This project has received funding from the ECSEL Joint Undertaking under grant agreement No 877539.
This Joint Undertaking receives support from the European Union's
Horizon 2020 research and innovation programme and the ECSEL member states.

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

Deliverable	***Standardization survey on standards involvement, technologies concerned and plan***		
Deliverable File	***D7.8***		
Project	ArchitectECA2030	**Grant Agreement Number**	877539
Lead Beneficiary	IFAG	**Dissemination Level**	Public
Involved SCs	SC1, SC2, SC3, SC4, SC5	**Related Task/s**	**Task 7.5: Standardisation**
Due Date	30 Jun. 2021	**Actual Submission Date**	10 Aug. 2021
Status	DRAFT	**Version**	V1.0
Contact Person	Dr. Cristina De Luca	**Organisation**	IFAG
Phone	Tel. +49 8923 43 8666	**E-Mail**	Cristina.DeLuca@infineon.com

Document history			
V	**Date**	**Author**	**Description**
0.01	25.03.2021	Dr. Cristina De Luca	Initial Version
0.2		Jürgen Niehaus Safetrans, Germany	Standardization Survey description
0.3		Cristina De Luca (INFINEON) Jürgen Niehaus (SAFETRANS) Reckenzaun, Jakob (VIF)	Standardization plan
0.4		All Partners	Standards related to the SC's demonstrators
0.5		Cristina De Luca	Chapter 1,2,3
0.6	March, April, May	ALL Partners/demos/Supply Chains	Survey on standards involvement
0.7		Jürgen Niehaus (SAFETRANS) Bastian Prugger, (AVL/AT)	Review
0.8	August	Cristina De Luca	Draft Version
0.81	August	Bastian Prugger	Review part 2
1.0	August	Cristina De Luca	Final Version

Disclaimer

The opinion stated in this document reflects the opinion of the authors and not the opinion of the European Commission. The Agency is not responsible for any use that may be made of the information contained (Art. 29.5 of the GA).

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Table of contents

1 Executive/ Publishable summary 6
2 Introduction & Scope 6
2.1 Purpose and target group 6
2.2 Relation to other activities in the project 7
3 Standardization and Homologation State of the Art 7
4 Standardization Plan Description and Timeline 10
4.1 Standardization Plan 11
5 Standardization Survey 14
6 Standards Involved 18
6.1.1 ISO 17359:2018 18
6.1.2 ISO 18129:2015 19
6.1.3 ISO/IEC 25010 20
6.1.4 ISO/IEC TR 24028 22
6.1.5 AI Safety / The Landscape of AI Safety 24
6.2 PERCEPTION: SC1 Failure modes, fault detection and residual risk in acquisition and perception systems 27
6.2.1 ISO15622:2018(E) 27
6.2.2 ISO20035:2019(E) 30
6.2.3 ISO 17387:2008(E) 34
6.2.4 SAE J2954 37
6.2.5 ISO26262:2018 41
6.2.6 ISO/PAS 21448:2019 45
6.3 PROPULSION: SC2 Failure modes, fault detection and residual risk in actuator and propulsion systems 50
6.3.1 IEEE Std 1856TM-2017 50
6.3.2 ISO 26262 53
6.4 CONNECTIVITY: SC3 Failure modes, fault detection and residual risk for safety and security in connectivity systems. 57
6.4.1 Demo 3.1 - ISO 26262 57
6.4.2 Demo 3.1 - ISO/PAS 21448 61
6.4.3 Demo 3.1 - ISO 4804 65
6.4.4 Demo 3.1 - SAE J2954 68
6.4.5 Demo 3.1 - IEC 61508 70

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6.4.6 Demo 3.1 - IPC 2551 72
6.4.7 Demo 3.1 - ANSI/UL 4600 73
6.4.8 Demo 3.1 - ISO/SAE FDIS 21434 74
6.4.9 Demo 3.1 - SAE J3061 75
6.4.10 Demo 3.1 - IEEE P2846 76
6.4.11 Demo 3.1 - IEEE P2851 77
6.4.12 Demo 3.1 - IATF 16949:2016 (replace ISO/TS 16949:2009) 78
6.4.13 Demo 3.1 - AEC Q100 79
6.4.14 Demo 3.1 - EN ISO 24534 80
6.4.15 Demo 3.1 - IEEE 802.11p 81
6.4.16 Demo 3.1 - IEEE 802.11bd 82
6.4.17 Demo 3.1 - IEEE P2020 83
6.4.18 Demo 3.1 - SAE J2735 83
6.4.19 Demo 3.1 - SAE J3016 84
6.4.20 Demo3.1 - Other comments 84
6.4.21 Demo 3.2 - IPC 2551 85
6.4.22 Demo 3.2 - ISO 26262 88
6.4.23 Demo 3.2 - ISO/PAS 21448 93
6.4.24 Demo 3.2 - AEC Q100 98
6.4.25 Demo 3.2 - ISO/TR 18161 102
6.4.26 Demo 3.3 - ISO 26262 105
6.4.27 Demo 3.3 - ISO/PAS 21448 109
6.4.28 Demo 3.3 - IPC 2551 112
6.4.29 Demo 3.3 - ISO 4804 112
6.4.30 Demo 3.3 - SAE J2954 115
6.4.31 Demo 3.3 - ANSI/UL 4600 118
6.4.32 Demo 3.3 - ISO/SAE DIS 21434 118
6.4.33 Demo 3.3 - IEEE P2846 118
6.4.34 Demo 3.3 - IEEE P2851 118
6.5 MONITORING: SC4 Failure modes, fault detection and residual risk for safety security privacy on overall system “monitoring device” architecture 119
6.5.1 SAE JA6268TM 119
6.5.1 SAE J3016 121
6.5.2 J3018 123

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6.5.3 UNECE Regulation 157 (ALKS) --> link 126
6.5.4 IEEE P2846 130
6.5.5 ISO 17361:2007(E) 133
6.5.6 ISO 11270:2014(E) 136
6.5.7 ASAM OpenDRIVE 140
6.5.8 ASAM OpenSCENARIO 143
6.5.9 ASAM OpenXOntology 146
7 Evaluation of the survey's results 149
8 Conclusion 161
8.1 Contribution to overall picture 161
8.2 Contribution to demonstration 161
9 References & Good to Know 161
10 List of figures 162
11 List of Tables 163
12 GLOSSARY OF ACRONYMS 164

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

1 Executive/ Publishable summary

The deliverable 7. 8 "***Standardization survey on standards involvement, technologies concerned and plan"*** gives an overview of the standards identified as significant for the different demonstrators in the ArchitectECA2030 project, which are of fundamental importance for understanding existing gaps with respect to the state of the art. Purpose is to describe the survey on standards involvement, technologies concerned and standardization plan.

Chapter 2 briefly introduces the target groups, the scope and relation to other activities in the project. This Deliverable is strongly related to the Supply Chain 5 "Global Alignment and Contribution to Standards activities" and is twinning with deliverable 7.2 "External Stakeholder Strategy". In Chapter 3 the state of the art for the topic of standardisation and homologation in autonomous vehicles is introduced, highlighting the link with the concept of "residual risk" and "monitoring device". Chapter 4 illustrates the timeline of the plan to take forward the standardisation support plan in relation to the project demonstrators, which were taken as examples of relevance to the topic. Chapter 5 describes the survey and summarises some general results, while chapter 6 lists the actual standards involved as relevant for the project. In chapter 7 are evaluated, also reporting some statistics, the survey's results, and number of standards, relevant organization, which step of the development and lifecycle process does the standard (mostly) apply and which type of errors/faults is the standard supposed to prevent and/or mitigate. The conclusions are explained in chapter 8.

We would like to emphasise that the list is not exhaustive as the subject is of considerable breadth and complexity in relation to the size of the ArchitectECA2030 individual project.

Key words: Standardization, homologation, survey, homologation, autonomous vehicles

2 Introduction & Scope

2.1 Purpose and target group

Purpose of the deliverable is to describe the survey on standards involvement, technologies concerned and standardization plan.

An important element in the development of a competitive European industry for automated vehicles is the establishment of technology standards. These are needed to define the interfaces between the different members of the various value chains, which are the backbone of competitive and future proof platforms. This will help to build a solid technology base in Europe. We will cooperate from the beginning with European and US based standardizations bodies such as our partner N.I.S.T and European based e.g. Cen-Cenelec.

This project will contribute by providing input to the standardization organizations in which the project partners are involved. An important focus will be on standards regarding subsystems, system integration and system architectures for automated vehicles. Existing experience in cooperation between funded projects and standardization bodies (e.g., within ENABLE-S3, by AVL and SAFE with ASAM standardization body; or within CP-SETIS, by SAFE, with ASAM and ETSI standardization bodies, will be heavily exploited in this task.

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

2.2 Relation to other activities in the project

This Deliverable is strongly joined to the Supply Chain - **SC5 Global Alignment and Contribution to Standards activities,** and particularly, in this phase of the project, with **Task 1.5** [SC5]: Requirements for standardization of methods and metrics for potential failure risks quantification, residual risk calculation and certification of level 3+ systems (leader: VIF, IMA, DATA, all) and the Deliverable 1.5, 31 Oct 2021-(m16). The other fundamental related document is the **D7.2 External Stakeholder Strategy.** The D7.2 deliverable describes the Stakeholder Management Plan for ArchitectECA2030, where 'Stakeholder' is meant to denote any organisation or individual that is (a) not a project partner, (b) active in the same technical area as ArchitectECA2030, i.e. residual risk based homologation of SAE level 3+ electric, connected and automated cars (ECAs), and (c) for whom cooperation in any form with the project would be of mutual benefit for the stakeholder and the project. We identify stakeholder groups by categorize organisations with respect to the role that they have in the value chain for developing, testing and homologating L3+ ECAs and map concrete organizations and individuals to these groups…The Stakeholder Management Plan will – together with other surveys and information retrieval activities most noteworthy those done in **Task 7.1 [SC5] External stakeholder strategy and alignment (leader: SAFE, all)** – be the basis for setting up the External Advisory Board and initiate twinning and other cooperation activities within ArchitectECA2030.", 30 Jun 2021 (m12).

