de la Vara J.L., Gómez Á., Gallego E., Génova G., Fraga A. (2017) Representation of Safety Standards with Semantic Technologies Used in Industrial Environments. In: Tonetta S., Schoitsch E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2017. Lecture Notes in Computer Science, vol 10489. Springer, Cham
Avalaible in https://doi.org/10.1007/978-3-319-66284-8_22

Representation of Safety Standards with Semantic Technologies Used in Industrial Environments

Jose Luis de la Vara[1], Álvaro Gómez[1], Elena Gallego[2], Gonzalo Génova[1], and Anabel Fraga[1]

[1] Departamento de Informática, Universidad Carlos III de Madrid, Spain
[2] The REUSE Company, Spain
jvara@inf.uc3m.es, alvarogomez.menendez@gmail.com, elena.gallego@reusecompany.com, ggenova@inf.uc3m.es, afraga@inf.uc3m.es

Abstract. Understanding and following safety standards with their text can be difficult. Ambiguity and inconsistency, among other issues, can easily arise. As a solution, several authors argue for the explicit representation of the standards with models, which can be created with semantic technologies such as ontologies. However, this possibility has received little attention. The few authors that have addressed it have also only dealt with a subset of safety standard aspects and have used technologies not usually applied for critical systems engineering. As a first step towards addressing these issues, this position paper presents our initial work on the representation of safety standards with Knowledge Manager, a tool used in industrial environments that exploits semantic technologies to manage domain information. The proposal also builds on prior work on the specification of safety compliance needs with a holistic generic metamodel. We describe how to use Knowledge Manager to specify the concepts and relationships of the metamodel for a given safety standard, and discuss the application and benefits of the corresponding representation.

Keywords: safety-critical system, safety standard, representation of safety standards, ontology, model, Knowledge Manager.

1 Introduction

Most safety-critical systems must comply with safety standards as a way of assuring that they do not pose undue risks. Examples of these standards [7] include IEC 61508 for a wide range of industries, DO-178C in avionics, EN 50128 in railway, and ISO 26262 in automotive.

Safety standards are typically large textual documents that consist of hundreds of pages and define thousands of criteria for compliance. The resulting complexity can hinder the comprehension of a standard. Ambiguity and inconsistencies are also usual in their text [6], and practitioners have indeed acknowledged issues in understanding and applying the standards [1][7]. This can lead to certification risks, as a system supplier might miss or misinterpret some criteria and thus not develop a compliant system. As a solution, several authors (e.g. [5]) argue that the use of structured representations of safety standards can help practitioners understand and follow them.

These representations have most often been UML or UML-based models such as a class diagram or a UML profile [2]. Nonetheless, the representations can also be developed with semantic technologies, e.g. as an ontology that includes the main concepts of a safety standard and the relationships between the concepts. Some authors have used this representation format in order to exploit semantic technology capabilities for safety assurance and certification.

Gallina and Szatmári [3] propose the creation of ontology-based models to ease the comparison of safety standards. They represent ISO 26262 and EN 50128 with OWL 2.0 and Protegé to later generate safety-oriented product lines in SPEM. The ontology focuses on the standards' activities. Jost et. al [4] propose the formalisation of ISO 26262 with an ontology to enable semi-automated selection of the standard's requirements. This way, ISO 26262 can be tailored to a given project. Jost et al. combine OWL and SPEM, and manage the ontology with Protegé and Pellet, focusing on the standard's terminology. Luo et al. [5] propose a model-based approach for compliance with safety standards and to facilitate assurance reuse. They use Protegé and OWLGrEd to specify and visualise, respectively, conceptual models of safety standards, and combine them with UML and SPEM. The approach is applied to ISO 26262, and the ontology focuses on the standard's terminology.

We find three main weaknesses in the state of the art. First, little attention has been paid to the use of semantic technologies to represent safety standards, thus its benefits (e.g. automatic reasoning) have been barely studied. Second, the proposed technologies have focused on specific aspects of the standards, namely their activities and terminology. Compliance however requires the consideration of more aspects [2], e.g. artefacts to manage and relationships between them. Therefore, no proposal has been made yet that provides an integrated ontological representation. Third, the semantic technologies adopted in the literature are seldom or not used in industry for critical systems engineering, which results in a gap between research and practice. We are not aware of any company using OWL or Protegé in real projects, and related studies on the state of the practice [1][7] do not provide evidence of their use.

