A pledge for safety-aware operational environment analysis

Daniel Hillen, Jan Reich

A pledge for safety-aware operational environment analysis

1st Daniel Hillen
Safety Engineering
Fraunhofer IESE
Kaiserslautern, Germany
daniel.hillen@iese.fraunhofer.de

2nd Jan Reich
Safety Engineering
Fraunhofer IESE
Kaiserslautern, Germany
jan.reich@iese.fraunhofer.de

***Abstract*—Safety engineering processes for automated driving systems (ADS) require representations of the operational environment. The operational design domain (ODD) is a fundamental artifact demanded by standards such as ISO 21448 and ISO 34503. The ODD specifies the environment in which the ADS operates. It therefore constraints under which conditions and in which environment the ADS can operate. The ODD is based on an ontology that describes relevant elements and aspects of the environment. Today, most ontologies that describe the public traffic environment aim to support validation and verification activities. However, the ODD must be considered by various other stakeholders and activities. The problem is that different activities focus on specific aspects of the environment so that one ontology cannot fit all. Therefore, it is necessary to tailor the ontology toward the specific activity. The tailored ontology must improve activity-specific quality criteria to provide a benefit over the original ontology. In this position paper, we want to motivate the need for practically applicable approaches to analyze operational environments for specific safety engineering processes. We discuss the benefits of a guideword-based method to tailor ontologies for safety engineering processes compared to purely data-based methods.**

***Index Terms*—Ontology, SOTIF, HARA, HAZOP**

I. Introduction

Safety engineering activities for automated driving systems must take into account elements and conditions of the environment. Therefore, standards such as the ISO 21448 (SOTIF) require defining a description of the environment in the form of the operational design domain (ODD). The ODD itself is therefore a fundamental artifact in developing and assuring ADS. Especially validation and verification activities rely on the ODD. Therefore, data-driven but also knowledge-based analysis methods are required according to EU regulations [1]. Today, most initiatives such as PEGASUS focus on developing data-driven approaches for assuring safety through testing and simulation. These data-driven approaches are necessary because the operating environment is too complex to be covered by knowledge-based methods only. Data-driven approaches can quantify realistic conditions but they are limited by the sample size that can never cover the whole situation space.

Due to the complexity of the operational environment, knowledge-based methods require a feasible environment model that is typically represented as an ontology. The ODD constrains the environment through conditions that refer to elements of the ontology. Various activities of different stakeholders have interfaces to the ODD [3]. However, different activities require different levels of abstraction of environmental elements. For example, a test engineer for a human detection algorithm needs to test the perception capabilities of humans with different colors of their clothes. The safety engineer, on the other hand, does not care about the color of the clothes for determining the risk of a hazard. These aspects are specified in an ontology. Stakeholders and their activities rely on specific quality attributes of the ontology, e.g., completeness. A safety engineer, e.g., must assume that the ontology is sufficiently complete so that the result of the related safety engineering process is sufficiently complete as well and no unacceptable risk is introduced. At the same time, the ontology should also be as simple as possible to reduce effort and to enable certain analyses which would become impractical for complex ontologies. Therefore, we conclude that one ontology is not enough to fulfill the need of all stakeholders and their activities. The challenge is therefore to tailor an ontology specifically toward a specific activity.

Today, engineers adapt ontologies ad-hoc without guidance so their confidence in these models is relatively low. Therefore, our research aims to define a guideword-based method to tailor existing environment models specifically toward a safety engineering activity. The goal is to tailor an ontology so that it specifies a) all relevant elements and b) only elements that are relevant to the activity. Therefore, it is a) most important for the safety-critical context of the activity while b) decreases the required effort and potentially even enables specific processes because the ontology remains of manageable size. In order to evaluate whether a tailored ontology is better, a quality criterion is necessary to measure the benefit in the context of an activity.

II. Guideword-based method

In today's knowledge-based safety engineering processes, guideword-based methods have been established successfully. Hazard analysis and risk assessment (HARA) are typically performed with the support of the HAZOP guidewords. Researchers also used HAZOP in the context of SOTIF and the identification of functional insufficiencies [5]. Failure analysis methods such as fault tree analysis can also benefit from

