An Environment-Driven Ontological Approach to Requirements Elicitation for Safety-Critical Systems

Jiale Zhou*, Kaj Hänninen*, Kristina Lundqvist*, Yue Lu*, Luciana Provenzano†, and Kristina Forsberg‡
*Mälardalen University, Västerås, Sweden
† Bombardier Transportation AB, Sweden
‡ Saab AB, Sweden
zhou.jiale@mdh.se

***Abstract*—The environment, where a safety critical system (SCS) operates, is an important source from which safety requirements of the SCS can originate. By treating the system under construction as a black box, the environment is typically documented as a number of assumptions, based on which a set of environmental safety requirements will be elicited. However, it is not a trivial task in practice to capture the environmental assumptions to elicit safety requirements. The lack of certain assumptions or too strict assumptions will either result in incomplete environmental safety requirements or waste many efforts on eliciting incorrect requirements. Moreover, the variety of operating environment for an SCS will further complicate the task, since the captured assumptions are at risk of invalidity, and consequently the elicited requirements need to be revisited to ensure safety has not been compromised by the change. This short paper presents an on-going work aiming to 1) systematically organize the knowledge of system operating environment and, 2) facilitate the elicitation of environmental safety requirements. We propose an ontological approach to achieve the objectives. In particular, we utilize conceptual ontologies to organize the environment knowledge in terms of relevant environment concepts, relations among them and axioms. Environmental assumptions are captured by instantiating the environment ontology. An ontological reasoning mechanism is also provided to support elicitation of safety requirements from the captured assumptions.**

I. Introduction

Safety-critical systems (SCSs) have become an intrinsic part of human daily life in multiple domains, such as automotive, avionics, and rail industries. Such systems are not only required to implement the functionality they should provide, but also have to satisfy a set of safety requirements in order to ensure the mitigation of hazardous consequences caused by system failure or malfunction in a certain environment. In this setting, requirements engineering (RE) is playing an essential role [1][2] in formulating the safety requirements ranging from declarative high-level to implementable low-level ones, and meanwhile the correctness of the safety requirements has to be ensured [3].

In our previous work, we have presented a method to break system-level safety requirements (high-level) down to software/hardware component requirements (low-level) based on Fault Tree Analysis (FTA) combined with a validation process [4], as well as have proposed approaches to early phase requirements validation via translating functionality and safety requirements into executable eTASM models [5][6]. These pieces of work contribute to detecting and mitigating hidden flaws of low-level requirements, counting on the assumption that high-level safety requirements are correctly elicited. Many popular methods such as goal-oriented approaches [7], scenario-based approaches [8], and FTA-based approaches [9] have been developed and experimented with to elicit high-level safety requirements. Nevertheless, these methods are too general, in the sense that they are for general problem domains. To achieve more efficient safety requirements elicitation, there is a need of an approach and tooling support that take full advantage of safety-related domain knowledge.

Our on-going work aims to alleviate this need, commercing with organizing the domain knowledge of system operating environment from the safety perspective. In particular, the environment where an SCS operates can either sporadically lead to system failures or be vulnerable to specific failures, and therefore it will inevitably impose a set of explicit or implicit safety requirements (referred as *environmental safety requirements*) to the system under construction [10]. By treating the system as a black box, such environment is typically defined and documented as a number of assumptions [10], based on which the imposed environmental safety requirements will be elicited. However, it is not a trivial task in practice to properly specify the environmental assumptions. The lack of certain assumptions or too strict assumptions will either result in incomplete safety requirements or waste many efforts on eliciting incorrect requirements. Furthermore, the properties of environment can vary a lot during the operation of an SCS, which makes the specified environmental assumptions at risk of invalidity. Consequently, the elicited requirements need to be revisited to ensure safety has not been compromised by the change. We believe that well-organized environment knowledge can to a large extent facilitate the specification of environmental assumptions and elicitation of environmental safety requirements.

Ontological modeling and semantic technologies provide a relatively recent yet mature basis that may support this organization purpose, which have been widely adopted in the area of requirements engineering, such as risk analysis [11], requirements specification [12] and verification [13], requirements management [14] and test case generation [15]. An ontology represents the effort to formulate an exhaustive and rigorous conceptual view within a given domain. The goal is to create an agreed-upon vocabulary and semantic structure

containing all the relevant concepts and their relations and axioms within that domain for the purpose of exchanging information and facilitating reasoning.

