Towards Integrating Ontologies into Verification for Autonomous Driving

Arut Prakash Kaleeswaran, Arne Nordmann, and Anees ul Mehdi
Robert Bosch Corporate Sector Research, 71272 Renningen, Germany

1 Introduction

With the recent boost in artificial intelligence, autonomous driving is one of the highly researched and invested areas. The focus of such work is not only constructing reliable (hardware) components but embedding intelligence into such components as well. For Bosch, a major supplier of automotive technologies, this has resulted in moving from being a components manufacturer to becoming a supplier of (sub-)systems that need to handle complex real-life scenarios autonomously. As these systems rely less on human intervention, verifying and assuring their intended behavior is of vital importance. However, classical formal verification methods focus on the functional integrity of the systems only. These methods do not take the complex context into account, which highly influences the behavior of these complex systems. In our approach, for the verification of requirements regarding their consistency with the external world, we complement formal model checking with ontologies: capturing the world knowledge and describing the system under test (SUT).

2 Requirement Verification: State-of-the-Art

We motivate our approach by considering a simple use case of an autonomous vehicle with components like radar sensors etc. Recently, pattern-based specification languages were adopted to describe the requirements for their model checking based verification. A *requirement* consists of conditions that need to hold under certain premises. As an example for SUT, we take the following requirement:

```
Globally, if {person} [is detected] then in response {brake}
[eventually initiated] within 5 time steps.
```

This requirement is then translated into a temporal logic. A model checker, provided with a description of SUT, is then used to check the consistency of SUT against this requirement. This approach has been successfully applied within Bosch as detailed by Post et al. [1] but it has some limitations: i) since the requirements are provided in a pattern-based language, a rather intrinsically error-prone step of translating the requirements to formal ones is required. Such translation needs to take the environment (external world) into consideration as well. In our example, the requirement engineer may opt for checking if a person is detected, the vehicle should brake. Meanwhile, in the SUT description, we may not have any notion of the concept Person and thus need to replace it by a native concept, say Obstacle. ii) if a requirement is not successfully verified, the traces (cause) of the inconsistency need to be translated back into a language

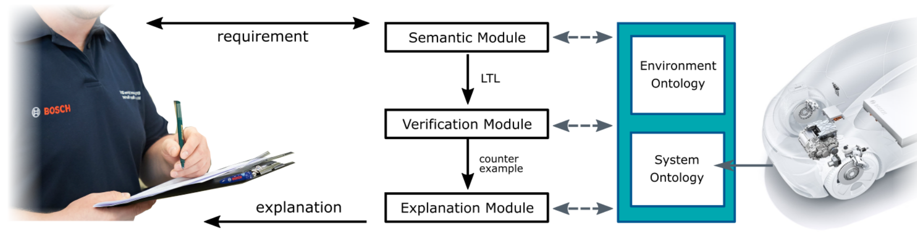

Figure 1. Overview of the proposed approach.

understandable to the requirement engineer. iii) manual checking of the plausibility of the requirements: the premises of a requirement rely on, say, an acoustic sensor which the SUT lacks.

3 Approach

We propose an approach that excels the state-of-the-art by addressing the aforementioned limitations. Figure 1 shows a conceptual view of our approach. At its core, the `Semantic Module` translates requirements using world knowledge (as captured in `Environment Ontology`) into formal representation. For example, suppose we have $\mathsf{Person} \sqsubseteq \mathsf{MovingObstacle}$, and $\mathsf{MovingObstacle} \sqsubseteq \mathsf{Obstacle}$ in the ontology[1]. Hence, using this information, the module translates the requirement into e.g, RTCTL expression: $\Box((\mathsf{obstacle}{:}\textbf{\textsf{true}}) \rightarrow \Diamond^{0..5}(\mathsf{brake}{:}\textbf{\textsf{true}}))$. This module also checks the plausibility of requirements against SUT using the mentioned ontologies. Suppose we have that the vehicle has a radar radarX capable of detecting static objects. This can be represented in `System Ontology` as $\exists \mathsf{detects.StaticObstacle}(\mathsf{radarX})$. Further, suppose that `Environment Ontology` contains $\mathsf{MovingObstacle} \sqcap \mathsf{StaticObstacle} \sqsubseteq \bot$. Based on these ontological information, the requirement is not plausible as SUT is incapable of detecting something which is a Person and hence a $\mathsf{MovingObstacle}$.

In `Verification Module`, a model checker is used for verifying the requirements. On encountering an inconsistency with a requirement, the counterexample generated by the model checker is provided to the `Explanation Module`. This module produces a natural language like explanation based on the counterexample using `Environment Ontology` and `System Ontology`.

4 Outlook

We presented a new approach based on ontologies for verification of requirements in autonomous driving. Such an approach broadens the verification scope compared to the classical ones. An ongoing task is the integration of `Semantic Module` with a `Verification Module`. A main research in our project focuses on `Explanation Module`. The idea is to generate explanations for the counterexamples in a natural-like language.

References

1. Post et al.: Formalization and analysis of real-time requirements: A feasibility study at BOSCH, VSTTE2012.

[1] We use description logic syntax to describe axioms in the ontologies.