ArchitectECA2030

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

The developments of electric, connected, and autonomous vehicle technologies aim to provide comprehensive social, economic, and environmental advantages and support and accelerate the green transformation of the transportation sector.

Ensuring the safety of autonomous vehicles introduces significant challenges to traditional software and hardware safety standards in terms of content and approach. Functional safety ensures that the system can adequately mitigate failure risk for identified hazards. The amount of mitigation required depends upon the severity of a potential failure event, operational exposure to hazards, and driver controllability of the system when the failure occurs.

Project Facts

Project Coordinator:
Dr. Georg Stettinger
Infineon Technologies Germany AG

Project Start: 01.07.2020
Duration: 42M
Total investment: ~€M 13
Requested EU contribution: ~€M 4
Requested National cont.: ~€M 3

Participating organizations: 20
Number of Countries: 8

ArchitectECA2030 has been accepted for funding within the Electronic Components and Systems for European Leadership Joint Undertaking in collaboration with the European Union's H2020 Framework Programme (H2020/2014-2020) and National Authorities, under grant agreement n° 877539

WP1: Requirements and targets

All activities in WP1 ended in month 16 (October 2021). Thus, WP1 successfully defined all functional and non-functional requirements related to individual demonstrators linked to different supply chains. Those requirements build a solid foundation for the upcoming evaluation of the targeted demonstrators within the planned activities in WP6: Validation of mission oriented ECS.

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

In the 2nd year of the project, WP2 has delivered 3 of its 5 designated deliverables, namely deliverables D2.1, D2.4 and D2.5 with success. In doing so, methods and tools for validation of perception systems (in the scope of SC1) and overall monitoring device concept (in the scope of SC4) was studied and reported. These developments were done in parallel to the respective demonstrator progress in both SC1 and SC4. Furthermore, the study of safety levels of safety and acceptable residual risk definitions across all technical supply chains were studied in the scope SC5 and reported in D2.5 respectively. Within this period, two of the four corresponding WP2 tasks (Tasks T2.3 and T2.4) were completed with the completion of the respective deliverables. In the 3rd and final year of the project, WP2 is active only for 6 months and is expected to be completed without any major delay by the submission of the 2 remaining deliverables.

