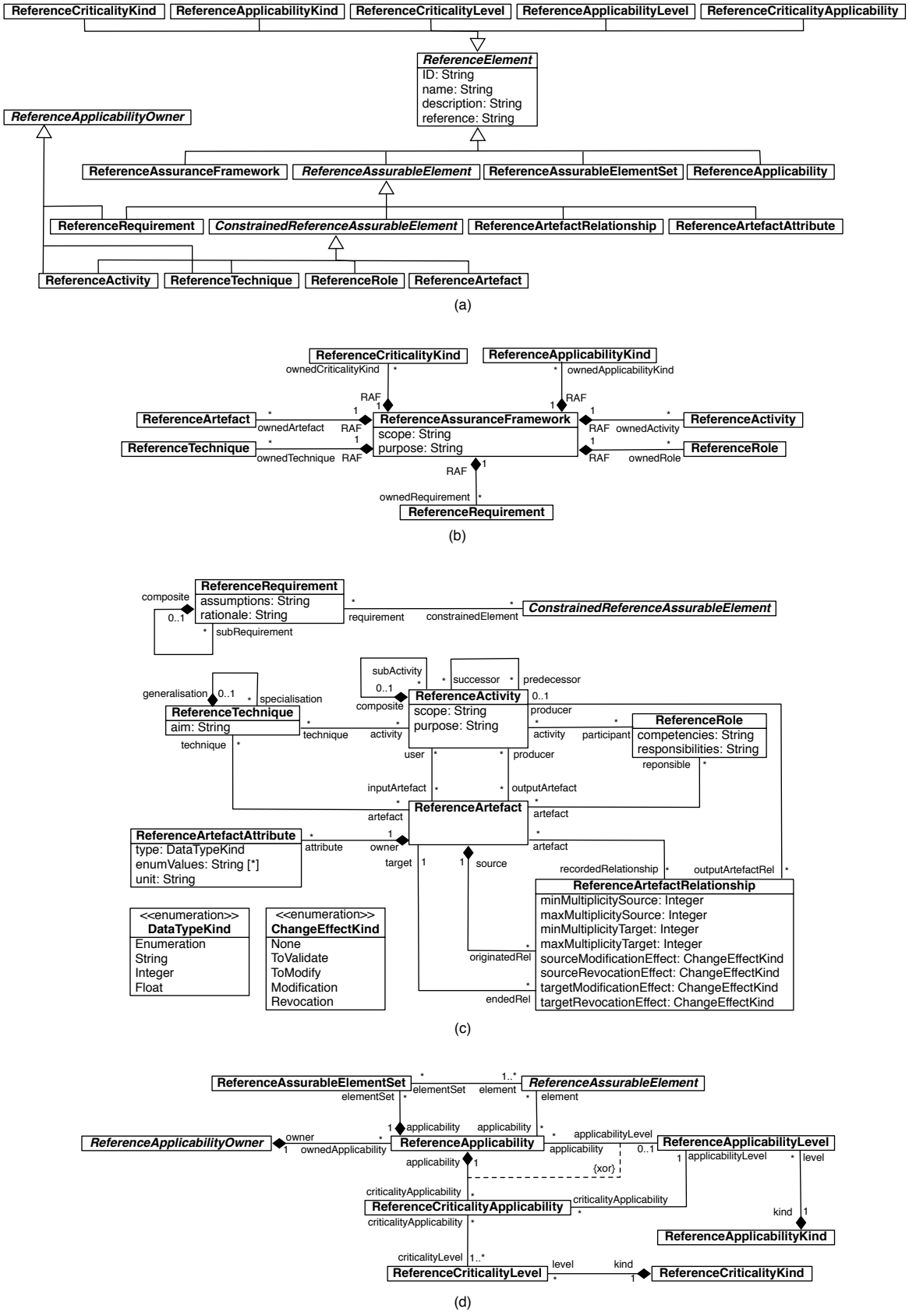

Fig. 2. RAF metamodel divided into (a) specialization hierarchy, (b) main components of a RAF, (c) reference assurable elements associations, and (d) RAF applicability information

RAF applicability information (Fig. 2 (d)) represents the safety criteria of standards regarding the circumstances under which compliance with reference assurable elements has to be shown, and how to show it. This information is arguably the most distinguishable characteristic of the RAF metamodel. RAF applicability information is provided in relation to some *Reference Applicability Level* (levels of relevance or appropriateness for a reference applicability kind) or to some *Reference Applicability Level* and some *Reference Criticality Level* (relative level of risk-reduction provided for a reference criticality kind). For example, IEC 61508 "recommends" and "highly recommends" (reference applicability levels) the use of some reference techniques for SIL 4 (reference criticality level), which is associated with an average probability of a dangerous failure on demand of a safety function (from 1e–5 to 1e–4). Safety standards provide applicability information (*Reference Applicability*) in the scope of reference activities, reference requirements, or reference techniques (*Reference Applicability Owner*), often by means of tables in their text. *Reference Criticality Applicability* roughly corresponds to the cells of these tables. Although applicability information usually only refers to single reference assurable elements (element of *Reference Applicability*; e.g. rows in IEC 61508 tables), the standards can also provide applicability information for several reference assurable elements (e.g. a valid combination of techniques in EN 50128) and for sets of reference assurable elements in relation to others (e.g. a set of reference roles that have to be independent from a given reference role).

Table 1 shows examples of the correspondence between the main concepts of the metamodel and the information in different safety standards. The cells with a hyphen ('-') indicate that the corresponding information is not explicitly provided by that safety standard, but that instead a system supplier has to decide upon a value for it (e.g. the roles in a DO-178C project).

Table 1. Examples of RAF concepts for specific safety standards

	Standard			
Concept	**DO-178C**	**EN 50128**	**IEC 61508**	**ISO 26262**
Ref. Criticality Level	Software Level A-E	SIL 0-4	SIL 1-4	ASIL A-D
Ref. Applicability Level	Objective satisfaction should be shown as Satisfied or Satisfied with independence, or is at applicant's discretion	Mandatory, Highly Recommended, Recommended, Not recommended, no recommendation for or against	Recommended, Highly Recommended, Not Recommended, no recommendation for or against	Recommended, Highly recommended, or No recommendation for or against
Ref. Activity	Software development processes	Component design	Software design	Software unit design
Ref. Role	-	Designer	Developer	Designer
Ref. Technique	-	Modelling	Formal methods	Control flow monitoring
Ref. Artefact	Software Requirements Data	Software Design Specification	System Design Specification	Software unit design specification
Ref. Artefact Relationship	Design Description *satisfies* Software Requirements Data	Software Component Design Specification *links to* Software Component Test Specification	Software System Design Spec. *derived from* Software Architecture Design and Hardware Architecture Design Descriptions	Software Unit Design Specification *links to* Software Requirements and *specifies* Software Unit Implementation
Ref. Requirement	(11.3b) Independence: A description of the methods for establishing verification independence	(7.4.4.1) Software Component Design Specification for each component	(7.4.5.3) Software modularity, testability, and safe modification	3-8.4.5.1.1 Consistency and compliance of Functional Safety Reqs. with respect to the safety goals

When compared to the version presented in [13], the RAF metamodel has both grown (e.g. from 12 to 19 classes and from 26 to 33 associations) and been adjusted (e.g. inclusion of *Reference Element* as a base class with the reference attribute) in order to meet further industry requirements and expectations for the specification of safety compliance needs. The most revised part of the RAF metamodel is the applicability information, which is essential for safety compliance because it

indicates how and when the criteria of a safety standard have to be fulfilled. *Reference Applicability*, *Reference Applicability Owner*, *Reference Assurable Element*, *Reference Assurable Element*, *Reference Applicability Kind*, and *Reference Criticality Kind* have been added. In the initial version of the metamodel, activities could not be the owner of a reference applicability, the element of a reference applicability could only be reference requirements or reference techniques, and no difference could be explicitly made among reference applicability kinds and among references criticality kinds.

More details about the metamodel can be found in [14].