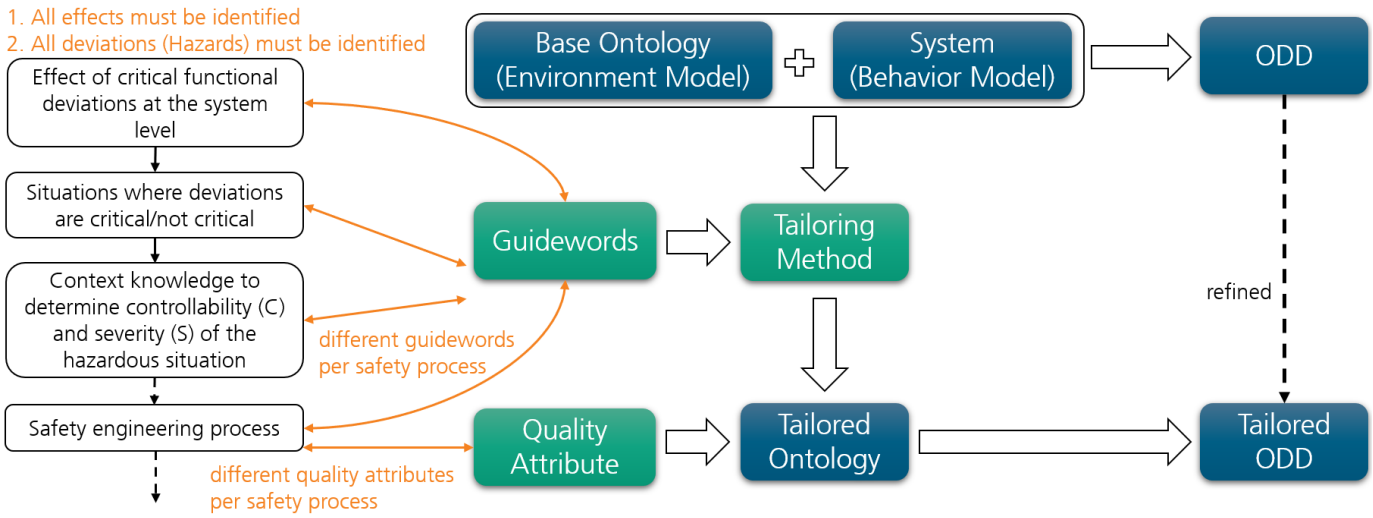

Fig. 1. Guideword-based tailoring of the environment

guideword-based approaches similar to HAZOP to automate processes [2]. While the HAZOP guidewords can be assumed to provide a certain degree of completeness in the safety analysis processes such as the HARA, they are very abstract to be applicable to environment elements. The SafeSpection framework provides a method to customize safety techniques using domain and project-specific guiding questions [4].

In our research, as illustrated in Figure 1, we develop a method to tailor an ontology specifically toward the needs of a safety engineer and its activities. Standardized and existing base ontologies should be tailored systematically toward a specific safety engineering process. The refined elements of the tailored ontology can be linked to the related base ontology elements to establish traceability. The ODD conditions can then also be refined based on the refined ontology to derive a tailored ODD.

Our tailoring method itself is based on guidewords so that engineers can apply them systematically to increase the quality of the ontology. These guidwords are not as generally applicable as those from HAZOP. They should rather be derived from a particular safety engineering process so that they are less abstract and more easily applicable to environmental elements. The goal of these guidewords is to provide (sufficiently) complete coverage so that engineers have high confidence in the method.

III. Quality of Ontologies

The tailoring of the ontology, as described before, must provide a better ontology. But what does ”better” mean in this context? Quality attributes for an ontology must be defined depending on the safety engineering process the ontology is used for. These quality criteria can be distinguished between absolute and process criteria. Absolute criteria provide an absolute value such as a certain percentage of coverage. Process quality criteria on the other hand require a method to be applied according to its specification to argue a certain quality level. For example, when performing a HARA according to ISO 26262 HAZOP is used to ensure that all hazardous events are identified due to the assumption, that the HAZOP keywords are complete. Absolute quality criteria are difficult to define for environment models due to the infinite situation space. A quality criterion for an ontology can be defined as

$$QualityCriterium = f(safetyActivity, system) <= X$$

That means that the quality of an ontology depends on the safety activity the ontology is tailored for. The environment model further depends on the behavior of the system and its capabilities. A system, that can fly requires different considerations than a car. Also, a vehicle in an urban environment differs from one operating on highways. The function f relates to an attribute such as coverage and must fulfill a threshold X.

In our research, we want to show that our tailored ontology is better than the original base ontology for a specific activity. This requires us to explore potential metrics and quality attributes to compare ontologies and determine the benefits of the tailored one. Another approach is to compare our guideword-based method to existing approaches such as HAZOP to systematically refine ontologies. In the context of HARA, HAZOP could be applied to ontology elements in combination with exposure, controllability, and probability. For example, pedestrians could be refined by looking for those that have lower controllability. While this could lead to sufficient refinement when applied by experienced engineers it might be too abstract and unintuitive to create a good ontology.

Acknowledgment

This work is funded by the project Layers Of Protection Architecture of Autonomous Systems (LOPAAS) funded by the Fraunhofer Gesellschaft

REFERENCES

[1] European Union (2022): Commission implementing regulation (EU) 2022/1426.

[2] Möhrle, Felix. “Automated Fault Tree Analysis by Composition of Type-Annotated Component Fault Trees.” Fraunhofer Verlag, 2023. https://publica.fraunhofer.de/handle/publica/437212.

[3] ASAM OpenODD Project, https://www.asam.net/standards/detail/openodd, accessed: 07.07.2023

[4] Denger, C., Trapp, M., Liggesmeyer, P. (2008). SafeSpection – A Systematic Customization Approach for Software Hazard Identification. In: Harrison, M.D., Sujan, MA. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2008. Lecture Notes in Computer Science, vol 5219. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-87698-4 _7

[5] Böde, E., Büker, M., Damm, W., Fränzle, M., Neurohr, B., Neurohr, C., Vander Maelen, S. (2019). Identifikation und Quantifizierung von Automationsrisiken für hochautomatisierte Fahrfunktionen.