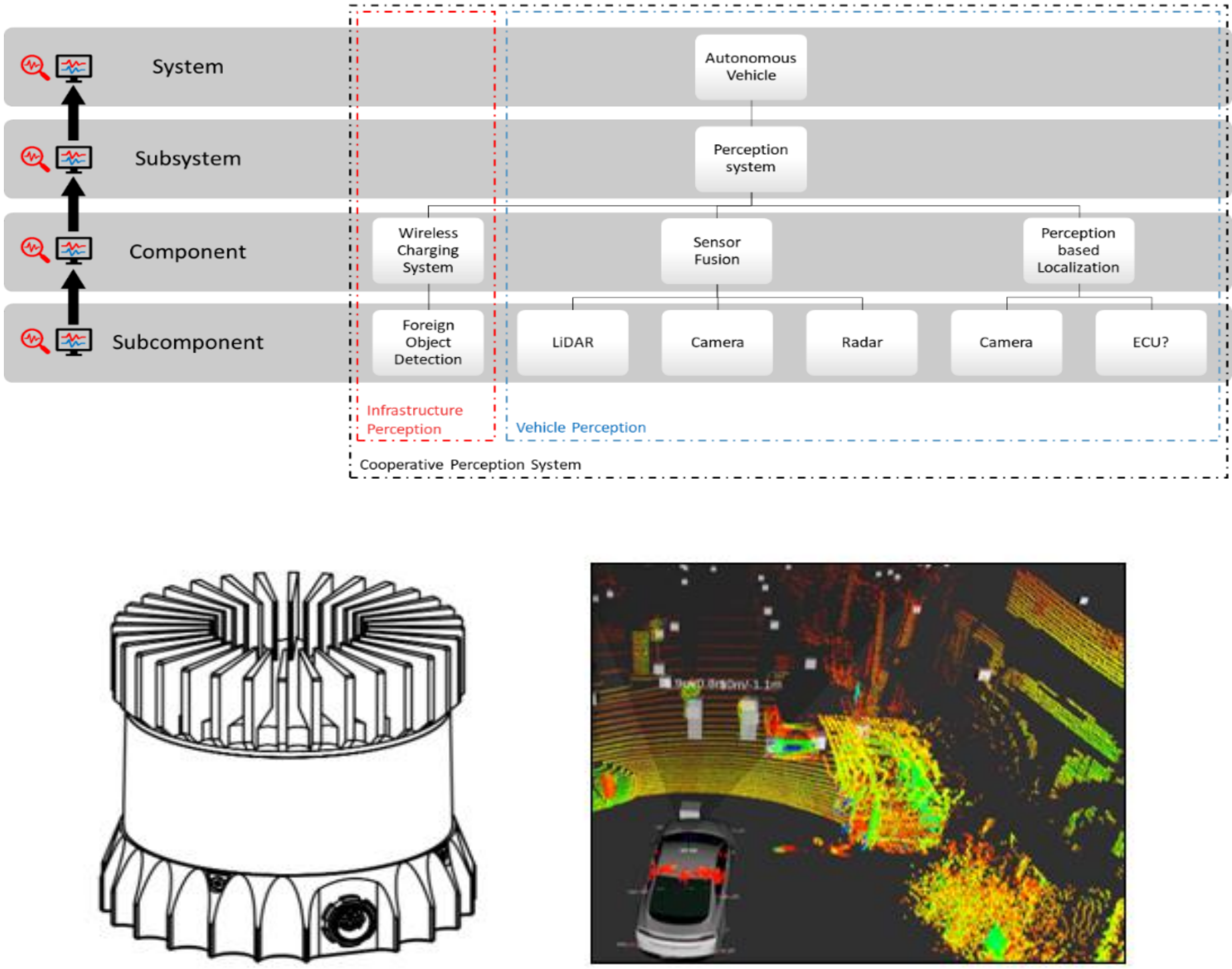


Fig. 1 Architecture, components and tools examples for validation of an automated driving vehicle system

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

During the 2nd year of the project, WP3 has delivered 3 deliverables connected to the monitoring device concept outlined in detail in deliverables D3.5, D3.6 and D3.7. In that light, WP3 activities focused on defining the hierarchical monitoring device concept which was successfully finished via the submission of deliverable D3.7. WP3 also delivered all WP3 related contributions that milestone MS1 and MS3 were successfully met. As a quick outlook, WP3 will focus on finalizing the 6 open deliverables (D3.1, D3.2, D3.3, D3.4, D3.8 and D3.9) connected to tools for fault detection and validation in the acquisition and perception as well as in the actuators and propulsion domain. In addition, prototypic implementations of automatically inserted safety mechanisms and standardization related activities are planned for the final period of the project.