3.2 Usage scenarios

The primary use intended for the RAF metamodel is the specification of safety compliance needs by means of RAF models. Fig. 3 shows an excerpt of a RAF model for IEC 61508 in the form of a UML (Unified Modeling Language) object diagram. The diagram represents examples mentioned above when introducing the classes and associations of the metamodel. We refrain from showing further parts of the models that we have created because the safety standards are under copyright. As can be observed in Fig. 3, the RAF metamodel enables the structured specification of how to comply with a safety standard, taking into account the possible criteria related to the objectives, process, and data required by the standard, and their applicability. We have chosen IEC 61508 to show an example because it is a generic standard used in many applications domains and from which domain-specific standards have been derived (e.g. ISO 26262 in automotive).

A RAF modelling tool has also been developed in OPENCOSS [51]. The development of the tool shows that the metamodel can be used for the specification of safety compliance needs. The tool comprises an Eclipse-based editor with which a user can create graphical representations of safety compliance needs by means of *Reference Activity*, *Reference Artefact*, and *Reference Role*, and can specify the possible remaining needs using forms.

The next subsections present the main usage scenarios on which we have worked in OPENCOSS.

3.2.1 Development of a common understanding of safety compliance needs

One of the main issues with the texts of safety standards is that they can be ambiguous, inconsistent, and hard to understand. The terminology can also vary among standards (e.g. “work products” in ISO 26262 vs. “data item” in DO-178C), which can hinder their comparison, especially since there is often incomplete conceptual overlap between safety-critical domains.

We are using the RAF metamodel to address these issues in two main ways. First, the concepts and relationships of the metamodel allow us to refer to safety compliance needs with a common, unified terminology. For example, OPENCOSS partners clearly understand what is indicated by a “reference activity”, regardless of the specific safety standard followed. Second, the creation of RAF models can help in developing a common understanding of the safety compliance needs of a given standard. The models can, for instance, make it much clearer how an artefact is used in relation to specific objectives.

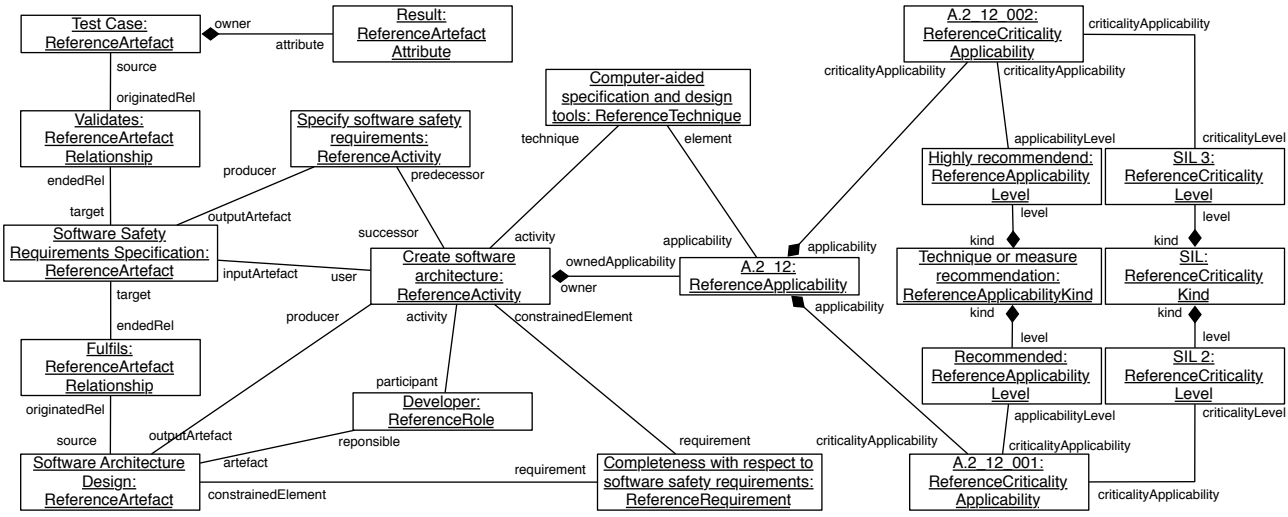

Fig. 3. RAF model for IEC 61508

Modelling a safety standard also makes its implicit information explicit, and facilitates the identification of aspects that might require further clarification (e.g. inconsistencies between objectives). This is useful when discussing different interpretations of the standard. By explicitly modelling these interpretations, the possible ambiguity of the standards can be reduced.

3.2.2 Specification of project-specific safety compliance needs

The OPENCOSS approach for safety assurance and certification (Section 2.1) includes the modelling of baselines for the specification of project-specific safety compliance needs. The corresponding models are based on the RAF metamodel, and can include: (1) the parts of an existing RAF model with which an assurance project has to demonstrate compliance, and; (2) the refinement, tailoring, or extension of a RAF model for project-specific purposes.

For example, a safety standard may not provide information about reference roles, but a company is likely to want to specify them for a given assurance project. Another example is the development of a Safety Element out of Context (SEooC) for the automotive domain. Such an element corresponds to a vehicle sub-system or component, developed with the intention of being applicable in multiple projects, and requires a selection of some ISO 26262 activities and their tailoring.

3.2.3 Management of safety assurance information

A RAF model can be regarded as what is sometimes referred to as a conceptual schema [52] or traceability information model [10] for an assurance project. In other words, when used in a baseline, a RAF model provides a reference of what the project is expected to do and how: reference requirements to fulfil, reference artefact relationships to record, etc.

Therefore, the use of RAF models supports the management of safety assurance information. First, it supports the specification of the information to manage in an assurance project. Second, it can be used as basis to determine whether all of the planned information has been collected. Third, information consistency can be assessed based on the structure of a RAF model (e.g. expected artefact relationships). Finally, the change-related information in reference artefact relationships can be used for managing impact analysis.

3.2.4 Specification of safety compliance

Mappings from project assets to the assets mandated by the standard (i.e., to a RAF model, and more concretely to a baseline) need to be created in order to demonstrate safety compliance. By doing so, we can show clearly how a particular asset created during a project complies with a particular standard. The use of mappings also provides a clear traceable link between the assets of a project and the standard to be complied with. This link is very difficult to show and maintain using textual documents, but can be more easily managed using models [8].

When a project needs to comply with multiple standards, the vocabulary can aid in mapping the assurance assets created in the project for compliance with one standard to those required by another standard, or at least in indicating where conceptual gaps exist between assurance needs in the standards. 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. OPENCOSS mappings metamodel provides for the specification and justification of incomplete mappings, which can help to clarify these additional needs. The model also provides for mismatches (“no map”), which can be important to record.

3.2.5 Specification of the correspondence between safety standards

One of the main objectives of the RAF metamodel is to provide a common means for the systematic comparison of safety standards and thus for the determination of similarities and differences between them. This is achieved by supporting the modelling of the safety compliance needs for different safety standards, which can also be used in different application domains.

The comparison of safety standards leads to the specification of the correspondence between them by means of mappings. This supports the indication of whether a concept (reference requirement, activity, artefact, etc.) from one standard is equivalent, partially equivalent, or not equivalent with a concept in another standard. Such information can be used for analysing asset reuse across standards and domains, by determining how safety assurance information according to a given standard fulfils the safety criteria of another standard. This is one of the main strategies proposed in OPENCOSS for making safety assurance and certification more cost-effective.

3.3 Discussion

In this section we discuss decisions made when creating the metamodel. Awareness of these decisions can be important for understanding and using the metamodel. Further information about practical aspects in using the metamodel is provided in Section 4.3 (Lessons learnt).

3.3.1 Terminology differences with specific safety standards

The concepts (i.e. the names of the elements) of the RAF metamodel correspond to abstract, generic notions of how to comply with safety standards. Such notions are common to different standards and different application domains, and the concepts can be named in different ways in different safety standards and application domains. Table 1 shows examples of the correspondence between RAF terms and the terms in some safety standards. Anyone using the metamodel must determine these correspondences in order to properly create RAF models.

We have selected the terms for naming the concepts in the RAF metamodel from the terminology used in safety standards, related work, and practitioners' feedback on their suitability. For example, *Reference Assurance Framework* was formerly named Safety Standard [13]. This change was based on practitioners' opinion regarding the common association of the term safety standard to international standards, but not for example to company-specific or recommended practices.