The analysis of standards and the effect on future vehicle approvals is carried out through all project phases and related WPs.

Cooperation with all those involved in these aspects, from suppliers and consumers, to vehicle manufacturers and all related industries, in general all stakeholder, is clearly crucial. At this level, there is a strong impetus for the standardization and homologation of future vehicles, which will also influence the OEM's research and market.

3 Standardization and Homologation State of the Art

Section 4 in Deliverable D7.2 "External Stakeholder Strategy" contains a high-level description about homologation (type approval) processes as they are implemented today and in the foreseeable future. The observations and explanations from that document that are most relevant for the purpose of this document are summarized here:

- Homologation (or type approval) refers to a certification process of a product – i.e., a car, a vehicle – demonstrating that it complies with all local standards and legal regulations applicable to this product, such as safety and environmental regulations.
- The regulations, against which compliance of the product needs to be checked, are local ones, i.e. they are part of the local law of the respective geographical – or, more correctly: judicial – area. Nonetheless, these local regulations are typically derived through a hierarchy of regulations issued on international level (e.g., by UNECE), European Union regulations and finally national regulations.
- Depending on the geographical – or more correctly the judicial – area for which type approval of a product needs to be achieved, the actual certification process is either done by the product manufacturer itself (self-certification, used e.g., in the US) or by an independent organization (third-party homologation, used e.g., in Europe). An example for such an independent organization in Europe is TÜV.

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

- Regulations that govern homologation seldom reference standards directly. Instead, standards represent the 'state of the art' descriptions of the technical means (processes and methods) that are sufficient to show compliance of the product to the relevant regulations. In Germany, for example, a part of the homologation argument of a Car Manufacturer (OEM – Original Equipment Manufacturer) for his non-automated (ie., SAE Level L1) vehicle could run as follows: "I, the OEM, can demonstrate that the E/E System of this vehicle complies to all applicable safety regulations because I have fully implemented and followed the ISO 26262 standard, and we all know and have agreed upon that this is sufficient for showing this compliance".
- Whenever new regulations are introduced – as they are now for L3+ vehicles – it needs to be checked whether the existing standards are still sufficient to uphold this agreement, i.e., that the standard still represents the technical state of the art such, that following resp. implementing this standard is a sufficient condition for demonstrating compliance to these regulations. It has been determined that for L3+ cars, following ISO 26262 alone is not sufficient anymore; The search for additional standards and/or extension to ISO 26262 is the object of many activities and publically funded R&D projects; similar extensions are needed for standards used for showing compliance to other sets of regulations (e.g., environmental ones).

From the above, it is evident that there is an increasing complexity of the relations among industry accepted standards, regulations, legislation addressing safety and security of vehicles and technologies. It is although also evident that the existing regulations evidence an enormous gap, because while on the road testing automated vehicles is done in a supervised real-word traffic where conditions and the data are used to validate the algorithms supporting automaton technologies; this is considered insufficient for validating their operational effectiveness that, would require traveling millions of kilometers.

"The homologation of automated and connected vehicles according to global regulations is essential for their safe and reliable development and deployment around the world. But existing regulatory safety frameworks applicable to conventional vehicles and their components are insufficient to fully assess the operational characteristics of current and future automated vehicle technologies. As with increasing automation vehicles transform into cyber-physical systems that no longer require a human driver, new safety challenges will have to be considered." Christian Gnandt - Head of Test and Validation, Autonomous Driving & ADAS - TÜV SÜD Auto Service GmbH, Business Unit Automotive, "Homologation of automated vehicles The regulatory challenge", White Paper[1].

The four ACES innovations – **autonomous driving, connected cars, electric vehicles, and shared mobility** – dominates the agenda of automotive industries and are built on the digitization of in-car systems, the extension of car IT systems into the back end, and the propagation of software.

Also if cyber security aspects are not included in the goals of ArchitectECA2030, this is considered one of the main aspects to consider for the state of the art. We would like to underline that *"Engine power, fuel consumption, driving comfort, and the precision of a car's chassis and body are just a few dimensions that define the quality of a car. With more and more core vehicle functions enabled by*

[1] https://www.tuvsud.com/en/-/media/global/pdf-files/whitepaper-report-e-books/tuvsud-autonomous-vehicles-homologation-whitepaper.pdf?la=en&hash=50F4F20A33968CC8E2615A0B88BB786A

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

software running on specialized hardware chips, the security of those components – cybersecurity – will become yet another dimension of quality in the automotive industry, in much the same way that physical safety is a major concern and quality parameter today.

This measure of quality is underpinned by regulatory activities that impose minimum standards for managing cybersecurity risks and require OEMs to have the ability to fix security issues via software updates. Cybersecurity will become nonnegotiable for the industry. In order to excel at cybersecurity, new processes, skills, and working practices along the automotive value chain will be required. This includes identifying cyber risks, designing secure software and hardware architectures, and developing and testing secure code and chips, ensuring that issues can be fixed – even years later – via software updates." [2]

This aspect is strongly related to the definitions of "residual risk" and "Monitoring device" that ArchitectECA2030 Consortium is researching and which results will be proposed to the regulatory bodies as basis for re-thinking the risk and monitoring of the vehicles.

Fundamentally, "if you cannot measure it, you cannot manage the risk through the vehicle lifecycle" ArhictecECA2030 Consortium.

[2] file:///T:/05_temporary/0000_IFAG/02_ArchitectECA2030/09_Deliverables_milestones/WP7/PAPERs/Cybersecurity-in-automotive-Mastering-the-challenge.pdf

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

4 Standardization Plan Description and Timeline

The standardization process is worldwide accepted and transparent. “Standards are an industry-driven tool that allows the industry and all interested parties to independently design technical specifications. Standards can only be successful, if potential is analysed early on and translated into action across bodies. It is essential to design a normative framework in a pro-active international manner, enabling new technologies and creating a uniform understanding within the industry [7].[3]

The goal of ArchitectECA2030 standardization plan[4] is:

- Creating an overview of the standards in relation to the demonstrators in the different supply chains. A refinement by consortia is requested and implemented.
- Identifying 3-4 standards related to homologation of L3+ ECAs of project’s relevance and development of a strategy for the individual standards contribution, possibly industry driven.
- Identification of the gaps. Due to the project topic and restricted funding only some of the standards and their actual gaps can be analysed.
- Building consensus within industry and stakeholders, not contradicting main stream ideas.
- The results of this research must be examined to determine the extent to which meaningful standardizations can be derived from them.

A fundamental aspects that ArchitectECA2030 will support are:

- *“Standardized management rules can support the cooperation of vehicle manufacturers, testing organizations and authorities involved in the approval of vehicles with automated driving functions. This ensures the certification of the parties involved and the process flow on the basis of corresponding standards.*
- *Regulatory requirements must be met for the approval of automated driving functions. In the future, these regulatory requirements will be examined using several building blocks. An analysis is recommended as to how the future approval process can be supported by standards.*
- *The AI requirements for automotive applications should be described normatively. A first step would be the definition of different AI levels for vehicle application.”*

The following topics were clustered across bodies and evaluated in terms of the time span (light blue/blue bars) in which significant standards and standardization activities can be expected with regard to the importance of introducing Level 3 systems:

[3] file:///T:/05_temporary/0000_IFAG/02_ArchitectECA2030/09_Deliverables_milestones/WP7/PAPERs/VDA_4699_Normungsroadmap_AdaptionEN_Web.pdf

[4] *“Due to the increased importance of standardization in funded research projects, the **DIN Automotive Standards Committee should be involved**. The aim is to ensure that the results of the funded project are used sustainably in standards, and that synergies are exploited. The preparation of concrete standards drafts as partial project results accelerates the process and ensures the use of the project results.”[7]*