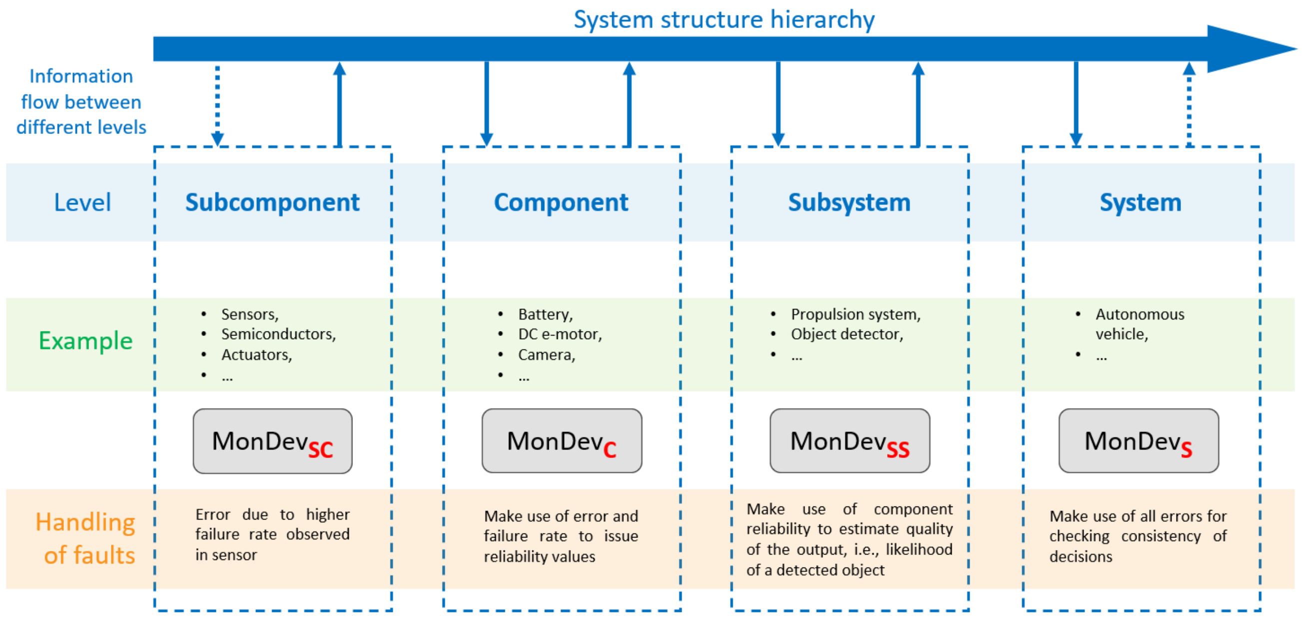


Fig. 2 Hierarchical monitoring device concept

WP4: Identification and management of risks in automotive ECS

WP4 identifies risks corresponding to automotive ECS within autonomous and automated driving, including risks related to methods developed within ArchitectECA2030, i.e., the monitoring device. For this purpose, the aim is to create a risk classification framework considering safety, security, and privacy concerns. In addition, the objective is to provide methodologies for identifying and evaluating risks for concrete components and systems at design and to estimate and manage risks at runtime for keeping systems safe during operation.

In particular, WP4 elaborates on risk estimation when introducing monitoring devices, which ArchitectECA2030 introduced for reducing the overall risks of autonomous and automated driving. In WP4, we devised a risk classification framework considering particular demonstrators for perception, actuation, propulsion, and communication. Furthermore, we identified sources for residual risks, i.e., risks introduced by a monitoring device. And we provide a draft methodology for residual risk identification and the flow for analyzing the residual risk for selected use cases. Moreover, we discussed the influences of other quality assurance measures, like using formal methods for risks and risk management.

WP5: Integration of the residual risk framework

Managing the residual risk (that remains after controls are accounted for), the evolving technology, and the changing operational environment are critical for autonomous vehicles to evaluate and improve the residual risk in the system continually.

This requires novel virtual validation methods and scenario-based testing aiming to assess the behaviour of automated vehicles using realistic and often complex test scenarios that the vehicle might encounter on the roads.

Integrating the residual risk framework in WP5 considers the residual risk identification, methodologies, and metrics developed for the automated and connected vehicles perception, cognition, connectivity, and propulsion domains (SENSE, THINK, CONNECT, ACT) using available tools, prototype methods to support virtual validation.

In this context, the main achievements are related to the definitions of use-case, scenarios, and scene integration for the vehicle perception, propulsion, and connectivity domains according to existing standards. The work includes the development of a failure catalogue to define known faults representing vehicle systems' behaviour as expected in the simulated environment.

In this context, the main achievements are related to the definitions of use-case, scenarios, and scene integration for the vehicle perception, propulsion, and connectivity domains according to existing standards. The work includes the development of a failure catalogue to define known faults representing vehicle systems' behaviour as expected in the simulated environment.

The work comprises detailed descriptions of residual risk identification process steps, including hierarchy, abstraction layers, and different standardization perspectives, considering mapping the project results to standards and methods while identifying the gap in the existing standards.

