AUTOMOTIVE 2021 VIRTUAL Conference

17-19 November 2021

ArchitectECA2030

ArchitectECA2030
Electric, Connected and Automated Vehicles, what about Risk, Trust, and Failure?

Cristina De Luca
Infineon Technologies AG
Cristina.DeLuca@infineon.com

ArchitectECA2030

Automotive Value chain

SME

Academic Research

Project Facts
RIA – ECSEL JU Project

Duration: 07/2020 - 06/2023

Total Costs EU: ~ € 13,3 Mio.

Consortium: 20 partners

https://architect-eca2030.eu/

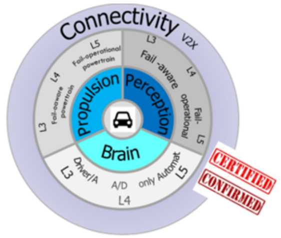
AUTOMOTIVE 2021 VIRTUAL Conference 17-19 November 2021

Infineon - ATV autonomous driving

Risk

Trust

Failure



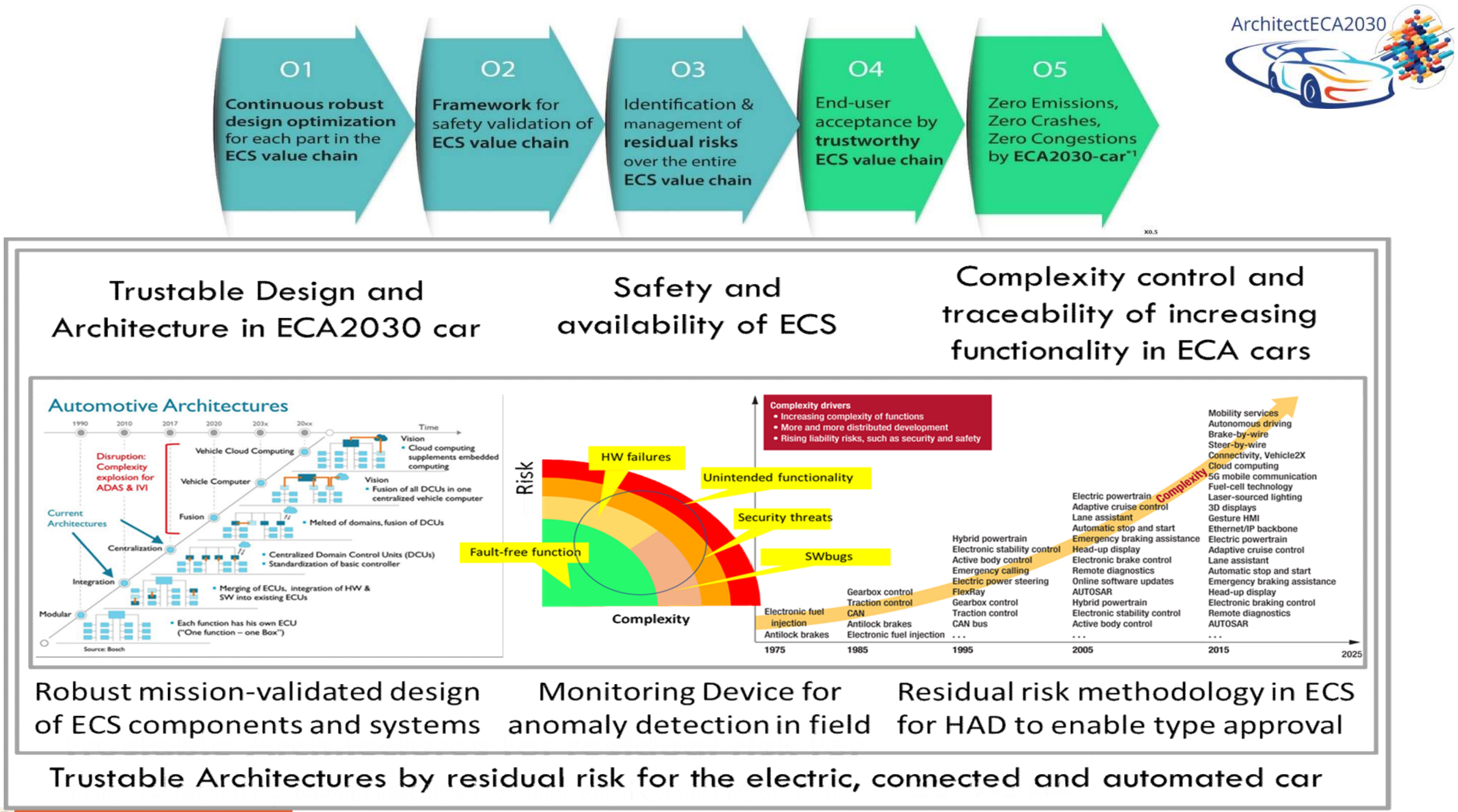
Vision & Goals

VISION

The vision of ArchitectECA2030 is 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

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.


ArchitectECA2030
O1
Continuous robust design optimization for each part in the 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*1
Trustable Design and Architecture in ECA2030 car
Safety and availability of ECS
Complexity control and traceability of increasing functionality in ECA cars
Automotive Architectures
Disruption: Complexity explosion for ADAS & IVI
Current Architectures
Vehicle Cloud Computing
Vehicle Computer
Fusion
Centralization
Integration
Modular
Time
Melted of domains, fusion of DCUs
Centralized Domain Control Units (DCUs)
Standardization of basic controller
Merging of ECUs, integration of HW & SW into existing ECUs
Each function has his own ECU ("One function – one Box")
Source: Bosch
Risk
Complexity
HW failures
Unintended functionality
Security threats
SWbugs
Fault-free function
Complexity drivers
• Increasing complexity of functions
• More and more distributed development
• Rising liability risks, such as security and safety
Complexity
1975
1985
1995
2005
2015
2025
Robust mission-validated design of ECS components and systems
Monitoring Device for anomaly detection in field
Residual risk methodology in ECS for HAD to enable type approval
Trustable Architectures by residual risk for the electric, connected and automated car