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

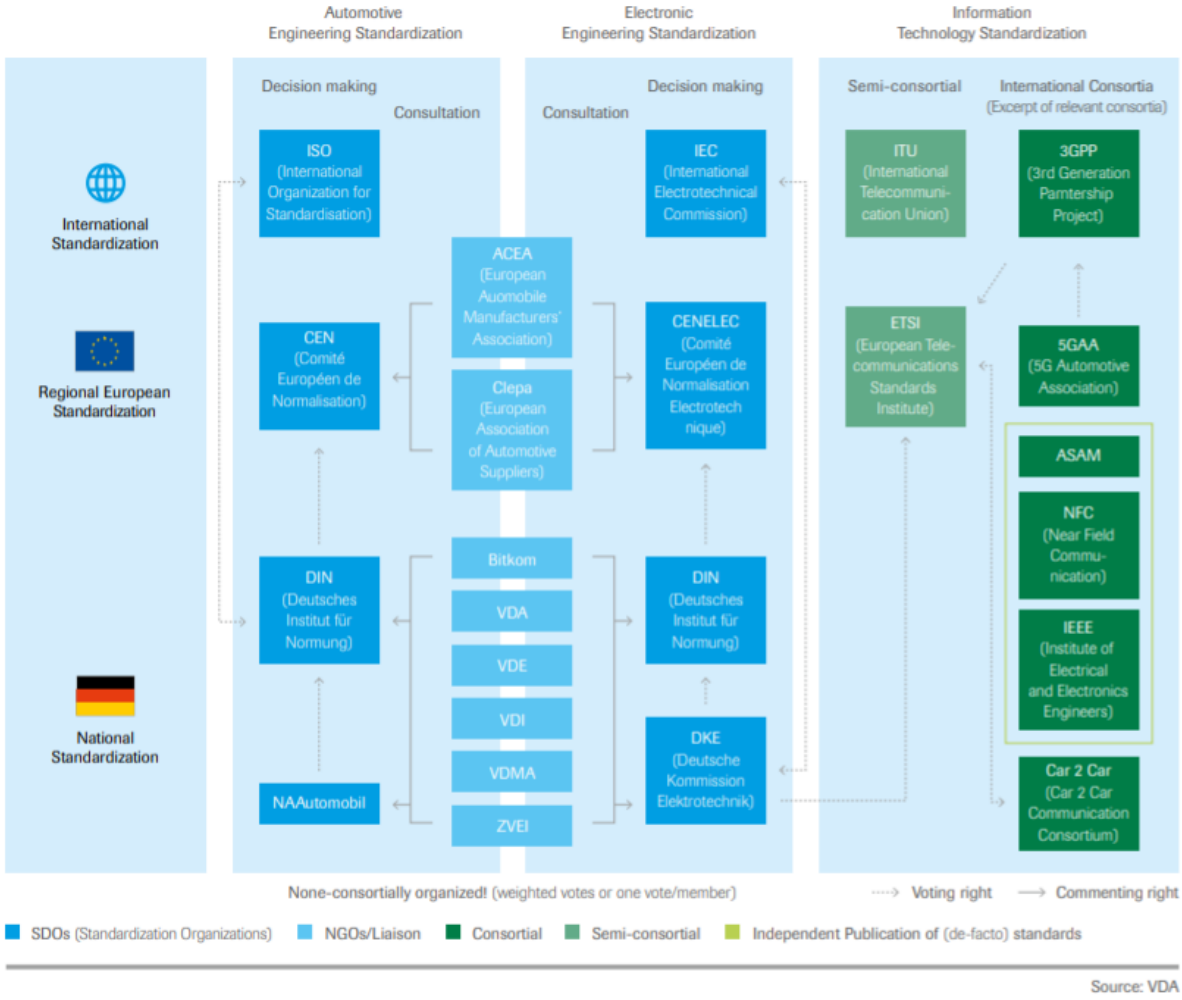


FIGURE 1 LANDSCAPE OF BODIES AND COMMITTEES

4.1 Standardization Plan

Why a standardization plan? In 2017 SafeTRANS has launched a strategy (the German roadmap on highly automated systems) how to succeed with a type approval for SAE L3+ vehicles. The roadmap has been strongly influenced by the following ArchitectECA2030 members: AVL, SAFE, and VIF. Given the enormous environmental complexity that precludes a sufficient level of field testing as a basis for deployment, a system of continuous supervision and learning from field observations was proposed. ArchitectECA2030 will incorporate these features from a mission-oriented ECS perspective within its framework for calculating the residual risk that enables ECA vehicle homologation.

The Figure below shows this meta-level learning process that learns from the experiences of the systems in the field through an assessment of such field data by an independent authority. This assessment provides directives or recommendations for new features and/or new capabilities to be integrated in the development and validation processes with the twofold goal of improving the perception abilities of the system and of assuring its adequate behaviour. The mechanism of such a learning process supports the evolution of autonomous systems thanks to the ability of their virtual release within the frame of a model-centric development process. Central building blocks of this process are architecture and algorithms, environmental models, verification and validation procedures and systematic gathering of operational data from the field. These basic elements need appropriate

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

standardization, a common open simulation environment and an accepted set of scenarios for homologation. [5]

Therefore, an appropriate plan has been developed in ArchitectECA2030 that addresses the topics along the way.

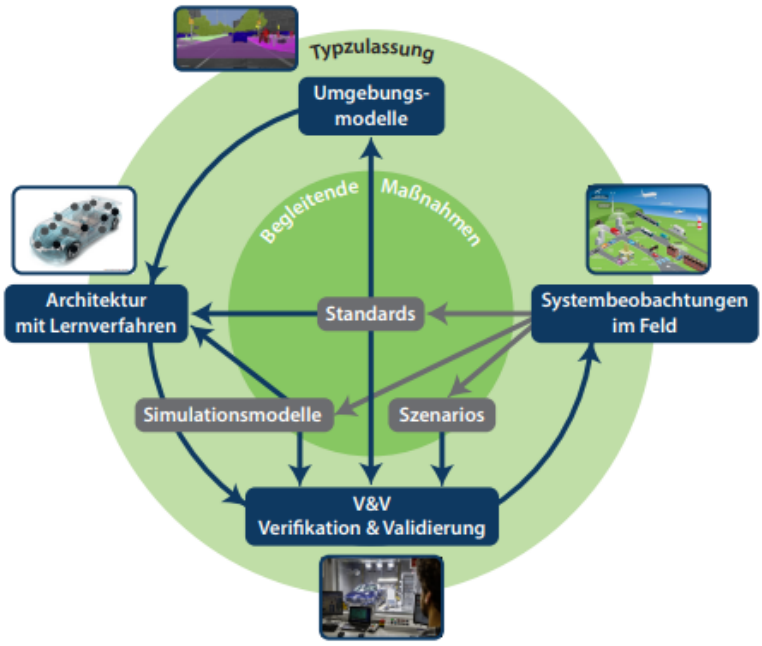


FIGURE 2 TYPE APPROVAL PROCEDURE FOR ECA VEHICLES. "HOCHAUTOMATISIERTE SYSTEME: TESTEN, SAFETY UND ENTWICKLUNGSPROZESSE – ROADMAP FORSCHUNGSFELDER UND HANDLUNGSEMPFEHLUNGEN", SAFETRANS, NOVEMBER 2017

The plan evolves throughout the three years of the project as follows

1) D7.8 *Standardization survey on standards involvement, technologies concerned and plan*
    a. Identification of ArchitectECA2030 related and relevant standards (m12)
2) D 1.5 *Report on requirements of standardization methods and metrics ensuring quality of homologation process (m16)*
3) D7.2 *External Stakeholder Strategy (m12)*
    a. Basis for
        i. Identification of standardization organizations
        ii. Providing input to the standardization organizations in which the project partners are involved.
4) D 3.9 *Elaboration of fail-operational strategies in terms of standardization (m25)*
5) *D5.4 Support of standardization activities for the elaborated methodology (m33)*
6) *D6.4 Consensus on validation results with standardization bodies (m36)*

In the Figure 3 is reported the plan for the standardization's deliverables.

[5] https://www.safetrans-de.org/de/Uploads/Aktuelle_Meldungen/SafeTRANS_AK_HS_Roadmap_v0.6.pdf?m=1520507227

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

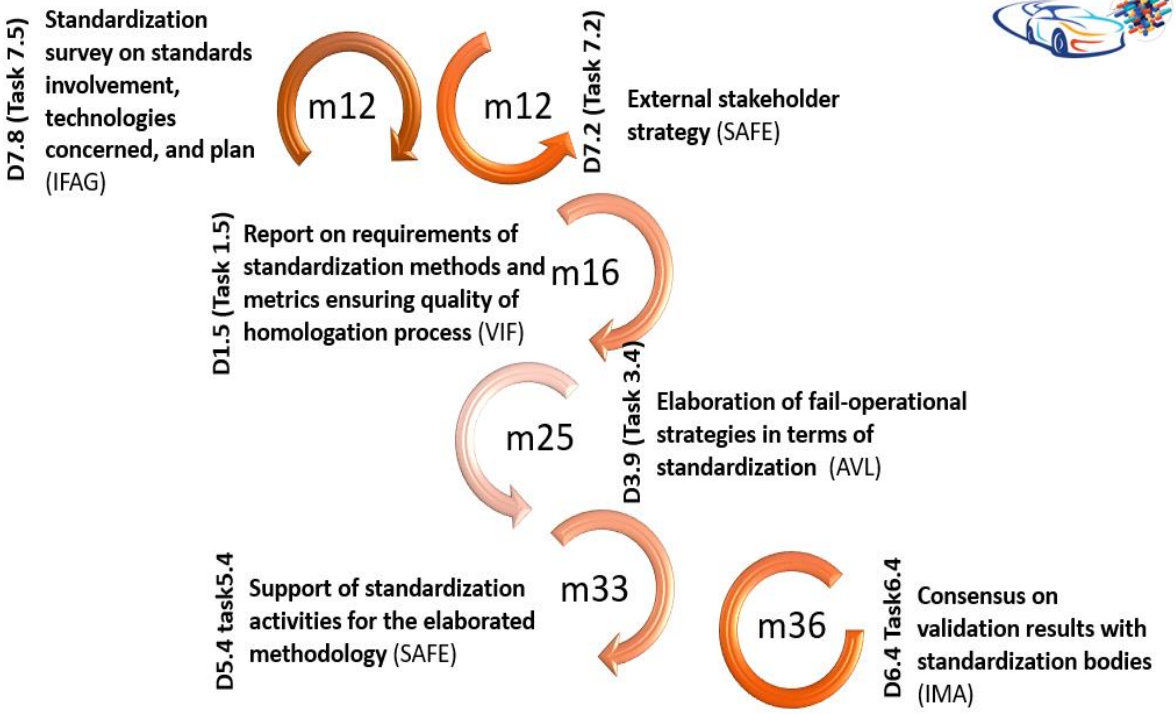


FIGURE 3 STANDARDIZATION DELIVERABLES PLAN

Legend:

m12 -> June 2021	m25 -> July 2022
m16 -> October 2021	m33 -> March 2023
	m36 -> June 2023

Testing and simulating the methodologies, functions and new technologies will be an essential factor for a correct certification. In this field standards plays a great role too. The goal in this context is to increase the compatibility and reproducibility. The simulation of models have to ensure the validity of the results in order to validate future driving functions and systems for automated vehicle.