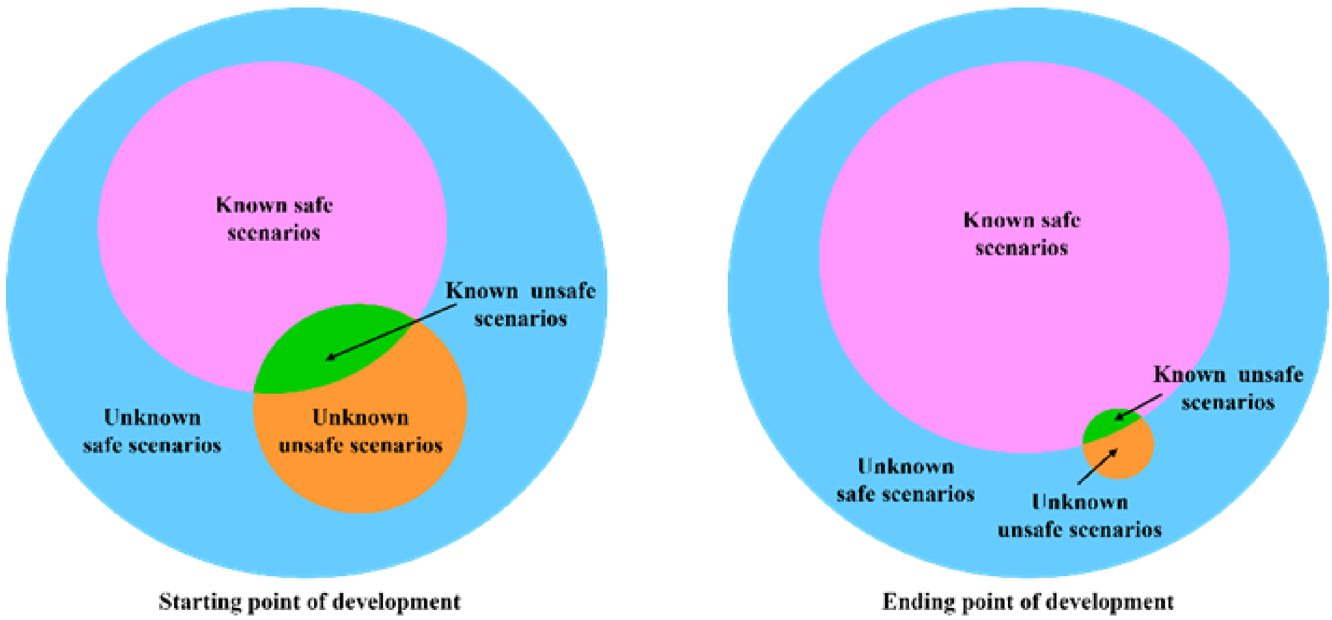


Fig. 3 Expected evolution based on SOTIF activities (source: ISO/PAS 21448)

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

ArchitectECA2030 SC1 aims to determine the remaining risk of hazards to persons and equipment caused by the acquisition and perception system, taking all planned safety measures into account and thus creating an essential basis for the homologation of automated vehicles. The second year of the project was dedicated to the SC1 demonstrators' development.

The graphic below shows the application of S1 demonstrators within a typical usage cycle of an electric, connected, and automated vehicle (ECA). This cycle consists of a charging phase, the actual driving task from start to target destination, and charging again. While demonstrator 1.1 aims to improve the charging phase by developing of a foreign object detection system, the other demonstrators address harsh conditions that may occur during the actual driving task.

Fig. 4 The application of S1 demonstrators

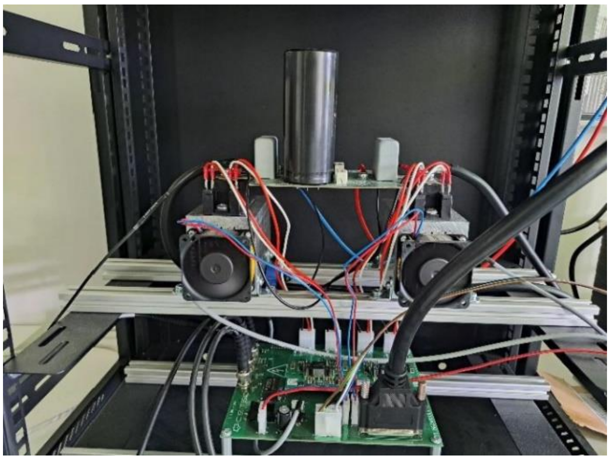
SC2: Failure modes, fault detection and residual risk in actuator and propulsion systems

In the second project year the main achievements of SC2 are first results from hardware and simulation setups comprising the relevant components of propulsion systems and monitoring device methods for fault detection and identification.

Testbench for IGBT modules accelerated ageing has been designed, built/assembled and equipped with a control and data acquisition system in order to analyze first test results for different load types, as constant overloading or power cycling.

A co-simulation framework for a HV battery and thermal control unit is setup and first results with respect to a fault injection model are analyzed by applying a monitoring device, represented as a formal model to detect unexpected behavior in the thermal controller.

An experimental setup comprising a hardware and simulation model of an electric motor is realized to perform initial measurements to identify mechanical vibration caused by imbalances in the rotor in order to verify simulation results.