In this short paper, our main contributions are to propose an ontological approach to elicitation of environmental safety requirements and to illustrate it by a preliminary example. In particular, we start by collecting building blocks of environment ontology. We then develop conceptual ontologies to organize the environment knowledge in terms of relevant environment concepts, relations among the concepts and axioms. Environmental assumptions are subsequently captured by instantiating such an ontology. An ontological reasoning mechanism is also provided to support elicitation of safety requirements from the captured assumptions.

The remainder of this paper is organized as follows: Motivation is elaborated in Section II. Details and preliminary results of our ontological approach are described in Section III. Section IV introduces state-of-the-art of related areas, and finally concluding remarks and future work are presented in Section V.

.

II. Motivation

Safety critical systems (SCSs) are characterized by the impact they may have on the users or on the surroundings of the system. A failure, or an unforeseen event, occurring in an SCS could result in an accident that may cause harm to humans or damage to the environment. Risk assessment and management are a pair of requirements elicitation practices in the development of SCSs. Risk assessment serves to identify the possible hazards that could pose harm, to evaluate the consequences of hazards and to classify the risks of the system under construction. Risk management aims to define measures to mitigate the risks and elicit corresponding safety requirements that implement safe-states or safety-actions, in order to control and maintain the residual risk at a tolerable level.

In performing risk assessment and management, the term *system* typically refers to the combination of the system under construction and its operating environment. The system under construction must be defined in terms of its functions, boundaries, and interfaces, while the assumptions about the environment and the environmental properties should be explicitly identified to enable various analysis and further elicitation of environmental safety requirements [10]. For instance, a system for rail service commuting between two cities could consist of passengers, freight trains, different types of signaling and electrification sub-systems, tracks, platforms, tunnels, weather conditions, etc., as shown in Figure 1.

Consequently, an analysis performed on the system and the elicited safety requirements based on the analysis are only valid in the context of such environmental assumptions, i.e., the identified environment with its properties. Whenever the environment or its properties change (e.g., another two cities need the same type of commuter rail), the environment need to be re-identified and thus the set of requirements is also subject to change.

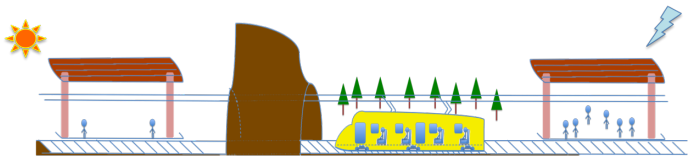

Fig. 1. A system for rail service commuting between two cities.

In this setting, we believe that it is necessary to develop an approach to organizing the knowledge of environment where SCSs operate, in order to facilitate:

- Modeling of complex environments with possibly varying properties. An example in the context of rail service could be the properties of tunnels which a train goes through. Some tunnels may provide evacuation possibilities in case of fire, whereas others may not. These types of properties are imperative to capture for analysis from the safety perspective.
- Early identification and elicitation of safety requirements. With the example of rail service system, the safety requirements that come in effect due to a fire may vary depending on the environment in which the fire occurs. A train on fire in a tunnel with evacuation possibilities could halt and allow passengers to get out from the train, whereas the same circumstance for the same train in another tunnel without evacuation possibilities would possibly have to provide enough torque to exit the tunnel. Thus different requirements may come in effect to mitigate the same type of hazard depending on the environment.
- Making the source of environmental safety requirements explicit, i.e., the set of safety requirements linked to specific environmental assumptions would be identifiable and traceable.
- Sharing common understanding of safety-related environment knowledge among different stakeholders. Taking the rail service as an example, the safety engineers may not realize that the evacuation exit of a tunnel is not available due to some reason in a certain case, while the rail operators can regard it as a common sense.
- Requirements management of generic products that may be deployed in varying type of environments. For instance, product lines are often based on generic subsystems that constitute the core functionality of the products. In addition to the core functionality, a customization and adaption of product is required for deployment in a safety context. An approach that allows early identification of the environmental safety requirements that come in effect due to customization and safety adaption would provide possibilities to better estimate the safety work required.