Test equipment is another important factor to increase reproducibility when testing automated driving functions and to set uniform data acquisition requirements.

In the first phase of the project we concentrate on the following aspects:

1) Identify some properties of the regulations and search for trends
2) Gap analysis
    a. Selection of A_ECA2030 Standards relevant for the Demos and to which we would like to concentrate
    b. Identify the need of new standards
    c. How we conduct “Control” at different aggregation levels
3) Homologation: How ArchitectECA2030 can contributes to homologation.
    a. probably only those related to safety and security in the Vehicle

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

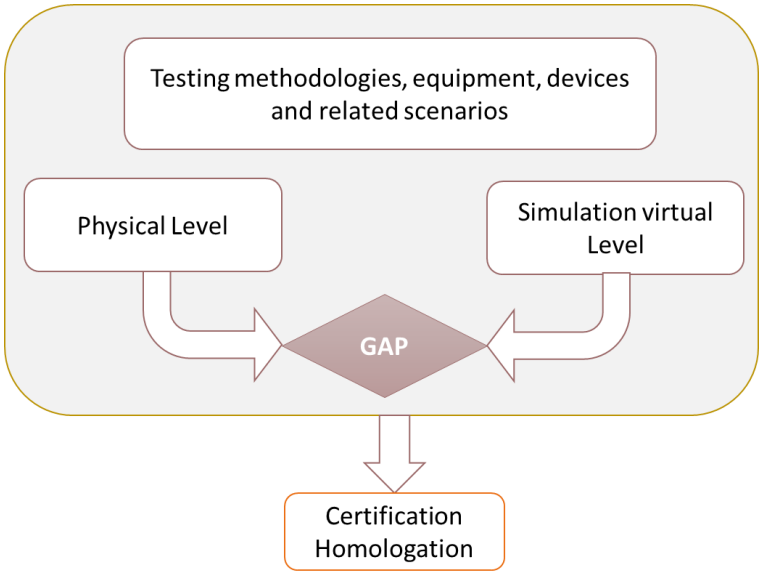


FIGURE 4 REPRESENTATION OF STANDARDIZATION PLAN AND CERTIFICATION

5 Standardization Survey

The survey in this deliverable 7.8 is complementary to the analysis realized in the Deliverable 1.1 -1.5. In this context each demonstrator was requested to map the standards in the ArchitectECA2030 V-model (e.g. Figure 3). We have used a template in order to standardize the requested information, see Table 1.

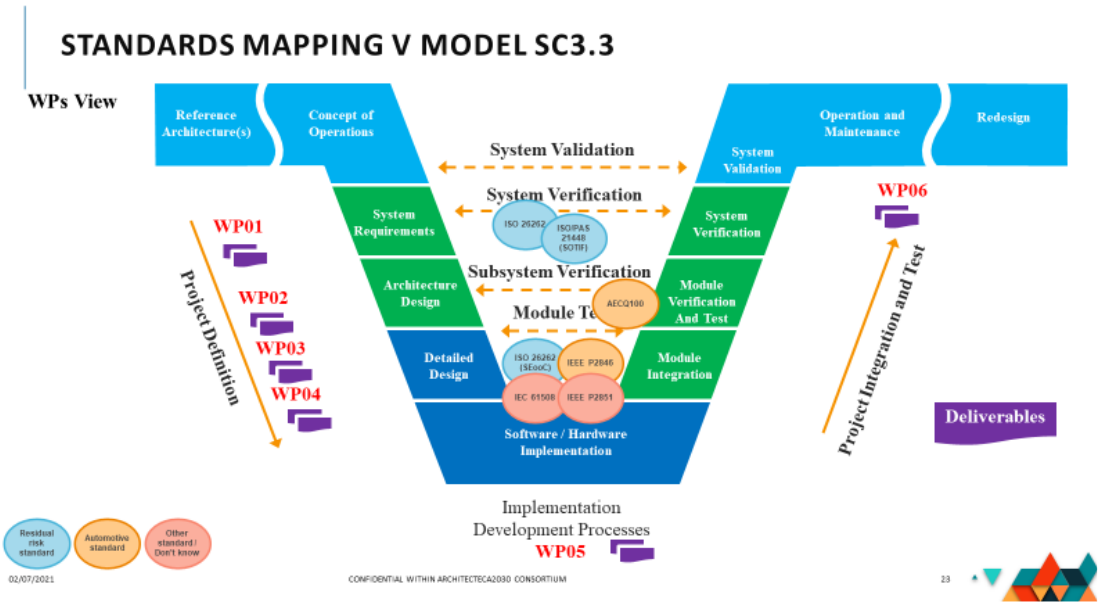


FIGURE 5 EXAMPLE OF V-MODEL MAPPING.

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

TABLE 1 TEMPLATE – SURVEY DESCRIPTION

<Standard short and long name>	ArchitectECA2030

Disclaimers:

1. In this survey 'Standard' is used to denote any set of specifications/set of rules that applies to development, implementation, V&V and Test, homologation and operation of CPS, regardless of whether this set is already a formal standard, a pre-standard, a standard proposal or a set of rules that (maybe) will become a standard one day.
2. Information should be provided as completely as possible. However, any question that is either not applicable for this standard and/or for which the answer is not known, can and should be left blank.

Formalia		
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these cannot be derived from the name already).		
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')		
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)		
Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	
	Technologies/methods/processes covered	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[ ] Requirements [ ] Development and Implementation [ ] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance		
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electromagnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).	
	Is **residual risk/probability of failure** handled in this standard? If so, how?		
ArchitectECA2030			

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?			WP/SC/Demonstrator: Partners:
If the Standard is used for a Use-Case/Demonstrator:			
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [ ] No [ ] Don't know yet
	If **Yes**:		
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[ ] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6 Standards Involved

Below the collection of the ArchitectECA2030 involved standards, identified by Supply Chains: perception, propulsion, connectivity and monitoring in relation to the related demonstrators. See also deliverables D1.1 – D1.5. Some of the standards are a reference for all the supply chains. Summary of the results on chapter 7.

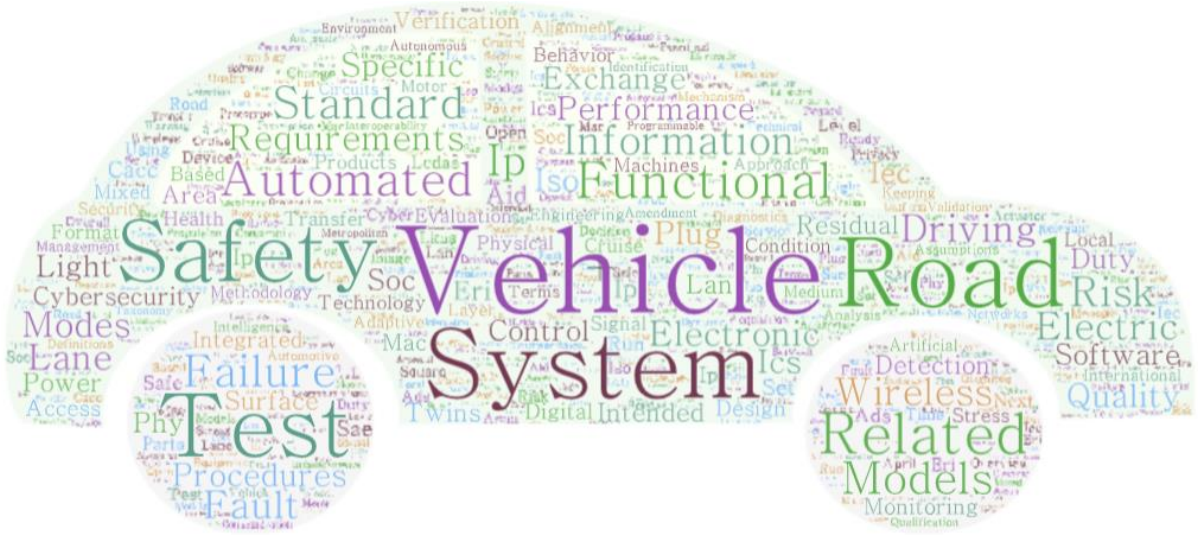


FIGURE 6 WORD-CLOUD OF THE STANDARDS' TITLES.

Disclaimers:

a) In this survey 'Standard' is used to denote any set of specifications/set of rules that applies to development, implementation, V&V and Test, homologation and operation of CPS, regardless of whether this set is already a formal standard, a pre-standard, a standard proposal or a set of rules that (maybe) will become a standard one day.

b) Information should be provided as completely as possible. However, any question that is either not applicable for this standard and/or for which the answer is not known, can and should be left blank.