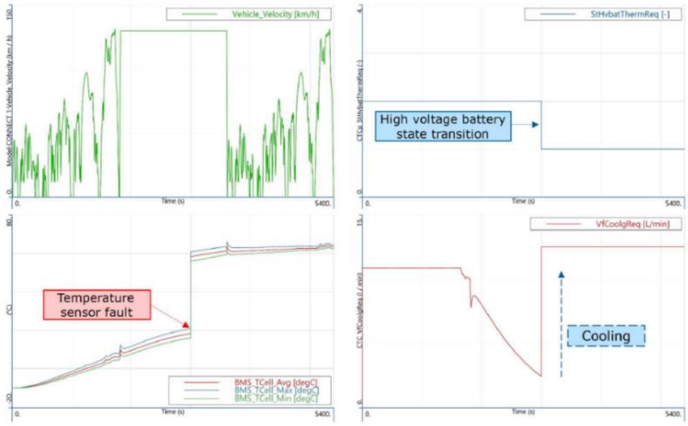


Fig.5 IGBT module accelerated ageing

Fig.6 HV battery thermal control unit simulation results

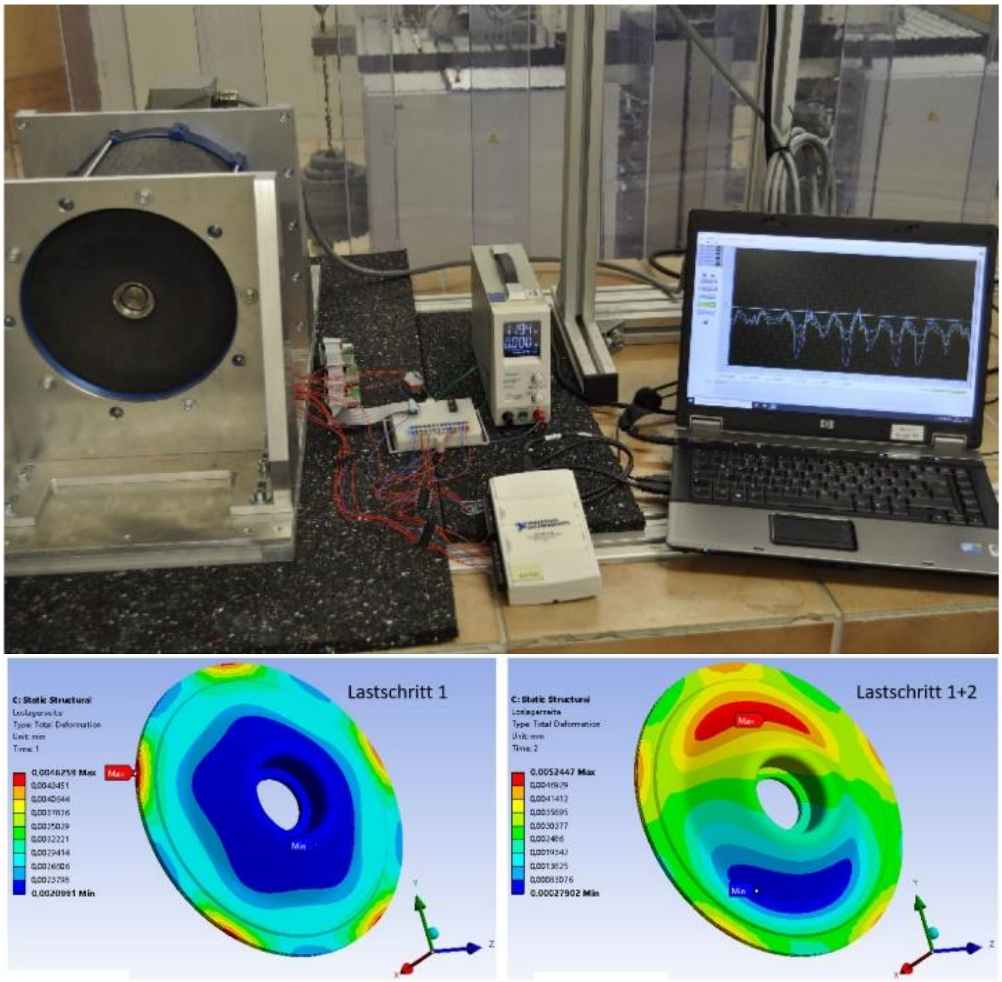


Fig. 7 Experimental hardware setup of an electric motor to measure mechanical vibrations caused by imbalances in the rotor

SC3: Failure modes, fault detection and residual risk for safety analysis in autonomous vehicles connectivity systems.