3.3.2 Specialization of reference artefact relationships

The RAF metamodel deals with (reference) artefact relationships in a very generic and abstract way. It does not impose a predefined set of possible relationships (e.g. satisfies, verifies, and implements), but rather allows the modellers to define their own relationships according to the safety standards that they follow. There is one main reason for this decision.

There are terms commonly used for naming relationships but whose semantics varies between safety standards and application domains. For example, the semantics of the terms 'validation' and 'verification' is different between DO-178C and EN 50128. Therefore, the specification of a class that specialises *Reference Artefact Relationships* into 'validates' and 'verifies' would not be suitable. In essence, it is hard and risky to define more specific common, cross-domain, and cross-standard notions for reference artefact relationships. We acknowledge that it could be done in some cases, but it would require a very detailed analysis and comparison of the possible relationships according to specific safety standards, including company-specific ones. It would very likely result in a large specialization hierarchy due to subtle differences, as with 'verification', and the complexity and prescriptiveness of this hierarchy could limit its usefulness. Instead, we opt for an abstract, highly specialisable relationship.

3.3.3 Relationships between reference requirements

As for any system, relationships exist between the requirements of a safety-critical system (e.g. 'AND' and 'OR'; [53]), including the requirements that safety standards impose (i.e. reference requirements). In a change from the previous version of the metamodel [13], we here prefer not to define specific relationships between reference requirements in the RAF metamodel beyond their refinement and decomposition (subRequirement). Other relationships between the requirements must be handled by means of reference applicability categories and levels, as is the case in the OPENCOSS target domains.

The main rationale for this decision is that the relationships can vary depending on, for instance, the criticality levels. The relationships also define constraint levels. For example, an 'AND' relationship is more restrictive than an 'OR'. Therefore, we regard them as applicability information, which should be specified with the corresponding elements of the RAF metamodel (Fig. 2 (d)). We further consider that the semantics and purpose of the relationships and types of relationships between reference requirements is very similar to the current semantics and purpose of other reference applicabilities with several elements. For example, safety standards can indicate that only one reference technique within a set of techniques needs to or must be used (i.e. at least one technique must be used, or one and only one), the same as they can indicate that only one reference requirement within a set of requirements needs to or must be fulfilled.

4 Validation

We have systematically validated the RAF metamodel by modelling and analysing safety standards, from their text, and in a workshop with practitioners. The first activity sought to address the question of whether the metamodel supports the specification of industrial safety compliance needs. The second activity was aimed to complement the first one by performing a systematic collection of practitioners' feedback on a set of RAF concepts and about the acceptance of the use of the metamodel.

In addition, we have received regular feedback on the metamodel from OPENCOSS industrial stakeholders at project meetings and as a result of their collaboration in using the metamodel in three industrial case studies in automotive, avionics, and railway [54], respectively. The case studies dealt with the certification and reuse of an automotive component, the reuse of a railway execution platform in avionics, and the certification and cross-country reuse of a railway signalling sub-system. This feedback was collected in a spreadsheet and later analysed. Changes in the metamodel were agreed from the feedback, leading to a metamodel that is more representative of industrial needs. The execution of the usage scenarios presented in Section 3.2 has also contributed to the validation of the RAF metamodel, as has the feedback from OPENCOSS advisory board. Therefore, we have received extensive feedback from practitioners on the metamodel, but this feedback has been systematically collected about a pre-defined set of aspects only in the workshop. Finally, an implicit validation activity has been the analysis of how well the safety standard-specific models presented in related work (Section 2.1) could be specified with the RAF metamodel.

In summary, the overall validation conclusions are drawn from a set of five different activities: modelling of standards, analysis of standards, analysis of related models and metamodels, collection of practitioners' feedback at the workshop, and collection of practitioners' feedback in other activities of OPENCOSS (e.g. industrial case studies and in over a dozen meetings with practitioners). In total, we have received feedback from around 50 practitioners. The need for all the classes and associations of the metamodel has been confirmed in at least one of the validation activities.

In terms of fit for purpose, the new version of the metamodel meets further industry requirements for the specification of safety compliance needs than the version in [13]. That version was adequate for the purposes initially analysed, but it does not meet e.g. all the requirements of OPENCOSS industrial case studies. OPENCOSS results have been developed and validated in three iterations [54], resulting in an incremental process where improvement opportunities were identified after each iteration. The initial version of the metamodel was specified and validated in the first iteration, whereas the current version is based on the final validation results.

The following subsections describe the systematic validation activities, presenting their research questions (RQs), data collection, results, discussion, and validity. We discuss validity according to the four perspectives proposed in [55]. We also present lessons learnt about using the RAF metamodel during the validation activities.

4.1 Modelling and analysis of safety standards

The first coordinated validation activity for the RAF metamodel was to analyse whether we could specify how to comply with different safety standards, according to their text. We first focused on standards from the application domains addressed in OPENCOSS (automotive, avionics, and railway), and afterwards analysed safety standards from other application domains (e.g. healthcare) or that had different overall purposes (e.g. product-based prescriptive standards). This has allowed us to cover a very broad range of safety standards and thus safety compliance needs.

4.1.1 Research Questions

The purpose of modelling and analysing safety standards was to establish whether the RAF metamodel supported the specification of industrial safety compliance needs. To this end, we formulated the following RQ.

RQ1. Can compliance needs in safety standards be specified with the RAF metamodel? This RQ was aimed at analysing the suitability of the metamodel for specifying safety compliance needs for different safety standards. This in turn allowed us to analyse the feasibility of applying the metamodel, and identify possible adjustments in the metamodel.

4.1.2 Data Collection

We analysed both system-level (e.g. EN 50126 for railway systems) and subsystem (e.g. EN 50128 for railway software) standards, and international (e.g. ISO 26262 for automotive) and national (e.g. MIL-STD-882E for the US) standards. We also considered the three main types of safety standards:

- Goal-based standards (e.g. Def Stan 00-56), which focus on the desired outcomes rather than the specific ways (e.g. techniques to use) to produce compliance evidence.
- Process-based prescriptive standards (e.g. IEC 61508), which focus on the processes to execute and the techniques to use in a system's lifecycle.
- Product-based prescriptive standards (e.g. ERA/ERTMS/003204), which focus on system features.

Appendix A lists all the standards analysed for validating the metamodel. Among all these standards, we modelled DO-178C, DO-297, EN 50126, EN 50128, EN 50129, ISO 26262, and a tailored DO-178. These safety standards, and the parts modelled from them, were selected because we needed them for validating OPENCOSS results in its industrial case studies. We examined the rest of the standards with the main purpose of discovering safety compliance needs that could not be specified with the RAF metamodel. More standards could have been modelled, but this would have required further resources in the project. We also consider that there is little value in modelling the simple parts of all the standards. The main value is to model the relevant parts for specific purposes (as for OPENCOSS industrial case studies) and to go through different standards, find aspects that are distinct, and try to model them. If it is not possible, then the metamodel must be revised. Hence some standards are modelled completely while others just examined.

The process for modelling the standards mostly consisted in reading the parts under consideration (i.e., those relevant for OPENCOSS industrial case studies), extracting the relevant information, and representing it in a RAF model. Several authors participated in the modelling of each standard, discussing and agreeing upon how to model the standards, and practitioners also provided feedback upon the validity of the models for the situations addressed in the case studies. This included the correction of mistakes, suggestions on how to represent some concepts (e.g. by means of reference activities instead of reference requirements), and the request to modify or include some elements. In some cases, practitioners created RAF models and excerpts on their own. Although most of the practitioners did not directly validate the metamodel but RAF models, their collaboration allowed us to identify aspects that could not be modelled with the metamodel or modelled as the practitioners preferred.

We kept a record of possible changes in the metamodel while modelling and analysing safety standards. This record also contained suggestions from other OPENCOSS partners, based on their experiences in using the metamodel in the industrial case studies and other pieces of work.

