

# ArchitectECA2030

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

The project will implement a unique in-vehicle monitoring device able to measure the health status and degradation of the functional electronics empowering model-based safety prediction, fault diagnosis, and anomaly detection. A validation framework comprised of harmonized methods and tools able to handle quantification of residual risks using different data sources (e.g., monitoring devices, sensor/actuators, fleet observations) is provided to ultimately design safe, secure, and reliable ECA vehicles with a well-defined, quantified, and acceptable residual risk across all ECS levels.

## Project Facts

Project Coordinator:  
Dr. Georg Stettinger  
Infineon Technologies Germany AG

Project Start: 01.07.2020  
Duration: 36M  
Total investment: ~€M 13  
Requested EU contribution: ~€M 4  
Requested National cont.: ~€M 3

Participating organizations: 20  
Number of Countries: 8

## Vision

To provide a harmonized pan-European validation framework enabling mission-oriented validation of electronic components and systems (ECS) for electric, connected and automated (ECA) SAE L3 to L5 vehicles to improve reliability, robustness, safety and traceability.

## Goals

- Manage failures, uncertainties, and misbehaviors across all layers (sub-components, components, sub-systems, and systems) propagating through the entire ECA vehicle stack.
- Develop a harmonized homologation framework, including methods, tools and processes to design safe, secure and reliable ECA vehicles with acceptable residual risk.
- Develop a concept for an in-vehicle monitoring device (MonDev) to identify the health status and possible degradations across all layers (sub-components, components, sub-systems and systems).
- Bring together the representative stakeholders (ECS value chain, standardization, certification).

## ArchitectECA2030 Objectives

**O1:** Continuous robust design optimization for each part in the Electric Components and Systems (ECS) value chain.

**O2:** Framework for safety validation of ECS value chain.

**O3:** Identification & management of residual risks over the entire ECS value chain.

**O4:** End-user acceptance by trustworthy ECS value chain.

**O5:** Zero emissions, zero crashes, zero congestions by ECA2030-car.

## PROJECT STRUCTURE

### Work Packages

- WP1** Requirements and targets
- WP2** Methods, architectures, models and tools for validation framework
- WP3** Components and sub-systems enabling virtual development and validation
- WP4** Identification and management of risks in automotive ECS
- WP5** Integration of the residual risk framework
- WP6** Validation of mission oriented ECS
- WP7** Twinning, dissemination, exploitation
- WP8** Project management and liaison.

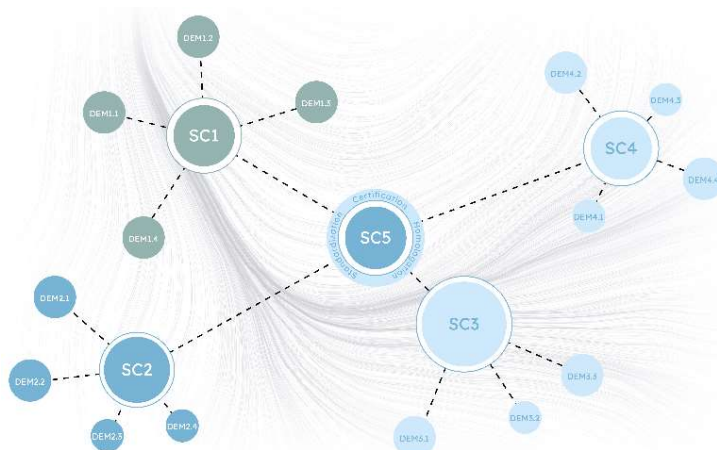


Fig. 1 ArchitectECA2030 SCs synergies

### Supply Chains

**SC1** Failure modes, fault detection and residual risk in acquisition and perception systems

**SC2** Failure modes, fault detection and residual risk in actuator and propulsion systems

**SC3** Failure modes, fault detection and residual risk for safety and security in connectivity systems

**SC4** Methods for monitoring and/or automated driving

**SC5** Global alignment and contribution to standards.

### WP1: Requirements and targets

In 2022, WP1 ended with the completion of the tasks and the related deliverable that defined, listed and described the requirements for standardization methods and metrics to ensure the quality of the certification process. ArchitectECA2030 partners provided a comprehensive overview of international efforts regarding vehicle homologation, starting from the vehicle perspective. An explanation was presented on how these international efforts are covered by treaties that themselves influence the rules and regulations of individual states resp. of the European Union. Furthermore, the link from international treaties to technical standards was shown. In combination with a collection of many relevant standards and an overview of currently running European projects, a well-balanced picture of the state of the art and the potential implications and challenges for semiconductor companies were outlined, supplementing the ‘pure’ vehicle perspective.