The supply chain aims to investigate residual risks of subsystems and systems used to build the connectivity functions for automated vehicles (L4, L5) and identify the critical elements needed to create an overall methodology for risk estimations of connectivity systems. SC3 addresses the planned system integrity and dependability elements by creating the basis for the residual risk identification and validation of autonomous vehicles' connectivity functions. SC3 concentrates on the three demonstrators.

The first demonstrator addresses the "Road condition detection and V2X connectivity (RCD-V2X) and the activities focused on the integration/interaction of the V2X connectivity and the perception of road conditions. Extensive tests were performed to evaluate residual risks aligned with the existing standards framework and use it as input to the methodology for risk estimations of connectivity systems to support virtual validation of automated and connected vehicles.

The second demonstrator worked on the "Digital twin package monitoring (DigiPack)" by focusing on developing data-driven and physics of degradation models combined with the Digital Twin technology for lifetime monitoring and design for reliability.
The third demonstrator addresses the "Built-in Connectivity Component Ageing Monitoring (BIAM)" to monitor IC health conditions in the field to make it possible for fail-prediction by using the SW/HW communication infrastructure to handle monitoring data.

Fig.8 Road condition detection monitoring integration into the vehicle

SC4: Methods for monitoring and/or automated driving

The aim of SC 4 is to work on and demonstrate a concept for a monitoring device along the ECS levels for detecting faults and assessing risks for safety and security privacy supporting on overall system architecture.

SC4 demonstrators focus on monitoring methods to address failure modes, fault detection and residual risk during the operating lifetime for safety, security, and privacy supporting an overall system architecture.

Within the last project year, partners elaborated a concrete example based on three of the SC4 demonstrators, which also have a connection to two Demonstrators in SC1.

- D4.1: Hardening automatism for Power or Motor Control Design
- D4.2: Lifetime Drift Model for Discrete Parameters
- D4.4: Automated Driving Demonstrator
- D1.2: Robust physical Sensors
- D1.3: Robust virtual perception

The concrete example follows the hierachical monitoring device concept across all layers as it is depicted in Figure 9.

Receive: Collect all information about the sub-component/ component/sub-system/system health status of the previous layer e.g. RUL, etc.

Monitor: Monitor and classify the health status of the current layer including the effect of the collected health status of the previous layer

- Analyze how a fault of a previous layer propagates within the current layer
- Can we correct/handle the fault? (turn them silent, ASIL-D)
- Do we have a fail-operational layer on (sub-component, component, sub-system, system) available to take over?
- Classify the health status of the current layer (optimal, acceptable, critical)

Transmit: Communicate current health status to the next layer.