The validation in our previous publication [13] was preliminary and aimed to confirm that the initial concepts and relationships were present in the text of four safety standards (DO-178C, EN 50128, IEC 61508, and ISO 26262). The main differences in the validation with safety standards reported in this section lie in (1) the creation of models of parts of safety standards for specific purposes in the scope of OPENCOSS industrial case studies, (2) the involvement of practitioners in the creation process, and (3) the analysis of a higher number of standards, also from a higher number of application domains. Modelling of IEC 61508 is not presented in the validation of this paper because this standard was not used in OPENCOSS industrial case studies. Although we have created some partial models for the standard [13], these models have not been validated by practitioners in the scope of a specific assurance and certification situation.

4.1.3 Results

In total, the RAF metamodel has been validated with 37 safety standards from 11 application domains: aerospace, automotive, avionics, defence, healthcare, machinery, maritime, oil and gas, process industry, railway, and robotics. Table 2 shows the number of RAF elements (classes and associations) of the models of safety standards that have been created for OPENCOSS industrial case studies. Mandatory elements in a RAF model (e.g. *Reference Assurance Framework* and the owned artefact-RAF association for each *Reference Artefact*) are not included in the table to keep it as small and simple as possible.

The largest RAF models were created for EN 50128 and DO-178C, as a result of their detailed specification of reference requirements and of applicability information. This was necessary for the cross-domain case study. The model for EN 50129 is considerably smaller because it specifically focused on safety-targeted aspects (e.g. creation and management of a hazard log and a safety case), in order to complement the models for EN 50126 and EN 50128. The model for DO-297 aimed to complement the model for DO-178C with modular avionics architecture aspects.

4.1.4 Discussion

We discuss the answer to the RQ for the modelling and analysis of safety standards in this section.

RQ1. Can compliance needs in safety standards be specified with the RAF metamodel? It is clear to us that the answer to this RQ is affirmative. We have used 37 standards from 11 different application domains for the modelling and analysis of safety standards, including company-specific and national standards, and used both goal-based and prescriptive (product-based and process-based) standards. Therefore, we are sure that we have validated the RAF metamodel with most types of safety compliance needs in practice. Furthermore, practitioners have validated the models created for DO-178C, DO-297, EN 50126, EN 50128, EN 50129, ISO 26262, and tailored DO-178.

Table 2. RAF elements used in the models created (associations in italics)

Element	Standard						
	DO-178C	**DO-297**	**EN 50126**	**EN 50128**	**EN 50129**	**ISO 26262**	**Tailored DO-178**
Ref. Criticality Kind	1	1	1	1	-	1	1
Ref. Criticality Level	5	5	5	5	-	5	5
Ref. Applicability Kind	2	1	-	1	-	1	2
Ref. Applicability Level	5	3	-	5	-	4	5
Ref. Activity	54	15	28	58	11	79	31
sub activity	45	13	14	50	-	77	30
successor - predecessor	-	10	13	0	6	65	-
Ref. Role	-	-	5	10	-	-	-
activity - participant	-	-	31	50		-	-
Ref. Artefact	24	24	55	38	7	52	26
user - input artefact	10	10	22	17	8	59	-
producer - output artefact	13	24	54	71	10	55	-
Ref. Technique	-	-	-	-	-	5	-
Ref. Requirement	355	7	68	439	-	50	28
sub requirement	-	-	-	-	-	-	-
requirement - constrained element	284	5	68	583	-	43	7
Ref. Applicability	172	-	-	213	-	1	62
Ref. Criticality Applicability	616	-	-	1065	-	1	215
Total	**1541**	**118**	**350**	**2556**	**42**	**421**	**382**

We can further confidently state that the RAF metamodel supports the specification of safety compliance needs for most safety-critical computer-based and software-intensive systems. Based on the demographics of the surveys reported in [1,2], we estimate that the standards modelled and analysed and the domains addressed cover over 90% of the safety assurance and certification industry for these systems.

4.1.5 Validity

As discussed in the previous section, we are confident in the overall validity of the modelling and analysis of safety standards. The aspects addressed (e.g. number of standards analysed and their nature) strongly contribute to construct, internal, conclusion, and external validity. Several people have also participated in the creation of the models, and practitioners have validated the models.

We acknowledge that others might have created different RAF models for the same safety standards (see Section 4.3), thus the results could be different. Nonetheless, this is an inherent characteristic of safety standard usage. There is no single way to interpret and follow a safety standard, and system suppliers and regulators usually have to agree on how to comply with a standard for a given project [3]. In this sense, it is necessary that the RAF metamodel supports practitioners in interpreting standards (e.g. by indicating that reference requirements, artefacts, and activities should be identified) and allows them to model and communicate an interpretation. It would be counterproductive for the metamodel to force particular interpretations of safety standards.

Other people might pose new requirements for the RAF metamodel based on some specific safety compliance need, and the modelling and analysis of further standards might lead to the discovery of new requirements for the metamodel. We cannot guarantee that the RAF metamodel will support the specification of *any* safety compliance need, but are sure that its current classes and associations can be necessary for the specification of these needs, barring radical changes in the overall conception of safety assurance in future. As with any other model or metamodel (e.g. UML), the RAF metamodel might evolve in the future for meeting further safety compliance needs.

There is a threat of having missed some type of safety compliance need when modelling or analysing safety standards. In this regard, modelling the standards resulted in a very thorough reading and understanding of the text of the safety standards, thus it is less likely that we missed some compliance need. Nonetheless, the analysis of the rest of standards resulted in the discovery of new safety compliance needs and, in many cases, to adjustments in the RAF metamodel. We also considered regular feedback from OPENCOSS industrial partners. Indeed, most of the adjustments made from the version of the metamodel presented in [13] have been targeted at better fulfilling practitioners' expectations. Thus a combination of these three mechanisms has mitigated the threat of having missed some type of safety compliance need.

4.2 Workshop with practitioners

In addition to validating the RAF metamodel by modelling and analysing safety standards, we took advantage of a two-day OPENCOSS event in which partners received training on the use of the project's results.

4.2.1 Research questions

The purpose of the workshop was to assess whether practitioners would accept using the RAF metamodel. For example, we aimed to study if practitioners consider that the metamodel supports their current practices for specifying safety compliance needs and avoids or mitigates possible challenges. To this end, we formulated two RQs.

RQ2. Does the RAF metamodel meet practitioners' needs? This RQ aimed at studying the suitability of the metamodel by analysing if its main concepts are easy to understand, easy to identify in the text of safety standards, and can readily be used in safety assurance and certification projects. We regard these characteristics as the main ones that the RAF metamodel must ensure in order to enable its application in the industry. If the characteristics are not ensured, then the metamodel will not meet practitioners' needs.

RQ3. Do practitioners find benefits in using RAF models? This RQ aimed at studying if the models are considered useful and easy to use, and thus can help in mitigating or avoiding issues in the specification of safety compliance needs. If practitioners do not find benefits in using RAF models for specifying and structuring safety compliance needs, among other aspects, then it is unlikely that the metamodel will be adopted in the industry.

4.2.2 Data Collection

Data was collected during a workshop aimed at training OPENCOSS partners on the use of the project's results. These results included the RAF metamodel and the RAF modelling tool. Eight people attended the session related to RAFs, and five of them were practitioners. The main speaker was the first author, and the second author supported him. The session lasted around 2 hours and 30 minutes.

The session was divided into four stages. First, the purpose of a RAF, its main concepts, and practical considerations (see Sections 3.3 and 4.3) were presented. The main concepts are *Reference Assurance Framework*, *Reference Criticality Level*, *Reference Applicability Level*, *Reference Activity*, *Reference Role*, *Reference Technique*, *Reference Artefact*, *Reference Artefact Relationship*, and *Reference Requirements*. This stage lasted around 60 minutes. Second, the RAF modelling tool was introduced and a simple RAF model was collectively created as an example of how to use the tool. This stage took 30 minutes approximately. Next, the attendees received a description of the EN 50128 software integration phase and were given 30 minutes to represent its safety compliance needs with the RAF modelling tool. Finally, the speakers and the attendees discussed the models created and the experience in creating them for other 30 minutes. The models created did not only include instances of the main concepts but also of others (e.g. associations and *Reference Criticality Applicability*). Examples were presented throughout the session and the attendees could ask questions at any time.