We are working towards addressing these issues by investigating how Knowledge Manager [8] (KM) can be used to represent safety standards and later exploit the resulting representation. KM is a tool used in industrial environments for critical systems engineering to represent domain knowledge with ontologies. These ontologies cover several aspects, from system terminology to system specification patterns, and can be used for different purposes, e.g. system specification, system artefact quality analysis, and system information reuse. KM usage in practice focuses on system-specific characteristics, e.g. system structure, but we argue that such usage can be extended to support compliance with safety standards.

This position paper presents our initial work on the representation of safety standards with KM. We use as a basis an existing holistic generic metamodel to specify safety compliance needs [2]. We describe how the compliance information in a safety standard can be specified with KM according to the metamodel. This requires both a specific configuration of KM and the subsequent specification of the compliance information in KM. We further discuss how the resulting representation could be exploited to facilitate compliance with safety standards and related activities.

The rest of the paper is organised as follows. Section 2 presents our proposal and Section 3 discusses it. Section 4 summarises our main conclusions.

2 Proposal to Represent Safety Standards with KM

Our proposal to represent safety standards with semantic technologies is based on two main elements: KM, as supporting approach and tool for semantic specification of a standard's information, and a holistic generic metamodel for the specification of safety compliance needs. The metamodel indicates the element types that must be considered when having to demonstrate compliance with safety standards, as well as the relationships between them. The overall purpose of our proposal is to provide guidance about how a standard's terminology, data items of the element types, and relationships between the items can be represented with KM.

An excerpt of the metamodel is shown in Fig. 1. The metamodel supports the specification of the different types of safety compliance needs: information about safety assurance requirements, artefacts, and activities, and about their applicability. This also includes additional information about roles, techniques, artefact attributes, artefact relationships, and relationships between the element types. All the classes in the metamodel specialise Reference Element, and Reference Activity, Reference Artefact, Reference Role, and Reference Technique specialise Constrained Reference Assurable Element. Further information about the metamodel can be found in [2].

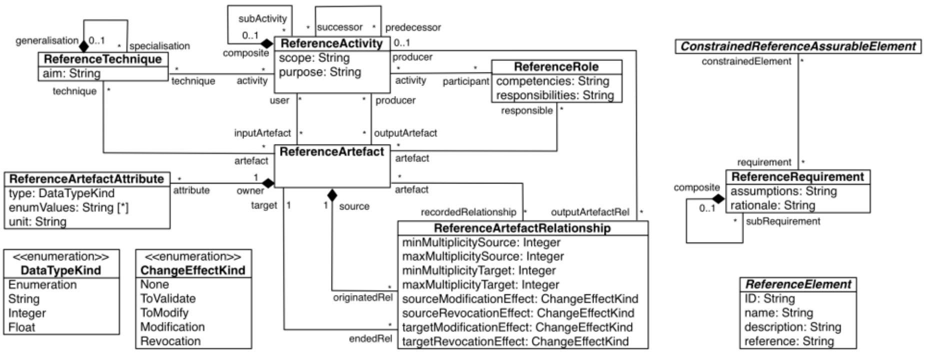


Fig. 1. Excerpt of the metamodel for the specification of safety compliance needs [2]

Fig. 2 shows the structure of an ontology in KM. An ontology consists of several layers, each depending on and extending the semantic information of the inner layer. The most inner layer (Terminology) corresponds to the terms of a domain together with their syntactic information. Relationships between the terms can be specified in the Conceptual model layer, as well as their semantics with clusters; e.g. the semantics of the terms 'car' and 'truck' can be 'system', and they specialise 'vehicle'. Patterns can then be developed to provide templates (aka boilerplates) for system information specification; the patterns refer to aspects of the two underlying layers. The Formalization layer includes information about how system information that matches a pattern will be semantically formalised and stored. Finally, at the Inference rules layer the data in all the other layers can be exploited for the specification of rules to derive new information, e.g. about the correctness of a system specification. At its current state, the proposal only deals with the Terminology and the Conceptual model layers. More information about these layers is provided in the next paragraphs when describing the proposal, and more information about KM is available in [8].