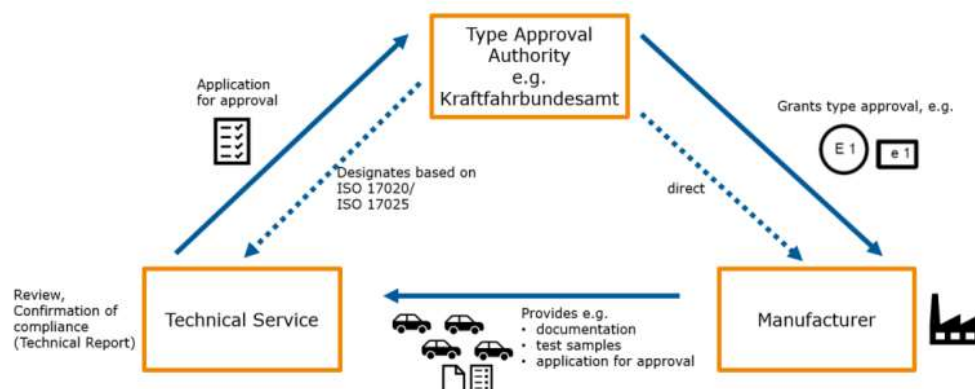


Fig. 2 The Concept of "Third-Party Certification"

### WP2: Methods, architectures, models and tools for validation framework

The main effort in WP2 was on the “Report on architecture for validation of perception systems” for automated driving. WP2 involved partners have discussed and unified the descriptions of terminology for key concepts such as architecture, framework, and methodology to have a common understanding. A concept of a hierarchical system and architecture for a Monitoring Device or Monitoring Function was developed. WP2 also focused on the Residual Risk classifications as well as a definition of safety levels, considering related standards such as ISO 26262, SOTIF, etc.

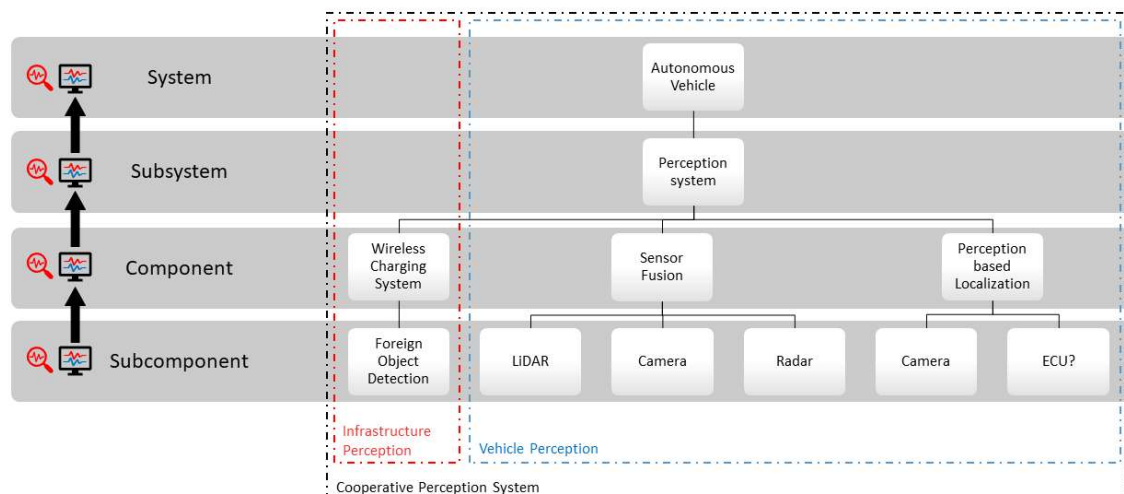


Fig. 3 Hierarchical Monitoring Overview



### WP3: Components and sub-systems enabling virtual development and validation

In WP3, the first tools and methods for virtual validation of corresponding perception systems were identified and presented. Significant progress was made in defining virtual simulation environments for ACC/LKA applications and foreign object detection for wireless charging. Furthermore, a first risk assessment methodology was conceived to be used for real-time monitoring functionality. In parallel, a software architecture for middleware to run on an MCU was developed, and the first prototype implementation was defined. To define tools for fault detection or prediction, as well as for the validation of the power inverter component in a vehicle transmission and an HV battery thermal controller, in this period, the individual components were implemented as models and tools. Test instrumentation was developed to acquire data from an IGBT device for further simulations. The main focus was on coming up with testing methodologies for autonomous and automated systems, including monitoring. For the virtual validation, the use of combinatorial testing for optimizing the overall testing process was suggested and discussed among task partners. In addition, the first work on verifying and validating a monitoring device has been suggested, which is based on metamorphic testing and other properties.

