CHALLENGES IN GENERATING AN ITEM DEFINITION FOR AN AUTOMATED DRIVING SYSTEM (ADS)

Robert Graubohm, Till Menzel, TU Braunschweig

An **ADS**, for which verification and validation methods are being investigated in the **VVM** project, represents a safety-relevant E/E system in a series production road vehicle and accordingly requires a functional specification in the form of an item definition in accordance with ISO 26262 [1]. The item definition is consulted by the further process steps in the automotive safety lifecycle, but as a living document it is also constantly supplemented and expanded within the concept phase [2].

For this purpose, ISO 26262 lists various requirements and recommendations for an item definition, including listing all known requirements, boundaries, and interfaces (cf. [1, Part 3, 5.4]). Yet, the **open context** in which an ADS operates poses a major challenge to a structured specification artifact. Incompleteness directly affects possible hazards, so that safety analyses that primarily focus on the item definition are likely insufficient. **VVM** is aiming to contribute to a solution of this problem.

Item definition of ISO 26262

A concrete challenge in the project context is the systemic complexity resulting from the definition of an **ADS** according to SAE J3016 [3, Sec. 3.2] as well as the extended scope of applicable processes and methods of verification and validation, whereas the requirements for an item definition in ISO 26262 are formulated independently of the system scope and a degree of automation.

In short, the two main objectives of an item definition according to ISO 26262 are (cf. [1, Part 3, 5.1]):

- to define **functions** to be developed and to describe **interactions with the environment**
- to ensure a common understanding of the system for **subsequent development activities**

SOTIF system specification

Since the SOTIF standard ISO/DIS 21448 [4] focuses on complex systems that provide safety-related functionality based on a sophisticated situational awareness, the guidance on system specification provided in Clause 5 is also a valuable input for performing an item definition for an **ADS**. There are key extensions named by the standard (cf. [4, Clause 5]); e. g.:

- Description of the Operational Design Domain (**ODD**)
- Vehicle-level **safety strategy**
- **Human-machine interaction**, including foreseeable misuse
- System **performance limitations** and countermeasures
- System **architecture** implementing the intended functionality
- **Degradation** and warning concept

CHALLENGES IN GENERATING AN ITEM DEFINITION FOR AN AUTOMATED DRIVING SYSTEM (ADS)

Sections of the example document developed in VVM based on preliminary work in the projects aFAS [5] and UNICARagil [6].

The figure illustrates sections of an **item definition** considered in **VVM**. Due to the project's focus on verification and validation activities and methods, not all sections will be elaborated; essentially, some information would require development decisions for an actual product. With regard to the prepared **item definition content**, a central role is assumed in the project context by the section "Domain description". The section outlines an initially targeted **ODD** and thus provides an interface between the **customer function** (cf. poster "Customer function") and the further advancement of the **ODD** (cf. poster "From OD over ODD"). The description of expected **conditions in the domain** and their limits is carried out in the document using the **6-Layer Model** [7]. Of less relevance, on the other hand, is the detailing of the system description within the document, since in the research project no specification of preliminary assumptions or requirements for the architectural design is intended by the item definition, and no integration of the intended functionality into a specific vehicle will be performed.

Literature

[1] *Road vehicles – Functional safety*, International Organization for Standardization Standard ISO 26262:2018.

[2] R. Graubohm, T. Stolte, G. Bagschik, M. Steimle, and M. Maurer, "Functional Safety Concept Generation within the Process of Preliminary Design of Automated Driving Functions at the Example of an Unmanned Protective Vehicle," in *Proc. 22nd Int. Conf. Engineering Design (ICED19)*, Delft, The Netherlands, 2019, pp. 2863–2872, doi: 10.1017/dsi.2019.293.

[3] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, SAE International Standard J3016 202104, 2021.

[4] *Road vehicles – Safety of the intended functionality*, International Organization for Standardization Standard ISO/DIS 21448:2021.

[5] T. Stolte, A. Reschka, G. Bagschik, and M. Maurer, "Towards Automated Driving: Unmanned Protective Vehicle for Highway Hard Shoulder Road Works," in *2015 IEEE Int. Conf. Intelligent Transportation Systems*, Las Palmas, Spain, 2015, pp. 672–677, doi: 10.1109/itsc.2015.115.

[6] T. Woopen et al., "UNICARagil - Disruptive Modular Architectures for Agile, Automated Vehicle Concepts," in *27th Aachen Colloq. Automobile and Engine Technology 2018*, Aachen, Germany, 2018, pp. 663–694, doi: 10.18154/RWTH-2018-229909.

[7] M. Scholtes et al., "6-Layer Model for a Structured Description and Categorization of Urban Traffic and Environment," in *IEEE Access*, vol. 9, pp. 59131-59147, 2021, doi: 10.1109/ACCESS.2021.3072739.

www.vvm-projekt.de   Twitter @vvm-project   LinkedIn VVM Project

Projektpartner