Based on these considerations, we propose an ontological approach to elicitation of environmental safety requirements,

which are introduced in Section III.

III. The Ontological Approach to Environmental Safety Requirements Elicitation

Ontology is a formal conceptualization of the domain of discourse. Typically, there are three kinds of facts about the domain stored in a domain ontology [16]: 1) *Concepts* represent entities with different properties in the problem domain, which can be material or immaterial and, 2) A *domain-specific relation* is a labeled directed connection between concepts of the domain and, 3) *Axioms* are used to model sentences that are always true, e.g., sub-class (which specifies that one concept is a sub-class of another concept) and equivalence (which expresses that two concepts having different names refer to the same entity in the domain) axioms. Recently, the use of ontologies in both industries and academia has gained popularity for two main reasons in the sense that 1) ontology facilitates knowledge organization and sharing and, 2) mature tooling supports like Protégé [1] have been provided for ontology editing and reasoning. In this section, we introduce our ontological approach to elicitation of environmental safety requirements, which makes full use of the benefits provided by ontologies to address the motivation in Section II. The approach consists of four steps as shown in Figure 2.

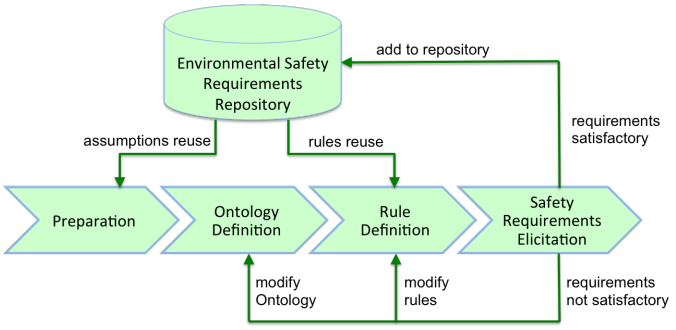

Fig. 2. An ontological approach to environmental safety requirements elicitation.

Step 1 ***Preparation****:* The first step is to collect building blocks of an environment ontology in terms of environmental assumptions from existing knowledge. The main sources of such building blocks include but are not limited to domain models from existing projects, domain standards, guidelines, safety checklists, domain taxonomies, industrial best practices, risk assessment reports, failure reports, experience of safety experts, etc. In our research, we are currently focused on the domain of automotive and rail. Figure 3 shows an excerpt of environmental assumptions checklist for passenger trains.

Step 2 ***Ontology Definition****:* The second step is to define ontology to organize environment knowledge based on collected environmental assumptions. The main tasks are to extract concepts of environment, define varying properties of the concepts, identify relations between them and specify axioms. Figure 4 depicts part of our preliminary environment

[1]http://protege.stanford.edu/

Typical Environmental Assumptions Checklist for Passenger Trains

- ☐ Open field without people
- ☐ Platform/station (underground, on ground level or elevated)
- ☐ Tunnel (with evacuation/ without evacuation)
- ☐ Steep hills/slopes/mountains
- ☐ In city with people and buildings
- ☐ Area with change of electrification (AC - AC, AC -DC, DC – AC)
- ☐ Development, parking, service and maintenance halls
- ☐ Testing facility, homologation tracks
- ☐ Railway crossings for people, cars and other vehicles (with and without signals)
- ☐ …

Fig. 3. An excerpt of environmental assumptions checklist.

ontology for automotive and rail domain. In brief, the ontology represents the following environment knowledge in the context of safety, including: 1) *Automotive/Rail System* (*ARS*) encounters a certain *Hazard* like *Fire* which happens in environment, or *Signal Interference* which is caused by environment, etc., and, 2) *ARS* runs on a certain *System Carrier* (*SC*), such as *Highway*, *Track*, etc., and, 3) *SC* can have various *Facility*, such as *Signal*, *Barrier*, etc., and, 4) *SC* is usually affected by different *Condition*, such as *Air Condition*, *Ground Condition*, etc., and, 5) *SC* is located in some *Area*, such as *Tunnel*, *Open Field*, etc., and, 6) *Tunnel* has a property of boolean type indicating if it has an evacuation exit or not and, 7) *Area* has *Building*, *Being*, etc.