After the session, we gave the attendees a short questionnaire to provide feedback on the RAF metamodel and RAF models. The questionnaire was created with close reference to related surveys [1,2,8]. It contained questions about:

- The respondents' background;
- The ease of understanding and identification of the RAF main concepts (strongly disagree, disagree, undecided, agree, strongly agree);
- The frequency of use of the concepts (never, few projects, some projects, most projects, every project);
- The expected benefits, challenges, and possible deficiencies in creating RAF models (strongly disagree, disagree, undecided, agree, strongly agree);
- The provision of additional comments and suggestions.

During the workshop, the attendees also made other comments on the RAF metamodel and its resulting models. We noted these comments and later analysed them and updated the metamodel accordingly. For example, we added the association between *Reference Role* and *Reference Artefact* based on one comment at the workshop.

4.2.3 Results

Four practitioners with experience in safety assurance and certification completed the questionnaire. Their background was as follows:

- Practitioner 1 was a safety assessor at a consultancy company, had more than 10 years and less than 5 projects, of experience, and had worked with DO-178, ISO 26262, CENELEC, and ECSS standards.
- Practitioner 2 was a safety assessor at a certification authority, had between 2 and 5 years and between 5 and 10 projects of experience, and had worked with CENELEC standards (EN 50126, 50128, and 50129) and with safety assessment regulations (EC 352 and 402).
- Practitioner 3 was a safety assurance manager at a manufacturer of final systems, had between 2 and 5 years and between 5 and 10 projects of experience, and had worked with ISO 26262
- Practitioner 4 was an engineer at a component supplier, had between 1 and 2 years and less than 5 projects of experience, and had worked with DO-178.

Fig. 4 shows the practitioners' opinion about the ease of understanding of the RAF main concepts and their ease of identification in the text of safety standards, as well as how often the practitioners had taken the concepts into account in safety assurance and certification projects. This information aims to answer RQ2. Most respondents agreed or strongly agreed upon ease of use and ease of identification, and had taken the concepts into account in most or every project. All but one respondent (Practitioner 3) were undecided about ease of understanding or ease of identification of some concept, two respondents reported use in every project (Practitioners 1 and 3), and only one respondent (Practitioner 4) reported use in few projects. Practitioner 4 was also the respondent that answered 'undecided' more times (seven out of 10), and this may be attributed to his short experience in the industry.

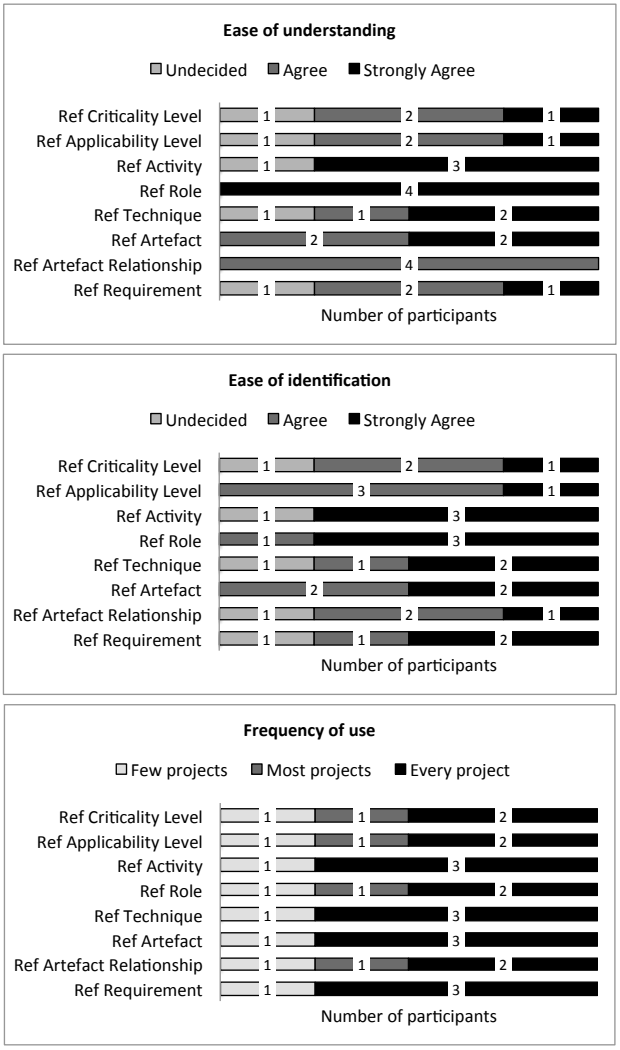

Fig. 4. Feedback on RAF main concepts

Regarding RQ3, Fig. 5 shows the practitioners' opinion about several statements on the ease of understanding, ease of use, and usefulness of RAF models. Most of the respondents agreed or strongly agreed upon most of the statements, only one respondent (Practitioner 1) strongly agreed upon some statement, and only one respondent (Practitioner 4) disagreed upon one statement. Two respondents (Practitioners 1 and 3) were not undecided about any statement, and Practitioner 4 again was the respondent that answered 'undecided' more times (three out of five). When asked to provide feedback on RAF models regarding the challenges when creating them, missing elements, and improvement suggestions, the participants mostly referred to possible improvements on tool support. The only change made on the metamodel from the feedback provided was the inclusion of an attribute (reference in *Reference Element*) to specify the part of a standard (e.g. a given clause) based on which a model element is created.

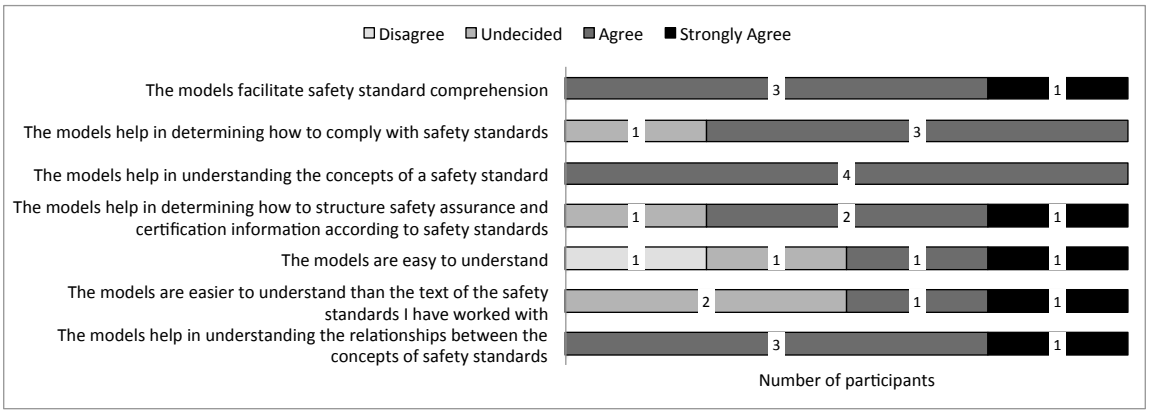

Fig. 5. Feedback on RAF models

4.2.4 Discussion

We discuss the answers to the RQs for the workshop with practitioners in this section.

RQ2. Does the RAF metamodel meet practitioners' needs? The results shown in Fig.4 provide evidence that the metamodel can meet practitioners´ needs. There was an overall agreement upon the ease of understanding and the ease of identification of the main concepts, which had also been used in most projects or in every project by the practitioners. The answers from Practitioner 4 can be regarded as more negative than the rest, but we think that the responses from the other practitioners are more valuable because they had wider experience in safety assurance and certification. The 'undecided' and 'few projects' answers from Practitioner 4 might be a result of his narrower experience. For example, he had only dealt with avionics software projects, and might not have had to use all the concepts.

RQ3. Do practitioners find benefits in using RAF models? The results in Fig. 5 show that practitioners find benefits, especially in safety standard comprehension, understanding of safety standard concepts, and understanding of the relationships between safety standard concepts. The median of only two statements ('The models are easy to understand' and 'The models are easier to understand than the text of the safety standards I have worked with') is lower than 'agree'. Although we explicitly requested the participants to answer independently of tool support-specific aspects, and based on the additional comments and suggestions, these lower medians might be a result of answering on tool support instead of the RAF models. As for RQ2, the more negative response from Practitioner 4 might have resulted from his narrower experience. The results are also in line with [8]. This publication analysed the possible use of an IEC 61508 conceptual model (i.e., a standard-specific safety compliance needs specification, which corresponds to a RAF model) for certification purposes with 12 practitioners. Most respondents indicated that the model was easy to understand, that they would very probably use the model to help in understanding the standard, and that they found the model simple enough to use for communication with a certification body.