6.1.1 ISO 17359:2018

ISO 17359:2018 **Condition monitoring and diagnostics of machines — General guidelines**	ArchitectECA2030
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these cannot be derived from the name already).	**ISO 17359:2018** **Condition monitoring and diagnostics of machines — General guidelines**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO**
Content / Coverage	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Scope of the Standard			
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**ISO 17359:2018 provides guidelines for condition monitoring and diagnostics of machines using parameters such as vibration, temperature, tribology, flow rates, contamination, power, and speed typically associated with performance, condition, and quality criteria. The evaluation of machine function and condition may be based on performance, condition or product quality.**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Industrial machines.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[ ] Requirements [ ] Development and Implementation [ ] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [**X**] not done at all	**Your line of work is…**

6.1.2 ISO 18129:2015

ISO 18129:2015 **Condition monitoring and diagnostics of machines — Approaches for performance diagnosis**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO 18129:2015** **Condition monitoring and diagnostics of machines — Approaches for performance diagnosis**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology,	**ISO 18129:2015 provides an introduction on how to apply performance monitoring and**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	(engineering) processes and/or organization):	**diagnostics for machines, groups of machines, up to complete industrial installation (equipment) typically covering the whole lifetime of the machines.**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Industrial machines.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[ ] Requirements [ ] Development and Implementation [ ] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [**X**] not done at all	**Your line of work is…**

6.1.3 ISO/IEC 25010

ISO/IEC 25010 **Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these cannot be derived from the name already).	**ISO/IEC 25010 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models; Version: ; Published: Mar 2011**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO/IEC**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**TC ISO/IEC JTC 1/SC 7 Software and systems engineering**
Content / Coverage	
Scope of the Standard	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The standard deals with quality metrics for software engineering in general.**
	Technologies/methods/processes covered	**Software engineering**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Only applicable to software engineering**
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [] Operation in the field [ ] Other (pls. specify): _____
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,		
	Short **description** of this relevance	**The standard specifies quality metrics that should mitigate failures of the system.**
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [**X**] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electromagnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		situations/scenarios that were not known/considered at design time) [X] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**Yes, Functional Suitability, Availability, Fault Tolerance, Recoverability, and Security of developed software is tackled in this standard.**

6.1.4 ISO/IEC TR 24028

ISO/IEC TR 24028 **Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO/IEC TR 24028 - Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence; Version: 1; Published: May 2020**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO/IEC**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/IEC JTC 1/SC 42 Artificial intelligence**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The standard is concerned with the general trustworthiness of AI applications. This includes methods to establish trustworthiness (e.g., explainability), associated threads and risks, and methods to assess reliability and safety.**
Technologies/methods/processes covered	**AI V&V**
Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE	**Systems providing or using AI**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')		
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** CPS V&V
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**Methods to assess availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems are given in the standard.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [**X**] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time)	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[X] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**Yes, mitigation strategies are given in the standard.**

6.1.5 AI Safety / The Landscape of AI Safety

AI Safety / The Landscape of AI Safety	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**AI Safety – Publications and initiatives dealing with all aspects related with trustworthy AI**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	none **yet**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	www.clais.org
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The standard focuses on a generally agreed version of a knowledge graph considering all areas that are related to AI safety. This includes verification and validation as well as ethical and moral questions, processes, and certification.**
Technologies/methods/processes covered	**All aspects dealing with safety for AI-based systems in the most general context.**
Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**No limitations regarding use. But the overall system has to deal with autonomous systems.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [**X**] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [**X**] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**The standard is relevant for all types of autonomous systems relying on AI technology. It describes the framework to be considered when applying verification and validation methods as well as certifications and goes beyond ordinary safety considerations. It also includes considering unintended consequences of autonomous systems.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

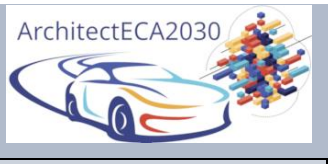
		situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator: We focus on trying to clarify whether the standard taxonomy can be applied in the context of autonomous driving. We may also contribute to the evolvement of the standard in the direction of autonomous driving. The work will be carried out as part of SC2 – Demonstrator: Formal-Method-based MonDev and SC4 – Demonstrator: Virtual Verification & Validation Framework** **Partners: TUG (in collaboration with AVL)**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [ ] No [X] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
	If **partly**: What is missing?	
	If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?	[X] Yes [ ] No [ ] Don't know yet

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**We will consider consequences of faults in the results of diagnosis/the MonDev to the overall system. Moreover, we will have a look at consequences of diagnosis to the overall risk.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [**X**] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**ISO 26262 or IEC 61508**

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

6.2.1 ISO15622:2018(E)

ISO15622:2018(E) **Adaptive Cruise Control Systems- Performance Requirements and Test Procedures**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO 15622:2018(E)** **Intelligent transport systems — Adaptive cruise control systems — Performance requirements and test procedures** **Third Edition 2018-09**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO (the International Organization for Standardization)**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**Technical Committee ISO/TC 204, Intelligent transport systems**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The standard refers to the technological and engineering aspects of Adaptive Cruise Control (ACC), specifically the performance requirements and test procedures for full speed range adaptive cruise control systems**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Technologies/methods/processes covered	**The goal of ACC is a partial automation of the longitudinal vehicle control and the reduction of the workload of the driver with the aim of supporting and relieving the driver in a convenient manner. The generic ACC system comprehends two classes: Full Speed Range ACC (FSRA) and Limited Speed Range ACC (LSRA). This document contains the basic control strategy, minimum functionality requirements, basic driver interface elements, minimum requirements for diagnostics and reaction to failure, and performance test procedures for ACC systems.**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**This document can be used as a system level standard by other standards, which extend the ACC to a more detailed standard, e.g. for specific detection and ranging sensor concepts or higher level of functionality. Therefore, issues like specific requirements for the detection and ranging sensor function and performance or communication links for co-operative solutions are not considered in this standard.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [**X**] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** **Research**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**This standard covers the performance requirements and specifically performance test procedures and methods for ACC systems.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly')	

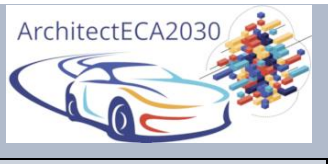
This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [X] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**NO**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP2/SC1/SC4 Automated Vehicle Demonstrator (VIF)** Partners: **VIF, DATA, IFAT**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [X] No [ ] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			[ ] No
		If **partly**: What is missing?	**Standard compliance of ACC for the demonstration purposes is not required.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There is also ISO20035:2019 (EN) on this topic. However, standard compliance of ACC function utilized for the use-case is not required for the demonstration purposes.**
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[X] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**In the corresponding VIF demonstrators, the propagation and evaluation of different systemic and synthetically generated faults during the functioning of the ACC operation will be emulated.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No
		If **partly**: What is missing?	**The standard contains and mentions only systemic failure at the subsystem level. Sensor signal quality and security aspects are not considered.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

6.2.2 ISO20035:2019(E)

ISO20035:2019(E) **Cooperative adaptive cruise control systems (CACC) - Performance requirements and test procedures**	

Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO20035:2019(E)** **Intelligent transport systems — Cooperative adaptive cruise control systems (CACC) — Performance requirements and test procedures** **First edition 2019-01**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO (the International Organization for Standardization)**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)		**Technical Committee ISO/TC 204, Intelligent transport systems**
Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The standard refers to the technological and engineering aspects of Cooperative Adaptive Cruise Control (CACC) which is an enhancement to the Adaptive Cruise Control (ACC) system by the addition of wireless communication with preceding vehicles and/or the infrastructure to augment the ACC active sensing capability. The document specifically discusses the performance requirements and test procedures for CACC systems.**
	Technologies/methods/processes covered	**Cooperative Adaptive Cruise Control (CACC) system is an expansion to existing Adaptive Cruise Control (ACC) control strategy by using wireless communication with preceding vehicles (V2V) and/or the infrastructure (I2V). Both multi vehicle V2V data and I2V infrastructure data are within the scope of this document. When V2V data is used CACC can enable shorter time gaps and more accurate gap control, which can help increase traffic throughput and reduce fuel consumption. It can also receive data from the infrastructure, such as recommended speed and time gap setting, to improve traffic flow and safety.** **This standard addresses two types of CACC: V2V, and I2V. Both types of CACC system require active sensing using for example radar, lidar, or camera systems. The following requirements are addressed in this standard:** • **classification of the types of CACC;** • **definition of the performance requirements for each CACC type;** • **CACC state transitions diagram;** • **minimum set of wireless data requirements;** • **test procedures.**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**The combined V2V and I2V CACC is not addressed in this standard. Also CACC:** • **does only longitudinal vehicle speed control;** • **uses time gap control strategy similar to ACC;** • **has similar engagement criteria as ACC.** **Coordinated strategies to control groups of vehicles, such as platooning, in which vehicle controllers base their control actions on how they affect other vehicles, and may have a very short following clearance gap are not within the scope of this standard. CACC system**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		operates under driver responsibility and supervision (i.e., SAE Level 3 or below). **This standard is applicable to motor vehicles including light vehicles and heavy vehicles.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [**X**] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** **Research**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**This standard covers the performance requirements and specifically performance test procedures and methods for CACC systems.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?		**NO**
ArchitectECA2030			
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?			**WP2/SC1/SC4 Automated Vehicle Demonstrator (VIF)**
			Partners: **VIF, DATA, IFAT**
If the Standard is used for a Use-Case/Demonstrator:			
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes**:		
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	**Standard compliance of ACC for the demonstration purposes is not required.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There is also ISO15622:2018 (EN) on this topic. However, standard compliance of ACC function utilized for the use-case is not required for the demonstration purposes.**
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**In the corresponding VIF demonstrators, the propagation and evaluation of different systemic and synthetically generated faults during the functioning of the ACC operation will be emulated.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		If **partly**: What is missing?	**The standard contains and mentions only systemic failure at the subsystem level. Sensor signal quality and security aspects are not considered.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

6.2.3 ISO 17387:2008(E)

ISO 17387:2008(E) **Lane change decision aid systems (LCDAS) —** **Performance requirements and test procedures**	

Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO17387:2008(E)** **Intelligent transport systems — Lane change decision aid systems (LCDAS) — Performance requirements and test Procedures** **01-05-2008**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO (the International Organization for Standardization)**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**Technical Committee ISO/TC 204, Intelligent transport systems**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Lane Change Decision Aid Systems (LCDAS) warn the driver against collisions that may occur due to a lane change manoeuvre. LCDAS are intended to supplement the vehicle's interior and exterior rear-view mirrors, not eliminate the need for such mirrors. This standard provides references to technological and engineering requirements as well as test procedures of such systems.**
Technologies/methods/processes covered	**This International Standard specifies system requirements and test methods for Lane Change Decision Aid Systems (LCDAS).**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**LCDAS are fundamentally intended to warn the driver of the subject vehicle against potential collisions with vehicles to the side and/or to the rear of the subject vehicle, and moving in the same direction as the subject vehicle during lane change manoeuvres. This standardization addresses LCDAS for use on forward moving cars, vans and straight trucks in highway situations. LCDAS are intended to detect vehicles to the rear and sides of the subject vehicle. When the subject vehicle driver indicates the desire to make a lane change, the system evaluates the situation and warns the driver if a lane change is not recommended. LCDAS are not meant to encourage aggressive driving. The absence of a warning will not guarantee that the driver can safely make a lane change manoeuvre. The system will not take any automatic action to prevent possible collisions. Therefore, the responsibility for the safe operation of the vehicle remains with the driver.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [**X**] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [X] optional [ ] not done at all	**Your line of work is…** **Research**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance		
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[X] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [X] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP2/SC1/SC4 Automated Vehicle Demonstrator (VIF)** Partners: **VIF, DATA, IFAT**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [X] No [ ] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		If **partly**: What is missing?	**Standard compliance of LCDAS for the demonstration purposes is not required.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There are also relevant regulations (UNECE Regulation 157) on this topic. However, compliance of LCDAS function utilized for the use-case is not required for the demonstration purposes.**
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**In the corresponding VIF demonstrators, the propagation and evaluation of different systemic and synthetically generated faults during the functioning of the ALKS operation will be emulated.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No
		If **partly**: What is missing?	**The information on quantifying how the residual risk accumulates is not described.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There are also relevant & regulations: UNECE Regulation 157, ISO17361:2007, ISO11270:2014 on this topic. However, standard compliance of LCDAS function utilized for the use-case is not required for the demonstration purposes.**

6.2.4 SAE J2954

SAE J2954 **Surface Vehicle – Wireless Power Transfer for Light-Duty Plug-in/Electric Vehicles and Alignment Methodology**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these cannot be derived from the name already).	**SAE J2954:2020 Surface Vehicle – Wireless Power Transfer for Light-Duty Plug-in/Electric Vehicles and Alignment Methodology** **(Standard / Published: 2020-10-20 / Previous Versions: 2019-04-23, 2017-11-27, 2016-05-26)**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**SAE International**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)		**Motor Vehicle Council / Hybrid - EV Committee**	
Content / Coverage			
Scope of the Standard			
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The SAE J2954 standard establishes an industry-wide specification that defines acceptable criteria for interoperability, electromagnetic compatibility, EMF, minimum performance, safety, and testing for wireless power transfer (WPT) of light-duty plug-in electric vehicles.** **SAE J2954 addresses unidirectional charging, from grid to vehicle. This standard is intended to be used in stationary applications (charging while vehicle is not in motion). In this version, only above-ground (surface mounted) installations are covered.** **SAE J2954 contains requirements for safety, performance, and interoperability. It also contains recommended methods for evaluating electromagnetic emissions.**	
	Technologies/methods/processes covered	**Focus on safety, EMF, performance and interoperability.**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Applicable for vehicles with a coil ground clearance less than 250 mm and for a maximum grid input power of 11.1 kVA.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [ ] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** Research and Teaching
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**Wireless charging is a way to transfer energy to an electric vehicle automatically. The charging**	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		system is typically formed by two components – one as part of the vehicle and one external component – provided by independent parties. This will lead to many combinations that were never used together in the field before. All components have to comply with a minimum set of functionalities that makes it possible to check interoperability and safety at runtime.
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[X] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [X] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	• **This standard mainly refers to other standards (in development) that deal with residual risk of components.** ○ **Vehicle components in a WPT system shall be designed**

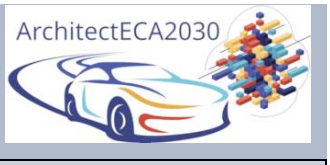
This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		according to functional safety in ISO 26262 related to possible hazards caused by malfunctioning behavior of safety-related electrical systems, including interaction of these systems. ○ **UL is writing a standard (UL 2750, in development) to cover the safety aspects of the off-vehicle components and operation of WPT.** • **WPT system designs should avoid a single point failure wherever possible.**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		SC1 / Demonstrator D1.1 "Foreign object detection within a wireless charger" Partners: • TU Dresden (TUDR)
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [ ] No [X] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
	If **partly**: What is missing?	
	If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?	[X] Yes [ ] No [ ] Don't know yet
	If **Yes:**	
	Shortly **describe** how residual risk/probability of failure will be considered:	**The use case is intended to show the residual risk in the detection of metallic and/or magnetic foreign objects in the operating area of a wireless charging system that uses selected passive inductive sensors for detection.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No
		If **partly**: What is missing?	• **The standard specifies that safety verification must occur prior to the start of power transfer and also during power transfer. However, the standard does not specify any measures to monitor or test the system for detecting foreign metallic objects and thus to ensure its functionality during the operating life of the wireless charging system.** • **Environmental conditions are not considered in the standard. The standard presumes that foreign metallic objects are located on the surface of the ground assembly unit – the part outside of the vehicle. If, for example, the ground assembly unit is covered with ice or snow in the winter time a light foreign object has a higher distance to the sensors. Can an object in this situation be detected?** • **Cybersecurity aspects are not considered in the standard. The preferred location of the foreign object sensors is the ground assembly unit – the part outside of the vehicle. If, for example, a foreign object is placed by an attacker beneath the underbody of the vehicle it is perhaps in the operating area of the wireless charger but the distance to the sensors is very high. Is such an object detectable?**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**No**

6.2.5 ISO26262:2018

ISO26262:2018 **Road Vehicles – Functional Safety**	
Formalia	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).		**ISO26262:2018 Road Vehicles – Functional Safety** **(12 Parts, ISO2626-1:2018 – ISO2626-12:2018)** **Published 12/2018 (previous version '…:2011')**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')		**ISO – International Organization for Standardization**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)		**ISO/TC (Technical Committee) 22/SC (Subcommittee) 32** **Electrical and electronic components and general system aspects**
Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**This document describes a framework for functional safety to assist the development of safety-related E/E systems for road vehicles. The standard helps to build the safety case for an item or element of the system, which is the evidenced-based argumentation that the functional safety is achieved. The item in the context of ISO 26262 is defined as system that realizes a function on vehicle level, which is observable by the costumer (example ACC).** **The system itself combines at least one sensor, one controller and one actuator.**
	Technologies/methods/processes covered	**Safety considerations need to start together with the conceptual phase of a series production development project. As first step, Hazard and Operability Study (HAZOP) and Hazard and Risk Assessment (HARA) are conducted while in parallel architectural concepts for the item are designed.** **These steps help to define safety goals which are the "top level" safety requirements. They need to need to be fulfilled to a certain integrity level (see below). In a subsequent step, the safety goals are translated to functional safety** requirements and technical **safety requirements. These requirements are then allocated to elements of the conceptual architecture and need to be fulfilled in further design steps (HW, SW design).**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE	**The standard needs to be applied to avoid unreasonable risks due to hazards caused by**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Failure of E/E systems or unintended behavior of an item.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [**X**] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [X] optional [ ] not done at all	**Your line of work is…** **R&D**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**The safety case is the evidence-based proof that functional safety is achieved and can be used as support for approval processes of automated and conventional vehicles.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[X] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [X] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [X] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time)	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**A risk assessment is covered in the ISO 26262 using a HARA methodology. In a first step, a Hazard and Operability Study HAZOP needs to be conducted for a certain use-case. This study helps to identify critical situations and system states that lead to a hazardous situation.** **The risk of these situations is then evaluated by performing a Hazard and Risk Assessment (HARA) to quantify the risk as combination of severity x frequency resp. severity x exposure * controllability. The severity is depending on the effects of a hazard on vehicle participants ranging from no injuries to fatalities.**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC1 /Demonstrator 2.1/2.2** **Partners: ViF/IFAT**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes**:	Standard compliance of for the demonstration purposes is not required.
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[ ] Yes [ ] No [**X**] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

