Contracts for Services in Software-Defined Vehicles

Prof. Dr. Mattias Nyberg, KTH Stockholm / Scania

The emergence of software-defined vehicles (SDVs) represents a paradigm shift in automotive software development — moving from system focus to service focus, where a service is not explicitly bound to an ECU or even to the vehicle itself. The result is open, dynamic ecosystems composed of distributed services. In this new context, service-based architectures and service-oriented systems engineering provide a foundation for integrating and evolving complex functionality across software, hardware, and even human interactions. A service view of all vehicle components — applications, actuator units, and sensor units — promotes a flat hierarchy where each element offers and consumes services. This enables horizontal service traceability in place of traditional vertical decompositions, fostering flexibility and modularity. However, such openness also demands rigorous specifications to ensure consistency and correctness across service interactions. This presentation explores how contract-based design and software contracts, in the form of pre- and post-conditions as used in ACSL (ANSI/ISO C Specification Language), can be employed to specify, reason about, and verify these service interactions. Formal contracts provide unambiguous interface definitions that capture both functional and non-functional expectations, enabling verification at multiple abstraction levels. Ambiguities that cannot be eliminated are instead managed explicitly through modeled dependencies.