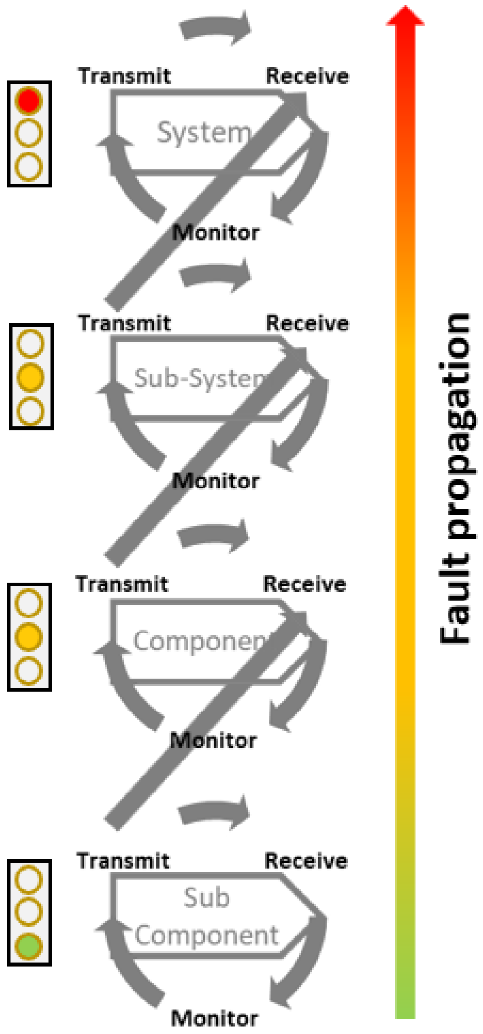


Fig. 9: Monitoring device concept

SC5: Global alignment and contributions to standards

At the current state of the project, SC5 is focusing on reaching out to external advisors and concretize the similarities between external regulatory and standardization efforts and the projects findings and research results in this regard. This is, understandably, a thrilling phase as it condenses all the work that has been done over the last 2.5 years in order to enable external stakeholder alignment and provide for an efficient and productive exchange with them. Especially the communication regarding Architect's Reference Homologation Process (RHP) is at the center of our endeavors as it is the process-based opportunity to converge results from our project with type approval relevant demands. Furthermore, the last deliverables are under preparation in order to be finished within the next 6-9 months. One of which will be a report describing the validation results of ArchitectECA2030 from the perspective of the project consortia and also from the perspective of standardization bodies, stakeholders from industry, governments and academia providing yet another "bridging" element to help relate the projects achievements to external positions.

ARCHITECTECA2030 MEETINGS AND EVENTS WP7

ArchitectECA2030 Mission meeting

On the 9th of June 2022, the project coordinator Georg Stettinger invited SCs, WPs and Tasks leaders to come to Mission Meeting in Munich, Germany. It was the first time the partners met live. The two days meeting was scheduled to discuss the project's status, the main technical achievements in SCs, demonstrators, the first review remarks and recommendations, dissemination and exploitations topics, and the following steps to be done.

The project partners are going to demonstrate how ArchitectECA2030 closes the gap between “bottom up“ (demonstrators, proof-of-concept MonDev big picture) and “top down“ view (validation framework, standardization, homologation).

Also, in the meeting, we prepared a plan for our upcoming important meetings to align successful work and ensure sufficient progress.

ENBIS Annual Meeting 2022

At the end of June, 2022, Lukas Sommeregger and Horst Lewitschnig from Infineon Technologies Austria AG participated at ENBIS Annual Meeting in Trondheim, Norway with the topic “Lifetime Drift Model for Discrete Data for Semiconductor Devices”.

In automotive industry, semiconductors play a critical role nowadays. Many applications, from airbags to sensors, require electrical components to function.

These semiconductors, or chips, have data sheets where their parameters are specified. These parameters can cover a wide variety of types. They can take continuous or discrete values.

Electrical parameters of semiconductor devices can drift over lifetime. Especially with the upcoming relevance of automated driving vehicles, it is important to control these electrical parameters and their potential drift over their whole life cycle to guarantee quality and safety for the end user.

ARCHITECTECA2030 AT EVENTS
WP7

The 1st ArchitectECA2030 External Advisory Board meeting

On the 16 th of September 2022, during the DSC2022 conference in Strasbourg, we had the first ArchitectECA2030 External Advisory Board (EOB) meeting, where the project coordinator Georg Stettinger from Infineon and Jürgen Niehaus from SafeTrans presented the project to EOB members: Siddartha Khastgir from the University of Warwick, Benjamin Engel from ASAM and Andras Kemeny from Renault.

ArchitectECA2030 and the homologation process – was the main topic of the meeting. Furthermore, we linked the ODD concept to the residual risk concept of ArchitectECA2030. EAB members shared their lessons learned and experience in standardization. To get the complete picture of what is already achieved, we discussed project references that had not been considered before. Also, we started to build a certification and homologation community and agreed on regular experience exchange in the future. EAB members will help to establish connections to similar projects to complete the full baseline and ensure harmonized and aligned work within ArchitectECA2030.

The 2nd Review Meeting

On 27th of September 2022 AchitectECA2030 partners met in the 2nd Review Meeting in Brussels, where SCs’ and WPs’ leaders presented the main second-year achievements, and the project officer Anton Chichkov and reviewers: Zlatko Petrov and Jan Louis Anthonis evaluated our progress.

According to the overall assessment, the project has achieved some of its objectives and milestones, however a lot of work still has to be done during the last year.

Upcoming Events

19.10.2022 Making Industry 4.0 Real
17.11.2022 ASAM Test Specification Workshop
14-17.11.2022 Transport Research Arena (TRA) 2022
24-25.11.2022 EFECS 2022
7-8.02.2023 ECS Brokerage Event 2023
14-16.02.2023 RTR Conference 2023
3-4.05.2023 EUCAD 2023
22-24.05.2023 ITS European Congress 2023

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.