**Semi-Formal Contract-based Design for Safety-Critical Software in Software Defined Vehicles**

Matthias Größler / Olivier Bockenbach, FSQ Experts

Because it dissolves the old hardware centric notion of ECU based architectures, the Software Defined Vehicle (SDV) concept enables the creation of a wide range of configurations for a given product, based on the applications it hosts (e.g., a vehicle may or may not be equipped with a parking assistant). The versions of these applications can change rapidly, yet the safety of the overall product must remain guaranteed. Because every single combination of applications and their versions needs to be certified, it represents from a functional safety perspective a significant effort to keep the safety cases up to date. Changes made to a particular application version are documented through its specification, either with addition, modification or deprecation of requirements. When these requirements are expressed in natural language, it becomes difficult to assess the impact of the changes on the application, and therefore to evaluate the need for safety analyses, whose results are needed for the safety cases. The introduction of the SDV concept therefore requires new approaches to systematically ensure the completeness, correctness and consistency of those requirements. A key enabler for this is Contract-based Design (CBD) in combination with Semi-Formal Notation (SFN) and Semi- Formal Verification (SFV). Together, these methods enable precise yet practical specification and verification of component behavior in complex, distributed system architectures. Semi-Formal Notation (SFN) provides a structured and machine-interpretable way to describe component contracts based on assumptions and guarantees. It establishes a foundation for consistent integration across different engineering disciplines — from model-based system and software design to safety engineering and verification. The main challenge lies in striking the right balance between sufficient formal rigor for safety evidence (e.g., in line with ISO 26262, SOTIF) and industrial feasibility in everyday development. Semi-Formal Verification (SFV) addresses this challenge by applying methods that allow automated consistency checking and verification of defined contracts without requiring full formal proof. In order to verify functional and safety relevant aspects, it combines model-based simulation, property checking, and constraint-based analysis. The focus of those activities aims at the early detection of risks regarding integration and the overall safety of the system, long before they lead to costly errors in later development phases. Proper usage of CBD and SFN/SFV enables the implementation of Checkable Safety Cases (CSC) and their corresponding argumentation. Such CSCs allow immediate assessment of how changes made to an application affect the relevance of existing evidence in the safety case and highlight where context, assumptions, or goals in the argumentation require adjustments. The path from customer requirements to successful product certification involves numerous processes and steps. Some of these may also be

revised (e.g., the introduction of a new version of a technical guideline). The use of AI agents in the relevant processes can reduce the effort required to update affected artifacts and accelerate the certification process. This facilitates the seamless integration of new components needed for the SDV concept. Aiming at transitioning existing applications to SDV capable models, the challenge to reformulate existing specifications written in natural language to CBD/SFN can be addressed through the usage of small language models augmented with the appropriate context. In the SDV context, combining CBD, SFN, and SFV provides a pragmatic path toward verifiable, modular, and reusable software architectures. It ensures that functional safety, cybersecurity, and updatability are considered together throughout the vehicle lifecycle. This approach thus forms a crucial foundation for future European reference architectures, as targeted by initiatives such as ECAVA and ECLIPSE S-Core.