In summary, the answers to RQ2 and RQ3, and also taking into account the results from modelling and analysing safety standards, suggest that the use of the RAF metamodel can be accepted in practice.

4.2.5 Validity

The main limitation of the validation through the workshop is the low number of practitioners that completed the questionnaire. Four participants are too few to draw strong conclusions (conclusion validity) and widely generalise the results (external validity). The relatively short duration of the workshop for performing several tasks (metamodel presentation, tool description, model creation, and discussion) is another limitation. Nonetheless, this validation activity was exploratory and aimed to complement the results from the modelling and analysis of the safety standards and the rest of feedback that we had previously received from practitioners. It must be further noticed that there is a general difficulty in obtaining participation from practitioners in research validation, and a specific difficulty in finding practitioners that can spend several hours on this activity. In addition, there are several aspects that make us believe in the relevance and value of the results from the workshop.

First, and based on the demographics of the surveys reported in [1,2], the four participants and their companies represent the main roles in safety assurance and certification of critical systems in the industry. We estimate from [1,2] that aerospace, automotive, avionics, and railway, and the standards mentioned by the respondents, correspond to around 70% of the industry of safety-critical computer-based and software-intensive systems. The participants also cover different ranges of experience in both years and number of projects. These characteristics mitigated threats to construct validity, and contribute to conclusion and external validity. Second, the feedback that the participants provided was based on the actual use of the RAF metamodel, not only on theoretical perceptions. This greatly contributes to conclusion validity.

Another limitation corresponds to the fact we did not ask about all the elements of the RAF metamodel, but asked only about the main concepts. This decision was aimed at focusing the questions on the most important concepts for the specification of safety compliance needs. It was also aimed at reducing the length of the questionnaire and thus mitigating possible threats related to participants' fatigue. The threats from providing incomplete lists of elements of the RAF metamodel were mitigated by allowing the participants to provide comments and suggestions in the questionnaire.

Last but not least, we do not consider that validation with only OPENCOSS partners could have led to result bias (e.g. more positive evaluation of the RAF metamodel). The participants are practitioners that are genuinely interested in the adoption and application of OPENCOSS results, thus they were aware of the importance of expressing their actual perspectives so that the metamodel fulfils their expectations.

4.3 Lessons learnt

The process of validating the RAF metamodel, via the modelling and analysis of safety standards and the workshop with practitioners, has allowed us to gain insights into the practicalities of creating a RAF model. We present the main practicalities by means of the following lessons learnt.

4.3.1 Difference between a RAF model and the text of a standard

RAF modellers must be aware of the fact that the text and structure of a standard does not exactly represent how to comply with it. The text of a safety standard is usually structured in sections, clauses, tables, etc., and sometimes it is not clear how certain needs have to be met in order to obtain compliance. In contrast, a RAF explicitly represents safety compliance needs and corresponds to a specific interpretation of the text and safety criteria of a standard, including the means of fulfilling these criteria. A direct, clear correspondence between the text of a standard and a RAF model does not always exist, but a modeller must analyse the standard to extract and classify the safety compliance needs specified. As explained in Section 2.2, this is the reason why existing safety regulation modelling approaches do not fulfil the objectives of the specification of safety compliance needs. For keeping traceability with the text of a safety standard, the reference of *Reference Element* should be used.

The information of a RAF can come from different parts of the text of a safety standard. For example, the standards usually present an overall lifecycle, but further reference activities might be identified in its clauses (e.g. in EN 50126). RAF modelling also implies the interpretation of a safety standard and of how to comply with it. If someone created for instance a RAF model for a goal- or product-based standard, decisions might be made in relation to the process to follow or the data to create for demonstrating compliance with the standard, even though such process and data were not explicitly requested by the standard. A key characteristic of the RAF metamodel is that it does not force a certain interpretation of a safety standard and thus mandate how to comply with it, but allows a user to represent his own interpretation.

4.3.2 Possible ambiguities, inconsistencies, and conflicts in RAF models

When modelling a RAF for a given safety standards, issues can arise regarding the existence of ambiguities, inconsistent information, or conflicting requirements in the text of the standard. Such issues must be resolved, and it must be decided, for instance, what alternative interpretation and thus specification is the most suitable one.

An agreement among those involved in a given safety assurance and certification effort (e.g. a system supplier and a certification authority) is advisable, and might even be necessary. Indeed, this agreement is necessary in most safety-critical domains. Otherwise, a certification authority might not agree upon how a safety standard has been followed. Systematic, model-based approaches for facilitating this agreement such as the one proposed in [3] can greatly help. Explicit models can assist in managing the complexities of reaching an agreement and can ease communication among the stakeholders.

4.3.3 Decomposition of reference activities and reference artefacts

Both reference activities and reference artefacts can be specified with different granularity levels. A reference activity can correspond to a system lifecycle phase and be later decomposed into other reference activities corresponding to sub-activities or tasks. A reference artefact can correspond to a document and be later decomposed into document constituents. For example, a software testing specification can be decomposed into test cases.

We do not provide detailed guidance about what an adequate granularity level would be for reference activities and artefacts. This will depend on the characteristics of a safety assurance and certification project, and even on the purpose for which a RAF model is used and who uses it. For example, a safety assurance manager might be mainly interested in artefact management at document level, such as a complete software requirements specification, whereas a system engineer might be interested in managing artefacts with lower granularity level, such as concrete low-level requirements for DO-178C. Nonetheless, we advise modellers to check existing guidance on process and data modelling (e.g. for traceability specification [10]) when deciding upon the necessary granularity.

4.3.4 Variability in reference assurance framework specification

There exists the possibility that different people will model how to comply with a safety standard in different ways. This depends on the perspective from which a standard is modelled, thus from which compliance will be addressed (e.g. process-based vs. requirements-based). For example, the content of some tables in some safety standards can be regarded as actions. The content of these tables could be represented in a RAF as reference activities or reference techniques, even as reference requirements. There also exists the possibility of differences between RAFs of the same safety standard because of differences in how the standard and its compliance needs are interpreted. In essence, the possible variability in RAF specification is mostly a consequence of the aspects presented in the previous lessons learned.

When creating RAF models collaboratively or for a common purpose (e.g. comparison of safety standards), we recommend that those involved in the effort reach an agreement upon how to model safety compliance needs. This will also indicate how a safety assurance and certification project will be executed and assessed (i.e. how compliance will be demonstrated). The process of creating a RAF model helps in reaching an agreement on these variations and thus leads to the creation of a common, shared interpretation for compliance.

5 Conclusion

Demonstration of compliance with safety standards, and thus determination of safety compliance needs, is essential for many critical computer-based and software-intensive systems. If it is not addressed properly, a system will not be allowed to operate. These activities can be very challenging, especially when a system is intended for deployment in various application domains. Therefore, approaches that facilitate compliance activities in these situations are necessary.

This paper has presented a metamodel for the specification of safety compliance needs for critical systems. The metamodel is generic, enables the specification of reference assurance frameworks (RAF), and abstracts concepts common to different application domains and standards. Unlike past work, the metamodel enables the holistic specification of safety compliance needs in the form of the requirements to fulfil, the data to manage, the process to execute, the relationships between these elements, and when and how the elements should be addressed for a given critical system.

The metamodel has been systematically validated by modelling and analysing safety standards and in a workshop with practitioners. We have also received feedback from practitioners in the context of other activities (e.g. OPENCOSS industrial case studies). The results from the validation make us

confident in the suitability of the RAF metamodel. They indicate that the metamodel can be used for the specification of safety compliance needs for most critical computer-based and software-intensive systems, and practitioners find benefits regarding the determination and specification of these needs. The resulting RAF models can also be more suitable than the text of the safety standards for understanding safety compliance needs, and thus for following the standards and complying with them.