6.2.6 ISO/PAS 21448:2019

ISO/PAS 21448:2019 **Road Vehicles – Safety of the intended functionality**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO/PAS 21448:2019 Road Vehicles – Safety of the intended functionality** **(PAS: Publicly Available Specification; Under development is ISO/DIS 21448, to appear, with DIS: Draft International Standard)** **Published 11/2019**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/TC (Technical Committee) 22/SC (Subcommittee) 32** **Electrical and electronic components and general system aspects**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology,	**"This document is intended to be applied to intended functionality where proper situational awareness is critical to safety, and where that situational awareness is derived**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	(engineering) processes and/or organization):	**from complex sensors and processing algorithms; especially emergency intervention systems (e.g. emergency braking systems) and Advanced Driver Assistance Systems (ADAS) with levels 1 and 2 on the OICA/SAE standard J3016 automation scales. This edition of the document can be considered for higher levels of automation, however additional measures might be necessary. This document is not intended for functions of existing systems for which well-established and well-trusted design, verification and validation (V&V) measures exist at the time of publication (e.g. Dynamic Stability Control (DSC) systems, airbag, etc.).”**	
	Technologies/methods/processes covered	**ISO/PAS 21448 presents a process that complements the ISO 26262 for unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is**	
	Pre-conditions and/or constraints for applying this standard (i.e., ‘only for SAE Autonomy level L2 and below systems’, ‘only for ‘military-grade products’, ‘only for…’)	**Standard is extension to ISO 26262 and aims to compensate parts where ISO 26262 is not sufficient.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [ ] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** **R&D**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**L3 + vehicles heavily depend on perception and perception algorithms as they need to gain a scene understanding of the surrounding environment around the vehicle. Therefore, the relevance of the standard increases with the degree of automation.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [X] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**In addition to the 4 types of scenarios (known & unknown; safe and unsafe), the standard provides in section 11 (validation) of the SoTIF** **In the Validation section, which targets area 3 of the SOTIF process, different methods are described to evaluate the residual risk.** **A** — **Validation of robustness to Signal-to-Noise Ratio degradation (e.g. by noise injection testing)** **B** — **Verification of the architectural properties including independence, if applicable** **C** — **In the loop testing on randomized test cases (derived**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			from a technical analysis and by error guessing)
		D	Randomized input testsa
		E	Vehicle level testing on selected test cases (derived from a technical analysis and by error guessing)
		F	Long term vehicle test
		G	Fleet tests
		H	Test derived from field experience
		I	Tests of corner casesb and reasonably foreseeable misuse
		J	Comparison with existing systems
		K	Simulation of selected scenarios
		L	Analysis of worst case scenarios
		a Randomized input tests can include erroneous patterns e.g. in the case of image sensors adding flipped images, altered image patches; or in the case of radar sensors adding ghost targets to simulate multi-path returns. b A corner case is a rare or unusual condition.	

ArchitectECA2030			
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?			**Relevant for SC1,** **Partners: VIF**
If the Standard is used for a Use-Case/Demonstrator:			
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [X] No [ ] Don't know yet
	If **Yes**:		**Standard compliance of for the demonstration purposes is not required.**
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [**X**] Partly

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			[ ] No
		If **partly**: What is missing?	**Sotif Risk Safety-Levels as known in the ISO 26262 (ASIL) are no content of ISO 21448/ SotiF**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

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

6.3.1 IEEE Std 1856TM-2017

IEEE Std 1856TM-2017 **IEEE Standard Framework for Prognostics and Health Management of Electronic Systems**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IEEE Std 1856TM-2017 - IEEE Standard Framework for Prognostics and Health Management of Electronic Systems. Approved 7 September 2017**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**Prognostics and Health Management of Electronic Systems Working Group, IEEE Reliability Society**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**This standard provides information on implementation of prognostics and health management (PHM) for electronic systems. It helps in selection of PHM and strategies.**
Technologies/methods/processes covered	**It covers all aspects of PHM of electronic systems, including definitions, approaches, algorithms, sensors and sensor selection, data collection, storage and analysis, anomaly detection, diagnosis, decision and response effectiveness, metrics, life cycle cost of implementation, return on investment, and documentation.**
Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**The use of this standard is not required throughout the industry. The knowledge and understanding of following standards is indispensable for the application of this standard. These are IEEE Std 15288, Systems and software engineering—System life cycle processes and IEEE Std 12207, Systems and software engineering—Software life cycle processes.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [ ] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** R&D
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**The standard describes the PHM of electronic systems in general. It contains just brief note about the cars which can be treated as a swarm of systems. The standard is not relevant to homologation.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**They are not handled.**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator:** **WP1,2,3,6** **SC2** **Demonstrator 2.2 - Condition Monitoring and Predictive Maintenance of Inverter Power Components**
		Partners: BUT
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [X] No [ ] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
	If **partly**: What is missing?	
	If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?	[ ] Yes [ ] No [X] Don't know yet
	If **Yes:**	
	Shortly **describe** how residual risk/probability of failure will be considered:	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

6.3.2 ISO 26262

ISO 26262 **Road Vehicles – Functional Safety**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO26262:2018 Road Vehicles – Functional Safety** **(12 Parts, ISO2626-1:2018 – ISO2626-12:2018)** **Published 12/2018 (previous version '…:2011')**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO – International Organization for Standardization**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/TC (Technical Committee) 22/SC (Subcommittee) 32** **Electrical and electronic components and general system aspects**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Engineering processes and methods (and some organizational issues) to ensure functional safety of E/E systems installed in road vehicles (trucks, cars, etc.), excluding mopeds by prescribing a certain design, implementation and Test (incl. validation and verification) methodology.** **The 12 parts of the standard deal with:** **1) Vocabulary** **2) Management of functional safety** **3) Concept phase** **4) Product development at the system level** **5) Product development at the hardware level**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		6) Product development at the software level **7) Production, operation, service and decommissioning** **8) Supporting processes** **9) Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis** **10) Guidelines on ISO 26262** **11) Guidelines on application of ISO 26262 to semiconductors** **12) Adaptation of ISO 26262 for motorcycles**	
	Technologies/methods/processes covered	**Focus on hazard and risk analysis, verification, validation, test**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**In principle, ISO26262 can (and should) be applied to any development of any E/E system. It ensures that – with a very high probability – the system behaves as specified. However, ISO26262 cannot answer the following questions** **(1) Is the specification correct (i.e., is a system that behaves according to this specification indeed functional safe)?** **(2) Is the specification complete (i.e., are all situations/use-cases that the system might encounter during operation covered)?** **a. … even those where users deliberately misuse the system?**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [**?**] Homologation [**X**] Operation in the field [**X**] Other (pls. specify): _Production, Decommissioning (see Part 7)_	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**The question of whether an implementation fulfills a specification is a very important one also for L3+ cars and thus ISO26262 is an important part of their V&V&T. However, for**	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		L3+ cars applying only ISO26262 is not sufficient for showing functional safety.
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [X] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**Each item (i.e., the system, each component, sub component, software item,…) is assigned a set of 'hazardous events' (i.e. events in which the item will cause damage; example: failing brakes).** **Each 'hazardous event' is classified according to** **a) S – Severity: The severity of the damage resp. the severity of the injuries caused by the item**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		b) E – Exposure: Relative probability that the hazardous event occurs during operation **c) C – Controllability: If the hazardous event occurs, how likely is it that the driver can prevent the damage?** **Each is then assigned an 'automotive safety integrity (ASIL) level', ranging from QM (Quality Management, no safety risk) via ASIL A (very low risk) to ASIL D (very high risk), according to these three parameters.** **Much simplified, the ASIL of an item (i.e. the system, component, software…) is then the highest ASIL of the hazardous events identified for it.** **Simplified again, for each ASIL level, ISO 26262 defines the needed methods and processes (including definition of safety goals and safety architectures, types and amount of validation, verification and test, etc.) that need to be performed in order to guarantee that the remaining (residual) risk of an item with this ASIL level is below an acceptable thresholds. For ASIL A items, only very few tests need to be done, for ASIL D an extensive safety case has to be devised and implemented. If properly done, at the end of the process each item has a sufficiently low residual risk of not being functional safe.**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator:** **Demonstrator 2.1** **Partners: IFAT**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [**X**] No [ ] Don't know yet

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6.4 CONNECTIVITY: SC3 Failure modes, fault detection and residual risk for safety and security in connectivity systems.

6.4.1 Demo 3.1 - ISO 26262

ISO 26262 **Road Vehicles – Functional Safety**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO26262:2018 Road Vehicles – Functional Safety. 12 Parts, ISO2626-1:2018 – ISO2626-12:2018. Published 12/2018.**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO – International Organization for Standardization**[6]**.**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/TC 22, SC 32 Electrical and electronic components and general system aspects**[7,8]**.**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Assessment and quantification of possible failures according to ISO 26262, (together with IEC 61508 and ISO/PAS 21448).** **ISO 26262 address safety-related systems that include one or more electrical/electronic (E/E) systems. The risk classification scheme ASIL (automotive safety integrity level) is a key component of ISO 26262 and defined in part 9. The ASIL scheme is focusing on the harm to the driver and other road users but is not addressing the technologies used in the system. Each safety requirement is assigned an ASIL of A, B, C, or D, where D is the most safety critical processes/ strictest testing regulations.** **Engineering processes and methods (and some organizational issues) to ensure functional safety of E/E systems installed in road vehicles (trucks, cars, etc.), excluding mopeds by prescribing a**