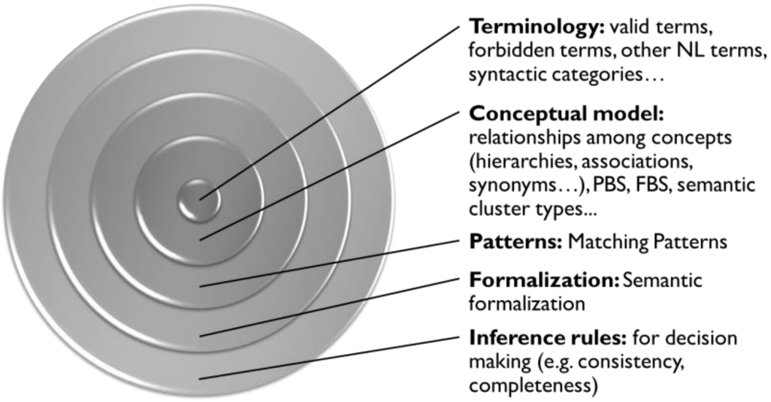

Terminology: valid terms, forbidden terms, other NL terms, syntactic categories…
Conceptual model: relationships among concepts (hierarchies, associations, synonyms…), PBS, FBS, semantic cluster types...
Patterns: Matching Patterns
Formalization: Semantic formalization
Inference rules: for decision making (e.g. consistency, completeness)

Fig. 2. Ontology layers in KM

The proposal consists of two main activities: KM configuration and specification of a standard's information. Each activity consists of several steps, as we explain below. We have already applied the proposal for certain parts of DO-178C, EN 50128, and ISO 26262.

1. KM configuration. This activity is necessary to tailor the default KM usage to represent safety standards, i.e. certain aspects of KM must be configured so that a user can create a suitable representation in accordance with the holistic generic metamodel. The configuration focuses on those semantic aspects of the standards that must be included in the representation. These aspects are specific to safety standards but independent of the specific standard to represent. Two tasks must be performed.

1.1 Specification of semantic clusters. New clusters must be added to the Conceptual model layer to be able to indicate the type of information that a term represents. First, a cluster with the name of the safety standard to be represented is necessary to later specify that a term falls within the scope of the standard. Second, semantic clusters must be added for Reference Artefact, Reference Artefact Attribute, Reference Activity, Reference Role, and Reference Technique, a cluster for each. These clusters are part of another new cluster called Reference Assurance Framework. The semantic clusters will be used to further categorise certain terms.

1.2 Specification of relationship types. KM also supports the specification of relationship types between terms. To represent a safety standard, a relationship type has to be created for each association in the metamodel between the metaclasses for which the new clusters have been added, e.g. for 'user-inputArtefact' between Reference Activity and Reference Artefact. This does not apply to the compositions, e.g. between Reference Artefact and Reference Artefact Attribute. KM has a predefined relationship type for composition, as well as for specialisation (to specify e.g. taxonomies) and for equivalence (to specify e.g. synonyms), among others. Another relationship type called 'Reference Artefact Relationship' must be added to be able to relate different Reference Artefacts in KM. The specification of the relationship types also includes the specification of the roles of the relationship ends.

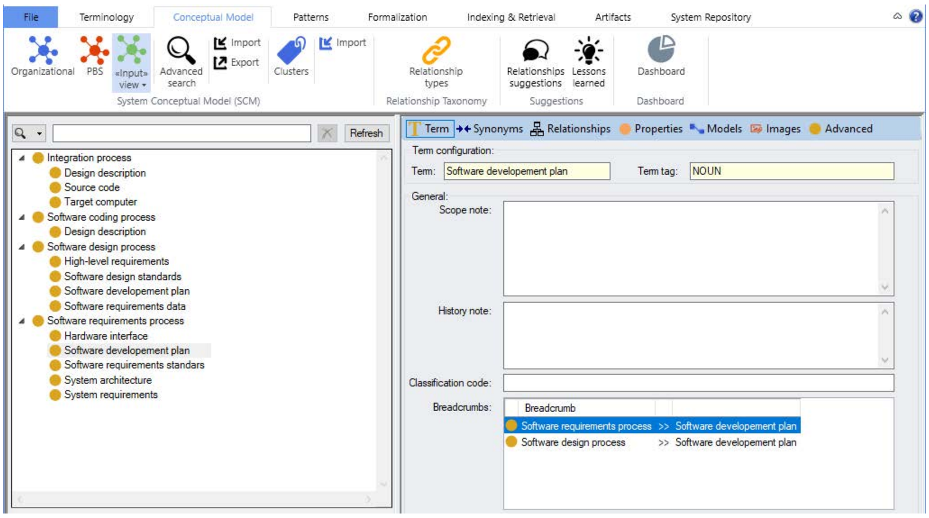
2. Specification of a standard's information. This activity results in the specific representation of a given safety standard. Two tasks can be distinguished. The tasks will usually be executed iteratively to incrementally represent a safety standard.