General Objectives and the Expected Impacts

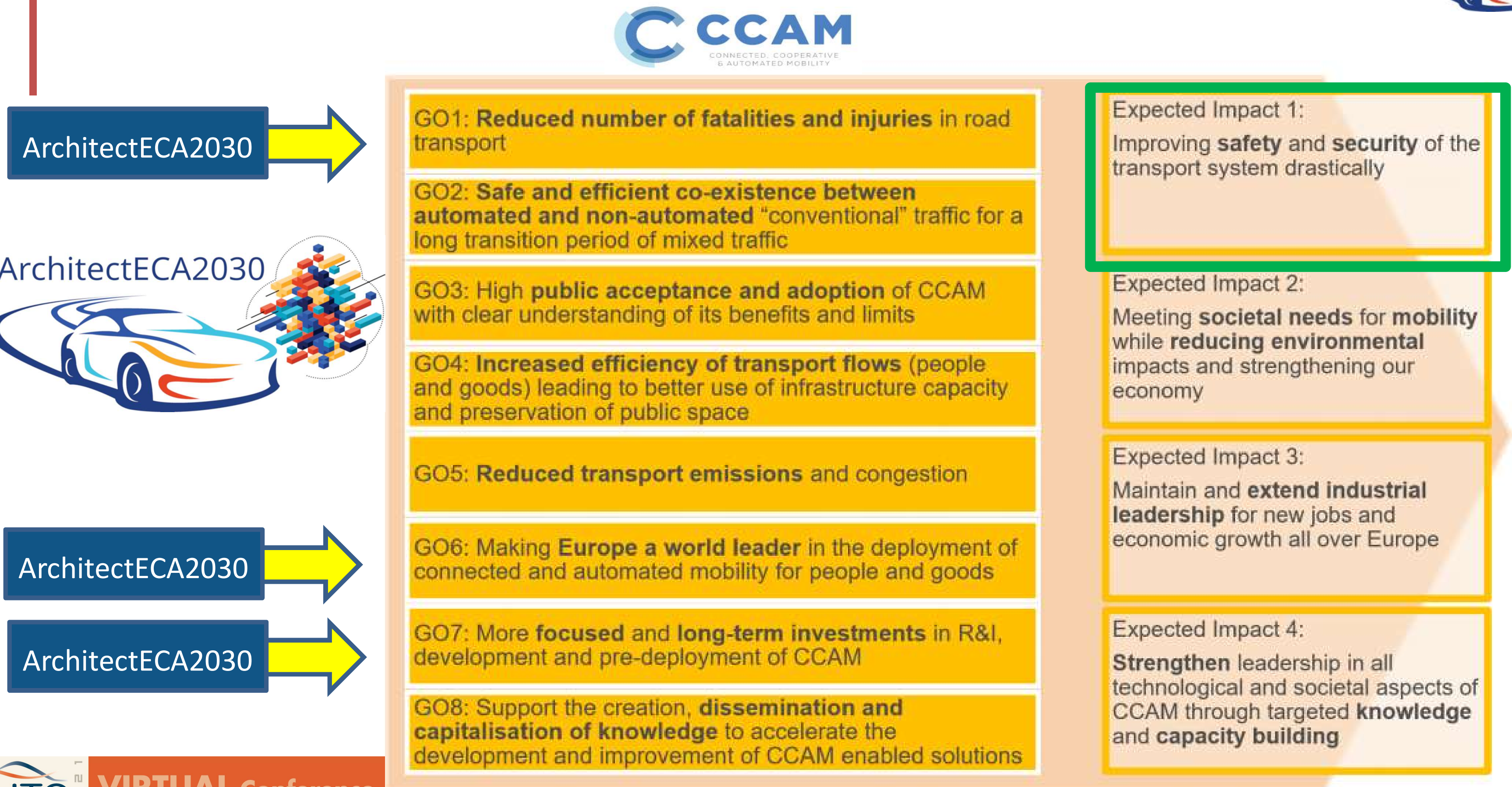
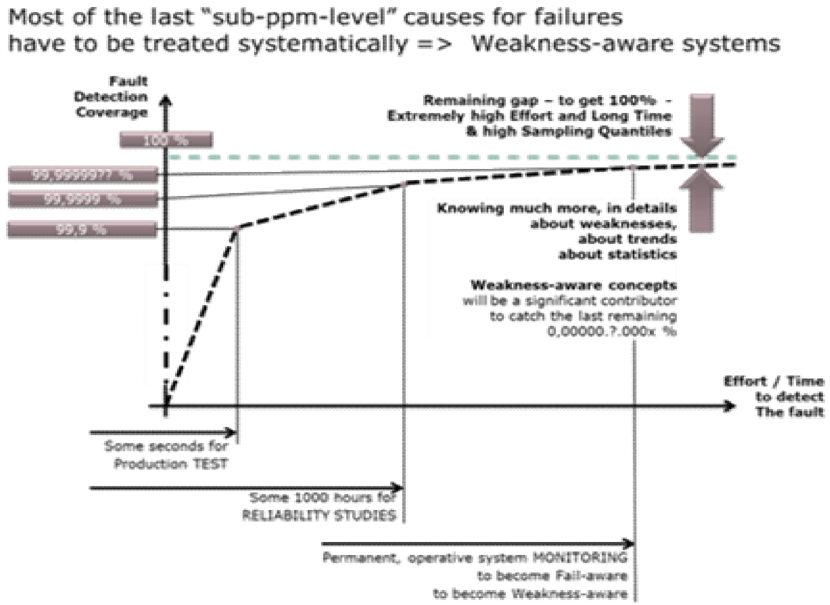


