ArchitectECA2030

Trustable architectures with acceptable residual risk for the electric, connected and automated cars

The mission of the project is related to the critical need for enhancing the safety and reliability of Electric, Connected, Automated (ECA) vehicles through mission-validated traceable design of electronic components and systems (ECS), quantification of accepted residual risk, and the development of an in-vehicle monitoring device. These innovations aim to establish a standardized approach for ECS design, ensure type approval with quantified residual risk, and introduce real-time health monitoring for electronic components. The envisioned outcome is the creation of safe, secure, and reliable ECA vehicles with well-defined and acceptable residual risk levels, paving the way for widespread adoption of these advanced automotive technologies.

Participation in ArchitectECA2030 project offered many benefits for AVL, that included the development of new methods, as well as making use of the competitive advantage in terms of engineering know-how within the company.

Within the scope of the project, AVL led the supply chains "Failure modes, fault detection and residual risk in actuator and propulsion systems", and "Global alignment and contribution to standards" and the work package "Validation of mission oriented electronic components and systems". Further AVL led and contributed to two demonstrators, the first one related to the supply chain "Formal-Model-based MonDev" and the second as part of the supply chain "Methods for monitoring and/or automated driving" with the title "Virtual Validation & Verification (V3) Framework".

The "Formal-Method-based MonDev" demonstrator focuses on creating advanced diagnosis and fault detection algorithms for ensuring the safe operation of high-voltage (HV) batteries in electric vehicles. This approach, applicable across various propulsion system components, utilizes a comprehensive physics simulation of the HV battery, incorporating virtual sensors, a thermal control unit, and a fault model. The co-simulation framework integrates the HV battery system with a vehicle and environmental model for realistic driving scenarios. A formal-method-based monitoring device identifies failures and constraint violations in the thermal control model, transforming detailed specifications into formal models for continuous monitoring throughout the system lifecycle, aiding in risk quantification.

The demonstrator "Virtual Validation & Verification (V3) Framework" is a virtual environment for validation and verification of ADAS/AD systems and SAE L3+ cars. The framework enables an efficient and deterministic process. To test developed methods, an AEB function was introduced as a basic system operated in the vehicle. The conducted co-simulation framework composed of a road network, traffic participants, and the vehicle utilizing the AEB function for testing the function. Thus, both safe and critical scenarios were executed to process the collected information with a novel analysis method, the CT-FLA (Combinatorial Testing and Fault Localization Analysis) approach to identify fault inducing critical simulation parameters.

During the project's efforts to globally align and contribute to standardization, most significant improvement was made on the topic of homologation / certification of future highly automated ECAs. In such complex systems, many different technical domains intertwine. Therefore, it was elaborated in the project that a harmonized definition and description of the residual risk as well

as standardization efforts will enable critical improvements during the future development of such cars – regarding both safety and security. Furthermore, the reference homologation process was described as a method-based approach to enhance efficiency, cross-domain safety argumentation, and prove compliance with applicable regulations & standards to relevant authorities or technical services in an iterative manner.