2.1 Specification of a standard’s terminology. This task has two main aspects to address. First, most standards have some glossary or vocabulary section. The corresponding terms and definitions, abbreviations, and acronyms must be added to the Terminology. Each time a term is added, it is necessary to (1) specify its syntactic category (e.g. noun or acronym) and (2) associate it with the semantic cluster that corresponds to the name of the standard; e.g. the term ‘algorithm’ would be added as a DO-178C noun. Next, the text of the standard must be analysed to identify terms that correspond to Reference Artefact, Reference Artefact Attribute, Reference Activity, Reference Role, or Reference Technique. Each time a term is identified, it is added to the Terminology and, in addition to the clusters for the glossary terms, the semantic cluster of the element type is associated; e.g. ‘Software Requirements Data’ is a DO-178C noun that also corresponds to a Reference Artefact.

2.2. Specification of the conceptual model of a safety standard. Once all the relevant terms have been introduced and classified, relationships between them can be specified in the Conceptual model. These relationships will be classified according to the available relationship types in KM, both the default ones and those created during KM configuration. A user must conform to the holistic generic metamodel when specifying relationships, i.e. only terms that correspond to the ends of a given association in the metamodel must be related. For example, ‘Software Requirements Data’ is an ‘output’ of ‘Software Requirements Process’ in DO-178C.

The user also needs to decide whether the relationships between Reference Artefacts should be specified as specialisations, as compositions, or with the Reference Artefact Relationship type. It is also possible to define specialisations of this relationship type if a user decides so, e.g. because it is a recurrent Reference Artefact Relationship. For instance, it is common that artefacts have to ‘conform to’ some plan or standard. Finally, it can also be necessary to specify specialisation and equivalence relationships between terms; e.g. ‘MC/DC’ and ‘Modified Condition/ Decision Coverage’ are equivalent for DO-178C.

Fig. 3 shows part of the resulting representation for DO-178C.



- ● Integration process
  - ● Design description
  - ● Source code
  - ● Target computer
- ● Software coding process
  - ● Design description
- ● Software design process
  - ● High-level requirements
  - ● Software design standards
  - ● Software developement plan
  - ● Software requirements data
- ● Software requirements process
  - ● Hardware interface
  - ● Software developement plan
  - ● Software requirements standars
  - ● System architecture
  - ● System requirements

Term configuration:

Term: Software developement plan

Term tag: NOUN

General:

Scope note:

History note:

Classification code:

Breadcrumbs:

Breadcrumb		
● Software requirements process	>>	Software developement plan
● Software design process	>>	Software developement plan

Fig. 3. Example of specification of a standard’s information with KM

3 Discussion

Once the proposal has been described, this section discusses how the representation of a safety standard with KM can be exploited for specific safety assurance and certification purposes. Within the overall purpose of demonstrating alignment or compliance with a safety standard, we currently envision six main possibilities to take advantage of the representations.

a) Quality analysis of the text of a safety standard. KM is part of a tool suite [8] that supports, among other features, system artefact quality analysis, including textual artefacts. More concretely, the suite can analyse artefact correctness, completeness, and consistency. Considering the text of a safety standard as an example of artefact, its text quality could be determined. This would be valuable because text quality is one of the most often weaknesses that practitioners find in safety standards. Parts that could be better specified or should be clarified could be identified.

b) System specification alignment. When specifying information for a specific system or analysing the information, the degree to which the specification is aligned with a given standard could be assessed. First, the system could be specified, e.g. its system requirement, according to patterns that refer to the semantic clusters added or to standard-specific terms. Second, an ontology of the system could be linked to the ontology of the standard, e.g. to specify that a given part of the system corresponds to the DO-178C component concept.