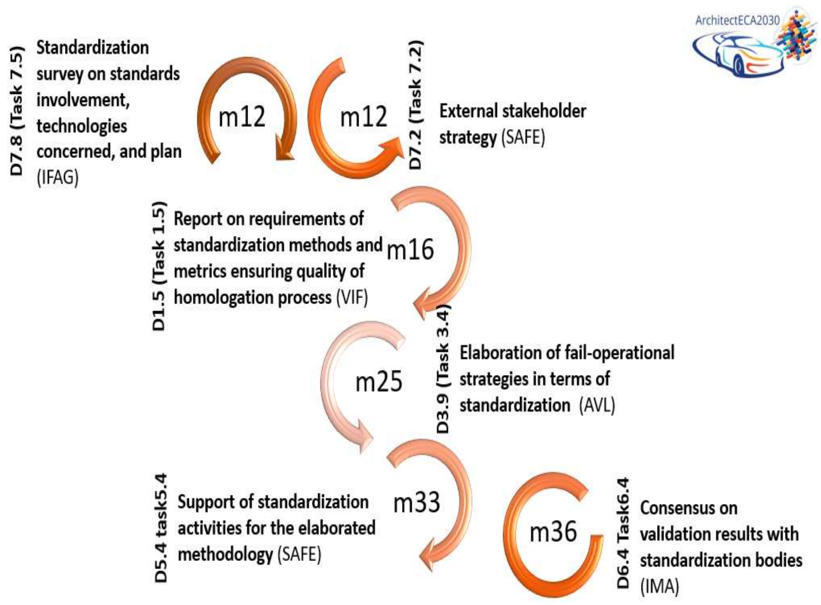
Figure 4: General Objectives and the Expected Impacts of the CCAM Partnership.

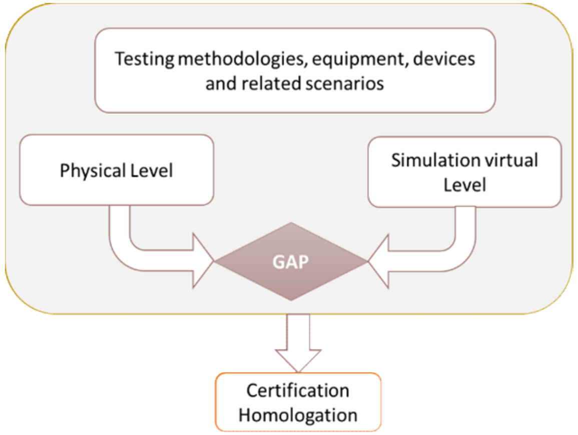
How to reach an harmonized pan-European validation framework?

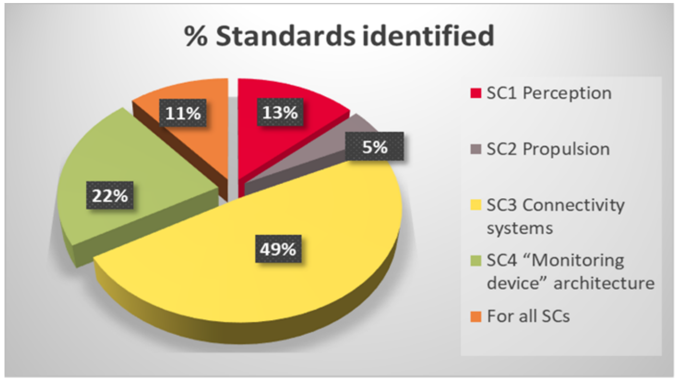
- **Analysis** of **fault modes** and their **consequences** on the behavior of actuator and propulsion systems.
- Providing **methods and tools for fault detection**, **localization** and **repair**.
- Coming up with a **verification methodology** specifically adapted to ensure quality of the proposed system fulfilling safety requirements of mission-critical systems.
- **Quantifying the residual risks** when applying the fault detection, localization, and repair methods.
- **Developing demonstrators** showing the applicability and the reduction in development time of the proposed methods and tools.