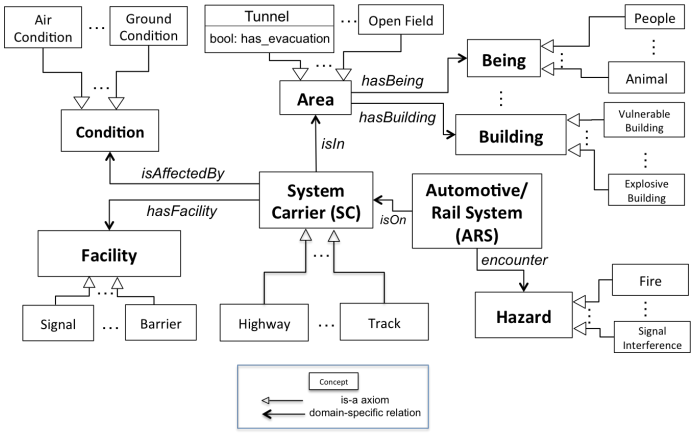

Fig. 4. A preliminary environment ontology for automotive and rail systems.

We are currently addressing several research questions to make the preliminary ontology more usable:

- What language is suitable to represent the ontology of environment from the safety perspective?
- What level of granularity and views are suitable to define the concepts of environment, for the purpose of safety requirements elicitation?
- How can we assure that axioms and relations between concepts are properly defined, for the purpose of safety requirements elicitation?

Step 3 ***Rule Definition****:* The third step defines reasoning rules based on the environment ontology. The reasoning rules intend to express the logic behind the environmental knowledge and safety requirements, which are written in simple *if-then-fi* form, i.e., **if** *given a set of environmental knowledge*, **then** *a corresponding safety requirement should be posed to the system under construction* **fi**". Based on the preliminary ontology introduced in the *Ontology Definition* step, an example of reasoning rule can be specified as shown in Figure 5:

```
if ARS isOn Track and Track isIn Tunnel
   and ARS encounter Fire,
then
    if Tunnel.has_evacuation = true
    then
       // a safety requirement in natural language
       "ARS should have independent brakes to stop and
       evacuate passengers."
    fi
    if Tunnel.has_evacuation = false
    then
       "ARS should have independent torque generators
       to exit the tunnel."
    fi
fi
```

Fig. 5. An example of reasoning rule

The reasoning rules can be inspired by the trace links between environmental assumptions and safety requirements in existing projects, or be formulated according to the experience and common sense possessed by safety experts.

Step 4 ***Safety Requirements Elicitation****:* The fourth step is safety requirements elicitation, which involves two tasks at first, i.e., 1) instantiating the ontology to represent the environmental assumptions that the system under construction has and, 2) performing reasoning to elicit environmental safety requirements. Assume that we are developing a passenger train that commutes between two countryside stations. A possible instantiation could be: passenger train as an instance of *ARS*, coach fire as an instance of *Fire*, rail track as an instance of *Track*, and mountain tunnel as an instance of *Tunnel* with *has_evacuation* property of *false* value. In this case, based on the reasoning rule specified in Figure 5, a safety requirement can be inferred that the passenger train should have independent torque generators to exit the tunnel.

Finally, the safety requirements will be validated to detect conflict or missing requirements. If the results are not satisfactory, we can go back to the *Ontology Definition* (Step 2) or *Rule Definition* (Step 3) step. The ontology and reasoning rules will be modified and updated accordingly. On the contrary, if the results are satisfactory, the pair of environment assumptions and safety requirement will be added to an *Environmental Safety Requirements Repository* to facilitate future elicitation.

IV. State of the Art

A. Safety-Critical Systems and Requirements Elicitation

Troubitsyna et al. [9] propose an approach to elicitation of safety requirements by utilizing the results of Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA). Furthermore, Du et al. [17] extend the traditional FTA with scenarios to elicit safety requirements. In particular, after performing the traditional FTA, a detailed state-based behavioral analysis, i.e., scenario analysis, is performed and the results will be integrated with the FTA results. In this way, safety constraints will be produced. Our work differs from theirs in the sense that our approach is to elicit environmental safety requirements based on the construction of environment ontology and corresponding reasoning rules.