### WP4: Identification and management of risks in automotive ECS

WP4 deals with the identification of risks that correspond to automotive ECS, where the goal is to come up with a framework for risk classification and methodologies for identifying and evaluating risks both at design time and during operation. The consortium started a discussion on the classification of risks and decided on the next steps within WP4. Moreover, further presentations and discussions regarding the use of combinatorial testing for risk identification, ideas of using probabilistic model-checking, and secondary risks when introducing monitoring devices were done. All tasks actively have been working on risks and residual risks as well as secondary risks related to their demonstrators and monitoring devices.

---

*The residual risk framework is expected to reduce safety threats such as residual risk of the intended function, through analysis, unintended behavior in known situations through verification, residual unknown situations that could cause unintended behavior, through validation of verification situations.*

---

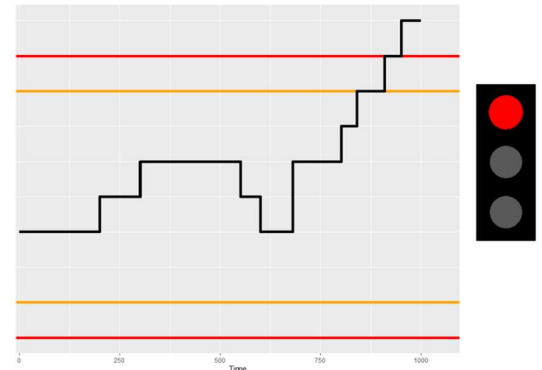
### WP5: Integration of the residual risk framework

WP5 focuses on the integration of a common residual risk framework by considering the residual risk identification and the methodologies and metrics developed for the automated and connected vehicles perception, cognition, connectivity, and propulsion domains (Sense, Think, Connect, Act) using available tools and prototype methods to support virtual validation. The residual risk framework is expected to reduce safety threats such as residual risk of the intended function, through analysis, unintended behavior in known situations through verification, residual unknown situations that could cause unintended behavior, through validation of verification situations. The common framework for residual risk analysis will be based on an extended V-model. ASIL is a risk classification scheme defined in ISO 26262, where ASIL-D refers to the highest classification of initial hazard and the most stringent level of safety measures for avoiding an unreasonable residual risk. During the residual risk analysis in WP4/WP5 we identified a gap in the standards and see a possible need for a new automotive safety integrity level. ASIL-E as a new proposal has been discussed and is under preparation. Identification, definition, and description of the monitoring devices (MonDev) for the demonstrators are ongoing.

### EuWoRel 2021 conference

On the 13<sup>th</sup>-14<sup>th</sup> of October, dr. Horst Lewitschnig representing ArchitectECA2030 partner Infineon Technologies Austria AG, participated in the 9th European Expert Workshop on Reliability of Electronics and Smart Systems, EuWoRel 2021, in Fraunhofer-Forum, Berlin.

During the conference, dr. Horst Lewitschnig presented “A Lifetime Drift Model for Discrete Parameters”. The main goals of this model are to guard banding, drift detection, and calculation of remaining useful lifetime. The model must handle calculations for a large number of parameters within a reasonable time and should be used on the edge devices.



### AEIT Automotive 2021

On 18<sup>th</sup> of November, 2021 dr. Cristina De Luca represented the project at a virtual International Conference on Electrical and Electronic Technologies for Automotive (AEIT Automotive 2021). Participants of the event had the opportunity to listen to the project-related presentation “Electric, connected and automated vehicles, what about Risk, Trust, and Failure?”



Vehicle automation is emerging in many forms and has many social implications. In order to take full advantage of emerging technologies, electric, connected and automated (ECA) vehicles need to be trustworthy. People must feel safe and want to use and buy new services that ECAs open up to them. Consequently, there is a strong need for independent and reproducible validation of automated vehicles even though it has to deal with non-deterministic elements.

The ArchitectECA2030 goals are to manage failure modes, uncertainties, and failure probabilities, propagating through the entire ECA vehicle stack consisting of on-board HW, on-board SW, off-board SW and data, development and validation methodologies, to support hazard identification, risk analysis, and sufficient risk mitigation.

### Upcoming Events

- 17.03.2022** Industry Strategy Symposium Europe (ISS Europe)
- 14-23.03.2021** Design, Automation, and Test in Europe (DATE) Conference 2022
- 27-29.03.2022** Machine Learning Prague 2022
- 6-9.04.2022** The 40<sup>th</sup> EPoSS Annual Meeting 2022
- 23-24.04.2022** ICEEVT 2022, International Conference on E-mobility and Emerging Vehicular Technology
- 26-28.04.2022** Smart Systems Integration Conference and Exhibition 2022
- 20-22.06.2022** HiPEAC 2022
- 23-29.07.2022** IJCAI-ECAI 2022, The 31<sup>st</sup> International Joint Conference on Artificial Intelligence





## FUNDING

ArchitectECA2030 project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 877539. The JU receives support from the European Union's Horizon 2020 research and innovation programme. It is co-funded by the consortium members and grants from Germany, Netherlands, Czech Republic, Austria and Norway.

