Information and Software Technology 72 (2016) 16–30

Contents lists available at ScienceDirect

Information and Software Technology

journal homepage: www.elsevier.com/locate/infsof

Model-based specification of safety compliance needs for critical systems: A holistic generic metamodel

Jose Luis de la Vara [a,*], 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

ARTICLE INFO

Article history:
Received 15 June 2015
Revised 29 October 2015
Accepted 22 November 2015
Available online 10 December 2015

Keywords:
Safety-critical system
Safety standard
Safety compliance
Safety assurance
Safety certification
Reference assurance framework

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.

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.

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

* Corresponding author. Tel.: +34 91 624 91 15; fax: +34 91 624 91 29.
E-mail 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 (Á. López), idoya.delrio@tecnalia.com (I. del Río), tim.kelly@york.ac.uk (T. Kelly).

http://dx.doi.org/10.1016/j.infsof.2015.11.008
0950-5849/

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).