Allenby et al. [8] present an approach to conducting hazard analysis on use cases requirements of the system under construction. In this way, safety requirements will be elicited, which are supposed to mitigate potential hazards. Comparing their work, our approach treats the system under construction as a black box and elicits the safety requirements originated from the environment.

B. Ontologies and Requirements Elicitation

Omoronyia et al. [18] investigate a rule-based approach to building domain ontologies by utilizing natural language processing techniques. Their approach can be integrated into ours, since we are building ontologies based on various documentary collections.

Kaiya et al. [19] present an requirements analysis and elicitation method based on domain ontologies. Given a domain ontology and a set of requirements mapped into the ontology, they define four metrics, i.e., correctness, completeness, consistency and unambiguity, to analyze the quality of requirements. If the quality is not sufficiently high, inference rules can help to elicit new requirements or modify existing ones. Their work is still too general to address the problems in SCS domain, but their metrics could be an option for our approach to validate requirements in the *Safety Requirements Elicitation* step.

Dzung et al. [20] propose an ontological technique to revise initial requirements in order to elicit new requirements and check the completeness and consistency of existing requirements. Different from ours, their work focuses on functional requirements that can be parsed into a set of short phrases of verb and noun.

Shibaoka et al. [21] proposed GOORE, an approach to goal-oriented and ontology-driven requirements elicitation. GOORE represents the knowledge of a specific domain as an ontology and uses this ontology for goal-oriented requirements analysis.

C. Ontologies and Safety-Critical System

Farfeleder et al. [16] present a tool-based method to requirements elicitation. In this work, a tool, DODT, can suggest attribute values of requirements templates (i.e., boilerplate) to requirements engineers. The suggestions originate from a given domain ontology. The DODT tool has been applied to a safety-critical control system to show its applicability [22].

Arogundade et al. [23] delve into the use of ontology for the formal representation of the use-misuse case domain knowledge for eliciting safety and security requirements, while our approach is to organize environment knowledge.

V. Conclusion and Future Work

In this short paper, we have introduced our on-going work that aims to facilitate safety requirements elicitation focusing on environmental aspects. To achieve this, we organize environment knowledge and have proposed a four-step ontological approach to elicitation of environmental safety requirements. In summary, our approach starts by collecting building blocks of environment ontology, and proceeds with defining an ontology to organize environment knowledge. The third step is to define reasoning rules to derive safety requirements from organized environmental knowledge. The final step is to instantiate the ontology to represent environmental assumptions for the system under construction, executing rules to elicit requirements, and validate the resulted requirements. If the results of validation are satisfactory, the pair of requirements and assumptions are added into a safety requirements repository for possible reuse.

Currently, we have built a preliminary environment ontology. Our next plan is to explore the questions formulated in the *Ontology Definition* (Step 2) step to improve the ontology. Moreover, we will delve into the possibility to substitute other languages for simple *if-then-if* form to specify reasoning rules in order to enhance the power of expressiveness. Another two pieces of work of interest are 1) to integrate our previous requirements validation technique into the fourth step of proposed approach and, 2) to extend our approach to include different safety-actions, thus improving the SCS fail-safe behavior in a broader environmental perspective. Finally, a tool will be provided to support our ontological approach, and we will validate our work with case studies on real railway systems.

References

[1] A. Ellis, "Achieving safety in complex control systems," in *Proceedings of SCSC'95*. Springer London, 1995, pp. 1–14.

[2] N. G. Leveson, *Safeware: System Safety and Computers*. NY, USA: ACM, 1995.

[3] D. Zowghi and V. Gervasi, "The three cs of requirements: Consistency, completeness, and correctness," in *Proceedings of REFSQ'02*, 2002.

[4] K. Forsberg, E. M. Isaksson, B. Gallina, K. Lundqvist, and A. Penna, "Elaboration of Safety Requirements," in *32nd Digital Avionics Systems Conference*, October 2013.