We have further provided practical information for the use of the RAF metamodel by presenting usage scenarios, decisions made when creating the metamodel, and lessons learnt from creating RAF models. This information is very valuable for anyone interested in the metamodel, as it provides details about why to use the metamodel, when, and how, as well as possible issues that might appear and decisions to make. Therefore, we have provided guidance on how to apply the RAF metamodel, and thus on how to analyse safety standards and specify safety compliance needs.

We are currently using the RAF metamodel for the usage scenarios presented in Section 3.2. This will lead to the validation of other OPENCOSS results, such as the approach for cross-domain assurance. Many different pieces of work can be based on the RAF metamodel in the future. Among them, we plan to analyse the use of the metamodel in industrial projects, and whether it can be used for the specification of further assurance needs (e.g. security). We would also like to compare in depth goal-based and prescriptive standards by means of RAF models, and create links with OMG specifications, both on assurance (e.g. SACM [56]; Structured Assurance Case Metamodel) and on systems modelling (e.g. SysML [57]; System Modeling Language). All of these activities could allow us to find new refinement and extension opportunities on the metamodel, as it would be used in more situations, for different purposes, and by different stakeholders. Another area for future work is the improvement of the current tool support for RAF modelling. Finally, we plan to define guidelines for RAF modelling from the text of safety standards.

Acknowledgement. The research leading to this paper has received funding from the FP7 programme under grant agreement n° 289011 (OPENCOSS). The authors also thank those OPENCOSS partners who provided input for and feedback on the metamodel for reference assurance frameworks and on the models created.

Appendix A. Safety standards analysed

Table A.1 lists all of the standards analysed for validating the metamodel and outlines their purpose.

Table A.1. Standards used for validation

Standard	Purpose
AC 20-115C	FAA Advisory Circular for Airborne Software Assurance
AC 20-148	FAA Advisory Circular for Reusable Software Components
AC 20-170	FAA Advisory Circular for Integrated Modular Avionics Development. Verification, Integration and Approval
ARP4754	Guidelines for Development of Civil Aircraft and Systems
ARP4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
CAP 670 SW01	Air Traffic Services Safety Requirements
CLC/TR 50126-2	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Guide to the application of EN 50126-1 for safety
CLC/TR 50506-1	Railway applications - Communication, signalling and processing systems - Application Guide for EN 50129 - Part 1: Cross-acceptance
CLC/TR 50506-2	Railway applications - Communication, signalling and processing systems - Application Guide for EN 50129 - Part 2: Safety assurance
Def Stan 00-56	UK Safety Management Requirements for Defence Systems
DNV-RP-D201	Recommended Practice for Integrated Software Dependent Systems
DNV-OS-D203	Offshore Standard for Integrated Software Dependent Systems
DO-178C	Software Considerations in Airborne Systems and Equipment Certification
DO-254	Design assurance guidance for airborne electronic hardware
DO-297	Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations
ECSS-E-ST-40C	Space engineering – Software
ECSS-Q-ST-80C	Space product assurance - Software product assurance

EN 50126-1	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Part 1: Basic requirements and generic process
EN 50128	Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems
EN 50129	Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling
EN 50155	Railway applications - Electronic equipment used on rolling stock
EN 50159	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems
EN 50239	Railway applications - Radio remote control system of traction vehicle for freight traffic
EN 80001-1	Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities
ERA/ERTMS/ 003204	ERTMS/ETCS Functional Requirements Specification
ESA PSS-05-0 Issue 2	ESA software engineering standards
IEC 60601-1	Medical electrical equipment - Part 1: General requirements for basic safety and essential performance
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511	Functional safety - Safety instrumented systems for the process industry sector
IEC 62304	Medical device software – Software life-cycle processes
ISO 10218	Robots and robotic devices - Safety requirements for industrial robots
ISO 12100	Safety of machinery - General principles for design - Risk assessment and risk reduction
ISO 13485	Medical devices - Quality management systems - Requirements for regulatory purposes
ISO 13849-1	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
ISO 26262	Road vehicles – Functional safety
MIL-STD-882E	US Department of Defense Standard Practice for System Safety
Tailored DO-178	Avionics company-specific application of DO-178C

References

1. de la Vara JL, Borg M, Wnuk K, Moonen L. Survey on Safety Evidence Change Impact Analysis in Practice: Detailed Description and Analysis. Simula Research Laboratory, Technical Report 2014-18; 2014.
2. Nair S, de la Vara JL, Sabetzadeh M, Falessi D. Management of Evidence for Compliance with Safety Standards: A Survey on the State of Practice. Inf Softw Technol 2015;60:1-15.
3. Falessi D, Sabetzadeh M, Briand L, Turella E, Coq T, Panesar-Walawege RK. Planning for Safety Standards Compliance: A Model-Based Tool-Supported Approach. IEEE Softw 2012;29(3):64-70.
4. Nair S, de la Vara JL, Sabetzadeh M, Briand L. An extended systematic literature review on provision of evidence for safety certification. Inf Softw Technol 2014;56(7):689-717.
5. de la Vara JL, Nair S, Verhulst E, Studzizba J, Pepek P, Lambourg J, Sabetzadeh M. Towards a Model-Based Evolutionary Chain of Evidence for Compliance with Safety Standards. In: Ortmeier F, Daniel P, editors. SAFECOMP 2012 Workshops - LNCS 7613, Heidelberg: Springer; 2012, p. 64-78.
6. Baufreton, P, Blanquart JP, Boulanger JL, Delseny H, Derrien JC, Gassino J, Ladier G, Ledinot E, Leeman M, Quéré P, Ricque B. Multi-domain comparison of safety standards. In: In 5th International Conference on Embedded Real Time Software and Systems (ERTS 2010)
7. Alexander R, Kelly T, Gorry B. Safety Lifecycle Activities for Autonomous Systems Development. In: 5th SEAS DTC Technical Conference; 2010.
8. Panesar-Walawege RK, Sabetzadeh M, Briand L. Supporting the verification of compliance to safety standards via model-driven engineering: Approach, tool-support and empirical validation. Inf Softw Technol 2013;55(5):836-864.
9. Sannier N, Baudry B. INCREMENT: A Mixed MDE-IR Approach for Regulatory Requirements Modeling and Analysis. In: Salinesi C, van der Weerd I, editors. REFSQ 2014 - LNCS 8396, Heidelberg: Springer; 2014, p. 135-151.
10. Mäder P, Jones PL, Zhang Y, Cleland-Huang J. Strategic Traceability for Safety-Critical Projects. IEEE Softw 2013;30(3):58-66.