c) Compliance assessment. An ontology of a safety standard created with KM could be used to assess process and product compliance. The tool suite capabilities could be used to compare process or product information with the ontology, in order to determine compliance gaps. The information could correspond to artefacts of different nature: textual specifications, documents, diagrams, spreadsheets…

d) Comparison of standards. The text or ontology of a safety standard could be compared with the ontology of another, in order to identify commonalities and differences. This usage can be regarded as an extension of (a) and is similar to [3].

e) Reuse of compliant system information. If a system's information (e.g. a system model) is linked with the ontology of a safety standard to declare compliance with the standard, it would be possible to search for compliant system information and, when found, to reuse it. It could even be possible to analyse system information reuse between safety standards if the ontologies of the different standards are linked. The linking of a system's information with the ontology could be based on (b).

f) Specification of standard-specific metrics. Specific metrics could be designed within the Inference rules layer based on the semantic information of a safety standard represented in KM. The metrics could assess (1) general compliance with the standard (e.g. the amount of Reference Artefacts that have been provided) and (2) artefact-specific characteristics that a standard defines (e.g. architecture specification consistency). Although the metrics would often not be directly declared in the safety standard (e.g. for the latter example), the standards' information would drive their definition by indicating the areas for which metrics could be designed and possible aspects to consider.

We do not provide further details about the exploitation possibilities due to page limitations. How these possibilities can be finally enacted is part of our ongoing and future work, which might include the exploitation of further benefits.

4 Conclusion

The use of explicit structured representations of safety standards has been proposed to facilitate compliance with the standards, and semantic technologies can be used to create such representations. However, further work on the topic is necessary, and it must be linked with and based on industrial practices.

This position paper has presented our initial work towards representing safety standards with semantic technologies already used in industrial environments. We have described how to create ontologies of safety standards with the Knowledge Manager (KM) tool, and according to a holistic generic metamodel to specify safety compliance needs. The proposal consists of two main activities: KM configuration and specification of a standard's information. We currently envision six main usage scenarios: quality analysis of the text of a safety standard, system specification alignment, compliance assessment, comparison of standards, reuse of compliant system information, and specification of standard-specific metrics.

The proposal represents a novel usage of KM and an attempt towards bridging the gap, for safety assurance purposes, between the benefits that semantic technologies can enable and how they are used in critical systems engineering practice.

The proposal is at an initial stage and further work is necessary to fully develop it. We plan to enact the usages presented in Section 3, which might allow us to identify improvement opportunities. The new capabilities that KM will have in the future (e.g. libraries of ontologies) can also enable further usages. Finally, the work is being performed within the scope of AMASS (http://amass-ecsel.eu/), which is a large H2020-ECSEL industry-academia project on assurance and certification of cyber-physical systems. We will thus be able to apply the proposal in industrial case studies.

Acknowledgments. The research leading to this paper has received funding from the AMASS project (H2020-ECSEL no 692474; Spain's MINECO ref. PCIN-2015-262).

References

1. de la Vara, J.L., et al.: An Industrial Survey on Safety Evidence Change Impact Analysis Practice. IEEE T. Softw. Eng. 42(12), 1095-1117 (2016)
2. de la Vara, J.L., et al.: Model-based specification of safety compliance needs for critical systems: A holistic generic metamodel. Inform. Softw. Tech. 72, 16-30 (2016)
3. Gallina, B., Szatmári, Z.: Ontology-Based Identification of Commonalities and Variabilities Among Safety Processes. In: PROFES 2015, pp. 182-189
4. Jost, H., et al.: Towards a Safer Development of Driver Assistance Systems by Applying Requirements-Based Methods. In: ITCS 2011, pp. 1144-1149
5. Luo, Y., et al.: Extracting Models from ISO 26262 for Reusable Safety Assurance. In: ICSR 2013, pp. 192-207
6. Nair, S., et al.: An extended systematic literature review on provision of evidence for safety certification. Inform. Softw. Tech. 56(7), 689-717 (2014)
7. Nair, S., et al.: Evidence management for compliance of critical systems with safety standards: A survey on the state of practice. Inform. Softw. Tech. 60, 1-15 (2015)
8. The REUSE Company: https://www reusecompany.com/ (online)