[5] J. Zhou, Y. Lu, and K. Lundqvist, "Towards Feature-Oriented Requirements Validation for Automotive Systems," in *Proceedings of RE'14*, August 2014.

[6] J. Zhou, Y. Lu, and K. Lundqvist, "A TASM-Based Requirements Validation Approach for Safety-Critical Embedded Systems," in *Proceedings of Ada-Europe'14*, June 2014.

[7] A. v. Lamsweerde, "Handling Obstacles in Goal-Oriented Requirements Engineering," *Journal of IEEE Transactions on Software Engineering*, vol. 26, no. 10, pp. 978–1005, 2000.

[8] K. Allenby and T. Kelly, "Deriving Safety Requirements using Scenarios," in *Proceedings of RE'01*, 2001, pp. 228–235.

[9] E. Troubitsyna, "Elicitation and Specification of Safety Requirements," in *Proceedings of ICONS'08*, 2008, pp. 202–207.

[10] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press, 2011.

[11] R. Gandhi and S.-W. Lee, "Ontology Guided Risk Analysis: From Informal Specifications to Formal Metrics," in *Advances in Information and Intelligent Systems*. Springer Berlin Heidelberg, 2009, vol. 251, pp. 227–249.

[12] F.-L. Li, J. Horkoff, A. Borgida, G. Guizzardi, L. Liu, and J. Mylopoulos, "From Stakeholder Requirements to Formal Specifications through Refinement," in *Proceedings of REFSQ'15*, 2015.

[13] I. Bicchierai, G. Bucci, C. Nocentini, and E. Vicario, "Using Ontologies in the Integration of Structural, Functional, and Process Perspectives in the Development of Safety Critical Systems," in *Proceedings of Ada-Europe'13*, 2013, pp. 95–108.

[14] N. Narayan, B. Bruegge, A. Delater, and B. Paech, "Enhanced Traceability in Model-Based CASE Tools using Ontologies and Information Retrieval," in *Proceedings of MARK'11*, Aug. 2011, pp. 24–28.

[15] G. Bonifacio, P. Marmo, A. Orazzo, I. Petrone, L. Velardi, and A. Venticinque, "Improvement of Processes and Methods in Testing Activities for Safety-Critical Embedded Systems," in *Proceedings of SAFECOMP'11*, vol. 6894, 2011, pp. 369–382.

[16] S. Farfeleder, T. Moser, and A. Krall, "Ontology-Driven Guidance for Requirements Elicitation," in *Proceedings of ESWC'11*, 2011, pp. 212–226.

[17] J. Du, J. Wang, and X. Feng, "A Safety Requirement Elicitation Technique of Safety-Critical System Based on Scenario," in *Proceedings of ICIC'14*, 2014, pp. 127–136.

[18] I. Omoronyia, G. Sindre, T. Stå lhane, S. Biffl, T. Moser, and W. Sunindyo, "A Domain Ontology Building Process for Guiding Requirements Elicitation," in *Proceedings of REFSQ'10*, 2010, pp. 188–202.

[19] H. Kaiya and M. Saeki, "Using Domain Ontology as Domain Knowledge for Requirements Elicitation," in *Proceedings of RE'06*, 2006, pp. 189–198.

[20] D. V. Dzung and A. Ohnishi, "Ontology-Based Reasoning in Requirements Elicitation," in *Proceedings of SEFM'09*, 2009, pp. 263–272.

[21] M. Shibaoka, M. Shibaoka, H. Kaiya, H. Kaiya, M. Saeki, and M. Saeki, "GOORE : Goal-Oriented and Ontology Driven Requirements Elicitation Method," *Advances in Conceptual Modeling - Foundations and Applications*, vol. 4802, pp. 225–234, 2007.

[22] T. Stålhane and T. Wien, "The DODT Tool Applied to Sub-Sea Software," in *Proceedings of RE'14*, 2014, pp. 420–427.

[23] O. T. Arogundade, A. T. Akinwale, Z. Jin, and X. G. Yang, "Towards an Ontological Approach to Information System Security and Safety Requirement Modeling and Reuse," *Information Security Journal: A Global Perspective*, vol. 21, pp. 137–149, 2012.