11. Briand L, Falessi D, Nejati S, Sabetzadeh M, Yue T. Traceability and SysML design slices to support safety inspections: A controlled experiment. ACM Trans Softw Eng Methodol 2014;23(1):9.
12. Habli I, Kelly T. A Model-Driven Approach to Assuring Process. In: 19th International Symposium on Software Reliability Engineering (ISSRE 2008), p. 7-16.
13. de la Vara JL, Panesar-Walawege RK. SafetyMet: A Metamodel for Safety Standards. In: Moreira A, Schätz B, Gray J, Vallecillo A, Clarke P, editors. MODELS 2013 - LNCS 8107, Heidelberg: Springer; 2013, p. 69-86.
14. OPENCOSS project. Deliverable D4.4 - Common Certification Language: Conceptual Model. Online, http://www.opencoss-project.eu/node/7; 2013.
15. Ferrari A, Gnesi S, Tolomei G. Using Clustering to Improve the Structure of Natural Language Requirements Documents. In: Doerr J, Opdahl AL, editors. REFSQ2013 - LNCS 7830, Heidelberg: Springer; 2013, p. 34-49.
16. Uusitalo EJ, Raatikainen M, Ylikangas M, Männistö T. Experiences from an industry-wide initiative for setting metadata for regulatory requirements in the nuclear domain. In: IEEE 7th International Workshop on Requirements Engineering and Law (RELAW 2014), p. 2-9.
17. Zoughbi G, Briand L, Labiche Y. Modeling safety and airworthiness (RTCA DO-178B) information. Softw Syst Model 2011;10(3):337-367.
18. Gribov V, Voos H. Safety oriented software engineering process for autonomous robots. In: IEEE 18th Conference on Emerging Technologies & Factory Automation (ETFA 2013).
19. Luo Y, van den Brand M, Engelen L, Favaro J, Klabbers M, Sartori G. Extracting Models from ISO 26262 for Reusable Safety Assurance. In: Favaro J, Morisio M, editors. ICSR 2013 - LNCS 7925, Heidelberg: Springer; 2013, p. 192-207.
20. Douglas BP. Real-Time Agility: The Harmony/ESW Method for Real-Time and Embedded Systems Development. Boston: Pearson Education; 2009.
21. Krammer M, Armengaud E, Bourroilh Q. Method Library Framework for Safety Standard Compliant Process Tailoring. In: 37th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA 2011), p. 302-305.
22. Porres I, Heidenberg J, Weijola M, Nordman K, Truscan D. Authoring IEC 61508 Based Software Development Process Models. In: Heidrich J, Oivo M, Jedlitschka A, Baldassarre MT, editors. PROFES 2013 - LNCS 7983, Heidelberg: Springer; 2013, p. 268-282.
23. Katta V, Stålhane T. A Conceptual Model of Traceability for Safety Systems. In: 2nd Complex Systems Design & Management Conference (CSD&M 2011).
24. Nejati S, Sabetzadeh M, Falessi D, Briand L, Coq T. A SysML-based approach to traceability management and design slicing in support of safety certification: Framework, tool support, and case studies. Inf Softw Technol 2012;54(6):569-590.
25. Kuschnerus D, Bruns F, Bilgic A, Musch T. A UML Profile for the Development of IEC 61508 Compliant Embedded Software. In: Embedded Real-Time Software and Systems 2012 (ERTS 2012).
26. Rupanov V, Buckl C, Fiege L, Armbruster M, Knoll A, Spiegelberg G. Employing early model-based safety evaluation to iteratively derive E/E architecture design. Sci Comput Program 2014;90(B):161-179.
27. Wu J, Yue T, Ali S, Zhang H. A modeling methodology to facilitate safety-oriented architecture design of industrial avionics software. J Softw: Pract Exp 2014 (accepted paper).
28. Mayr A, Plösch R, Saft M. Towards an Operational Safety Standard for Software: Modelling IEC 61508 Part 3. In: 18th IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS 2011), p. 97-104.
29. Sojer D, Knoll A, Buckl C. Synthesis of Diagnostic Techniques Based on an IEC 61508-aware Metamodel. In: 6th IEEE International Symposium on Industrial Embedded Systems (SIES 2011), p. 59-62.
30. Stallbaum H, Rzepka M. Toward DO-178B-compliant Test Models. In: Workshop on Model-Driven Engineering, Verification, and Validation (MoDeVVa 2010), p. 25-30.
31. Adedjouma M. Requirements Engineering Process according to Automotive Standards in a Model-driven Framework. PhD thesis, University of Paris Sud XI; 2012.
32. Müller JR, Drewes J, May J, Trog C. The Formal Representation of the Safety Case Processes described in the EN 5012x norms. In: International Railway Safety Conference (IRSC 2009).
33. Biggs G, Sakamoto T, Kotoku T. A profile and tool for modelling safety information with design information in SysML. Softw Syst Model 2014 (accepted paper).

34. Panesar-Walawege RK, Sabetzadeh M, Briand L. Using UML Profiles for Sector-Specific Tailoring of Safety Evidence Information. In: Jeusfeld M, Delcambre L, Ling TW, editors. ER 2011 - LNCS 6998, Heidelberg: Springer; 2011, p. 362-378.
35. Papadopoulos Y, McDermid JA. The potential for a generic approach to certification of safety critical systems in the transportation sector. Reliab Eng Syst Saf 1999;63(1):47-66
36. Zeller M, Höfig K, Rothfelder M. Towards a Cross-Domain Software Safety Assurance Process for Embedded Systems. In: Bondavalli A, Ceccarelli A, Ortmeier F, editors, SAFECOMP Workshops 2014 - LNCS 8696, Heidelberg: Springer; 2014, p. 396-400.
37. McCaffery F, Dorling A. Medi SPICE development. J Softw Maint Evol: Res Pract 2011;22(4):255-268.
38. Regan G, McCaffery F, McDaid K, Flood D. Medical device standards' requirements for traceability during the software development lifecycle and implementation of a traceability assessment model. Comput Stand Interfaces 2013;36(1):3-9.
39. eDiana project. Deliverable D6.3-B Specifications of Certification Metamodel. Online, http://s15723044.onlinehome-server.info/artemise/ediana_publicdocument.php; 2010.
40. Nair S, de la Vara JL, Melzi A, Tagliaferri G, de-la-Beaujardiere L, Belmonte F. Safety Evidence Traceability: Problem Analysis and Model. In: Salinesi C, van der Weerd I, editors. REFSQ 2014 - LNCS 8396, Heidelberg: Springer; 2014, p. 309-324.
41. Rempel P, Mäder P, Kuschke T, Cleland-Huang J. Mind the gap: assessing the conformance of software traceability to relevant guidelines. In: 36th International Conference on Software Engineering (ICSE 2014), p. 943-954.
42. Chung PWC, Cheung LYC, Machin CHC. Compliance Flow - Managing the compliance of dynamic and complex processes. Knowl Based Syst 2008;21(4):332-354.
43. Gallina B, Pitchai JP, Lundqvist K. S-TunExSPEM: Towards an Extension of SPEM 2.0 to Model and Exchange Tunable Safety-Oriented Processes. In Lee R, editor. SERA - SCI 496, Heidelberg: Springer; 2014, p. 215-230.
44. Verhulst E, Sputh BHC. An Unified Meta-model for Trustworthy Systems Engineering. In: Ortmeier F, Daniel P, editors. SAFECOMP 2012 Workshops - LNCS 7613, Heidelberg: Springer; 2012, 92-105.
45. Ankrum TS, Kromholz AH. Structured Assurance Cases: Three Common Standards. In: Ninth IEEE International Symposium on High Assurance Systems Engineering (HASE 2005), p. 99-108.
46. Cyra L, Górski J. SCF - A framework supporting achieving and assessing conformity with standards. Comput Stand Interfaces 2011;33(1):80-95.
47. Graydon P, Habli I, Hawkins R, Kelly T, Knight J: Arguing Conformance. IEEE Softw 2012;29(3):50-57.
48. Holloway CM. Making the Implicit Explicit: Towards an Assurance Case for DO-178C. In: 31st International System Safety Conference (ISSC 2013).
49. Holloway CM. Explicate '78: Discovering the Implicit Assurance Case in DO-178C. In: 23rd Safety-critical Systems Symposium (SSS 2015).
50. Luo Y, van den Brand M, Engelen L, Klabbers M. A Modeling Approach A to Support Safety Assurance in the Automotive Domain. In: Selvaraj H, Zydek D, Chmaj G, editors. Progress in Systems Engineering: Proceedings of the Twenty-Third International Conference on Systems Engineering - Advances in Intelligent Systems and Computing 330, Heidelberg: Springer; 2015, p. 339-345.
51. OPENCOSS project. Deliverable 4.6 - Implementation of the Reference Framework Editor and Manual. Online, http://www.opencoss-project.eu/node/7; 2013.
52. Olivé A. Conceptual Modeling of Information Systems. Heidelberg: Springer; 2007.
53. Pohl K. Requirements Engineering: Fundamentals, Principles, and Techniques, Heidelberg: Springer; 2010.
54. OPENCOSS project. Deliverable 1.4 - Implementation of Use Cases on Top of OPENCOSS Platform. Online, http://www.opencoss-project.eu/node/7; 2015.
55. Wohlin C, Runeson P, Höst M, Ohlsson MC, Regnell B. Experimentation in Software Engineering. 2nd ed. Heidelberg: Springer; 2012.
56. OMG. Structured Assurance Case Metamodel (SACM). Online, http://www.omg.org/spec/SACM/; 2015.
57. OMG. System Modeling Language (SysML). Online, http://www.omg.org/spec/SysML/; 2014.