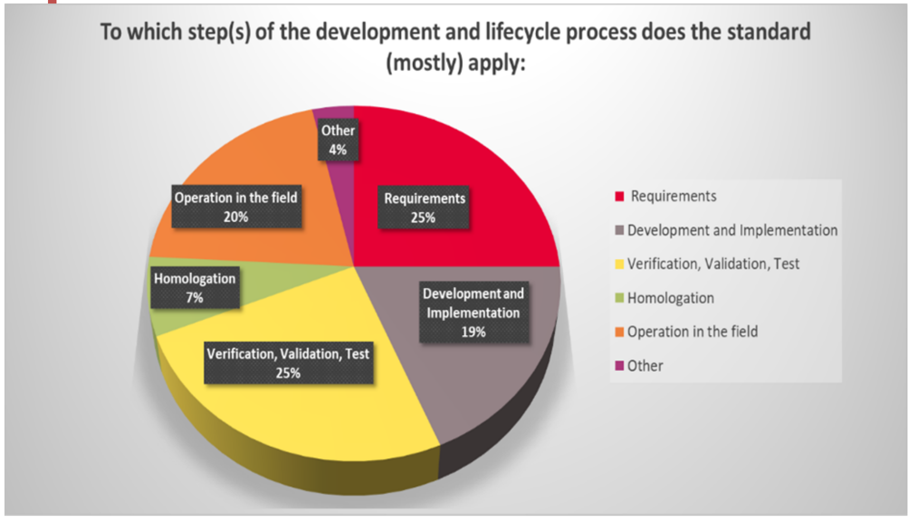
Standardization survey on standards involvemen technologies concerned and plan (D7.8) - PUBLIC

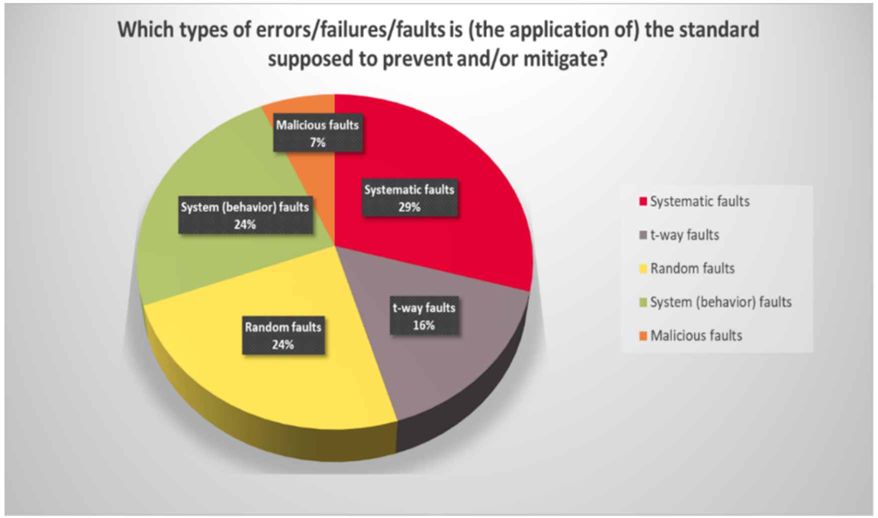






Some Results





The ArchitectECA2030 Consortium in relation to the project's supply chains-demos, has mapped 34 different standards to the supply chains/demos, among others addressing e.g. the Road Vehicles – Functional Safety (ISO 26262), condition monitoring and diagnostics of machines, systems and software engineering standards, Information technology — Artificial intelligence, road vehicles – safety of the functionality, cybersecurity engineering, taxonomy and definitions for terms related to driving automation systems, safety analysis and safety verification, and more others.

Conclusion

While significant challenges remain in certifying the security of the type of algorithms that provide vehicle autonomy, it seems more feasible to instead architect the system and its design process to utilise existing software security approaches (using ISO 26262, ISO PAS 21448 - SOTIF - Safety of Intended Functionality and related cybersecurity specifications).

Consequently, there is a strong need for alternative methods to supplement real-world testing in order to assess ECA vehicle safety and shape appropriate policies and regulations.

These methods may include but are not limited to accelerated testing, residual risk quantification, virtual testing and simulations, scenario and behaviour testing, and pilot as well as extensive focused testing of HW and SW systems.

National Funding

Federal Ministry of Education and Research of Germany

www.bmbf.de

Austrian Research Promotion Agency

www.ffg.at

Ministry of Education, Youth and Sports

www.msmt.cz

Netherlands Enterprise Agency

www.rvo.nl

The Research Council of Norway

www.forskningsradet.no

Thank You !

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.

European Funding

ECSEL Joint Untertaking

www.ecsel.eu

Horizon 2020 Programme

ec.europa.eu

European Union

europa.eu