[6] https://www.iso.org/home.html

[7] TC: Technical Committee

[8] SC: Sub Committee

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		certain design, implementation, and test (incl. validation and verification) methodology. **The 12 parts of the standard deal with:** **13) Vocabulary** **14) Management of functional safety** **15) Concept phase** **16) Product development at the system level** **17) Product development at the hardware level** **18) Product development at the software level** **19) Production, operation, service, and decommissioning** **20) Supporting processes** **21) Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis** **22) Guidelines on ISO 26262** **23) Guidelines on application of ISO 26262 to semiconductors** **24) Adaptation of ISO 26262 for motorcycles**
	Technologies/methods/processes covered	**Focus on hazard and risk analysis, verification, validation, and test.**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**An established family of standards addressing functional safety management, HW random and systematic failures. Main issues:** • **Autonomous vehicle complexity (multiple items combined, thousands of safety requirements) requires a more agile development flow.** • **No autonomous vehicles system architecture references.** • **The PMHF targets do not match with modern technologies/components.** • **ISO 26262-6 is difficult/very challenging if applied to open-source SW.** • **Guidelines are missing on how to apply ISO 26262 to Artificial Intelligence.** **In principle, ISO26262 can (and should) be applied to any development of any E/E system. It ensures that – with a very high probability – the system behaves as specified. However, ISO26262 cannot answer the following questions:** **(3) Is the specification correct (i.e.., is a system that behaves according to this specification indeed functional safe)?** **(4) Is the specification complete (i.e.., are all situations/use-cases that the system might encounter during operation covered)?** **a) … even those where users deliberately misuse the system?**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [?] Homologation [**X**] Operation in the field [**X**] Other (pls. specify): Production, Decommissioning (see Part 7).	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**The question of whether an implementation fulfills a specification is a very important one also for L3+ cars and thus ISO26262 is an important part of their V&V&T. However, for L3+ cars applying only ISO26262 is not sufficient for showing functional safety.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [**X**] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**Each item (i.e., the system, each component, sub-component, software item,) is assigned a set of 'hazardous events' (i.e., events in which the item will cause damage; example: failing brakes).** **Each 'hazardous event' is classified according to** **d) S – Severity: The severity of the damage resp. the severity of the injuries caused by the item.** **e) E – Exposure: Relative probability that the hazardous event occurs during operation.** **f) C – Controllability: If the hazardous event occurs, how likely is it that the driver can prevent the damage?** **Each is then assigned an 'automotive safety integrity (ASIL) level', ranging from QM (Quality Management, no safety risk) via ASIL A (very low risk) to ASIL D (very high risk), according to these three parameters.** **Much simplified, the ASIL of an item (i.e., the system, component, software…) is then the highest ASIL of the hazardous events identified for it.** **Simplified again, for each ASIL level, ISO 26262 defines the needed methods and processes (including definition of safety goals and safety architectures, types and amount of validation, verification and test, etc.) that need to be performed in order to guarantee that the remaining (residual) risk of an item with this ASIL level is below an acceptable threshold. For ASIL A items, only very few tests need to be done, for ASIL D an extensive safety case has to be devised and implemented. If properly done, at the end of the process each item has a sufficiently low residual risk of not being functional safe.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6.4.2 Demo 3.1 - ISO/PAS 21448

ISO/PAS 21448 **Road Vehicles – Safety of the intended functionality**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO/PAS 21448:2019 Road Vehicles – Safety of the intended functionality** **(PAS: Publicly Available Specification; Under development is ISO/DIS 21448, to appear, with DIS: Draft International Standard)** **Published 11/2019.**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO – International Organization for Standardization**[9].
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/TC (Technical Committee) 22/SC (Subcommittee) 32** **Electrical and electronic components and general system aspects**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Requirements and specifications for defining the methodology for identifying residual risks for connectivity systems for automated and connected vehicles in link with the ISO/PAS 21448 framework. Propose a methodology for risk estimations of connectivity systems considering the planned system integrity and dependability measures based on the framework. Assessment and quantification of possible failures according to ISO/PAS 21448, (together with ISO 26262 and IEC 61508).** **ISO/PAS 21448 provides guidance on the applicable design, verification and validation measures needed to achieve the safety of the intended functionality (SOTIF). Examines whether a needed safety functionality is successfully delivered in the absence of a failure, such as performance limitations (e.g., systems, subsystems, sensors, unexpected road environment changes).**

[9] https://www.iso.org/home.html

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		The absence of unreasonable risks due to hazards resulting from functional insufficiencies of the intended functionality [of the E/E system/product] or by reasonably foreseeable misuse is referred to as Safety of the Intended Functionality (SOTIF). ISO 21448 provides guidance on the applicable design, verification and validation measures needed to achieve the SOTIF.	
	Technologies/methods/processes covered	**Focus on design processes, verification, and validation methods**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**New standard targeting:** • **The inadequacy/inefficiency of the function to correctly comprehend the situation and operate safely.** • **Insufficient robustness of the procedure/function concerning sensor input variations or diverse environmental conditions.** **Main issues:** • **The standard is at a high level to produce consistent/interoperable industry practices.** • **Not clear enough which are the different requirements between autonomous vehicle levels (L3/L4/L5).** • **Several annexes (e.g., machine learning) needs extra work.** **ISO 21448 is applied when ISO 26262 alone is not sufficient anymore (e.g., because the system behavior cannot fully be specified due to its complexity and/or its openness). Thus, ISO 21448 is aiming at (design and V&V of) L3+ cars.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [ ] Development and Implementation [**X**] Verification, Validation, Test **[Not yet, but high potential]** Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all	**Your line of work is…**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,		
	Short **description** of this relevance	**ISO 21448 provides a way to cope with (a) incomplete and (b) erroneous specifications. Whereas ISO 26262 solves the problem of whether the systems functions are correct according to the specification, ISO 21448 also asks whether the functions are sufficient to guarantee safety in any scenario of any use-case for which the system was build. Thus, it is highly relevant for L3+ cars.**
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [X] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro-magnetic interference), ageing, accidental mechanical stress, etc. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [X] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Is **residual risk/probability of failure** handled in this standard? If so, how?	**ISO 21448 considers four types of scenarios to handle:**
		1. **Known scenarios (i.e., scenarios of which the engineers know that they can occur within an intended Use-Case of the system/product) in which the system is known to behave safe.**
		   - **Need not be handled.**
		2. **Known scenarios in which the system is not known to behave safe.**
		   - **These are handled via methods from e.g., ISO 26262 (slightly extended to include intended functionality and foreseeable misuse) to achieve safe behavior and a sufficient low residual risk.**
		   - **Scenarios in this class thus 'move into class 1' above, leaving this class (ideally) empty (or at least with only a few, highly improbable scenarios).**
		   - **This class also (typically) includes.**
		     - **Sensor faults or other causes of misperception of the environment**
		     - **Foreseeable misuse**
		3. **Unknown scenarios (i.e., scenarios that were unknown to engineers at design time) for which the system is not known to behave safe.**
		   - **This case is typically handled by either or both of**
		     - **Employment of methods similar to fail-aware and fail-operational concepts ('Recognizing that the system is in an unknown scenario (fail-aware) leads to safe (probably degraded) behavior (fail-operational)**
		     - **Restriction of the Use-Cases**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		○ **With this argument, also Class 3 scenarios are 'moved to' classes 2 and 1.** **4. The fourth case, unknown scenarios with known safe behavior is not considered.** **A safety case with ISO 21448 typically includes am argument that the residual risk of a system is acceptable because it has been proven to have this residual risk in Class 1 above (using ISO 26262 methods) and Class 2 and Class 2 are small enough so that there is no relevant residual risk there, either.**

6.4.3 Demo 3.1 - ISO 4804

ISO/TR 4804 **Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO/TR 4804:2020 Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation** **(TR: Technical Report)** **Published 12/2020** **This standard is based upon a whitepaper titled "Safety first for Automated Driving" published by various OEMs, Tier Suppliers and Technology Providers (see below); the whitepaper is available – amongst others – at** **https://www.daimler.com/innovation/case/autonomous/safety-first-for-automated-driving.html . All information in this survey is taken from the whitepaper, not from the actual standard document. However, according to the table of contents of the standard from the ISO website, ~90% of the chapter names in the whitepaper and the standard are the same (and therefore presumably the content is quite similar, too).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO – International Organization for Standardization[10].**

[10] https://www.iso.org/home.html

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/TC (Technical Committee) 22** **Road Vehicles (no subcommittee assigned yet)** **Publishers/Authors of the whitepaper (see above):** **APTIV (was: Delphi Automotive), Audi, Baidu Apollo, BMW, Continental, Daimler, FCA (Fiat Crysler Automobiles), HERE (was: Smart2Go, Map24, Navteq, Ovi Maps and Nokia Maps), Infineon, Intel, VW**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Processes and methods – often based upon a combination of existing methods and standards, i.e., ISO26262, ISO21448 SOTIF and similar – for a comprehensive approach to safety and security for L3 and L4 automated cars.**
Technologies/methods/processes covered	**The followed approach is to break down safety principles into safety by design capabilities, elements and architectures, each of which should be validated by existing approaches (i.e., by methods from ISO 26262, ISO21448, and others) and which together are meant to guarantee safety (and security). The standard defines:** - **12 (safety and security) principles of automated driving.** - **7 fail-safe and 6 fail-degraded capabilities that the ECA must implement (capabilities are mapped to the 12 principles.** - **5 challenges for V&V and Test; each challenge defines what must be shown by which means/methods during V&V&Test (in addition to what must be shown by application of the existing standards anyway) in order for the 12 principles to hold (and thus for the system to be safe and secure).**
Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Aims at SAE Level 3 and Level 4 cars.**
To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [?] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**The approach outlined in this standard (see above under 'technologies covered') will be highly relevant for V&V&Test of L3 and L4 ECAs; it has the potential to become THE one standard that is needed for showing safety and security for L3 and L4 cars (with the disclaimer that it references and builds upon other, existing standards, and thus the referenced standards will be needed, too).**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [**X**] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [**X**] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).	
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**Not directly, but indirectly by relying upon other existing standards.**	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6.4.4 Demo 3.1 - SAE J2954

SAE J2954 **Surface Vehicle – Wireless Power Transfer for Light-Duty Plug-in/Electric Vehicles and Alignment Methodology**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**SAE J2954:2020 Surface Vehicle – Wireless Power Transfer for Light-Duty Plug-in/Electric Vehicles and Alignment Methodology** **(Standard / Published: 2020-10-20 / Previous Versions: 2019-04-23, 2017-11-27, 2016-05-26)**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**SAE - SAE International[11].**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**Motor Vehicle Council / Hybrid - EV Committee**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The SAE J2954 standard establishes an industry-wide specification that defines acceptable criteria for interoperability, electromagnetic compatibility, EMF, minimum performance, safety, and testing for wireless power transfer (WPT) of light-duty plug-in electric vehicles.** **SAE J2954 addresses unidirectional charging, from grid to vehicle. This standard is intended to be used in stationary applications (charging while vehicle is not in motion). In this version, only above-ground (surface mounted) installations are covered.** **SAE J2954 contains requirements for safety, performance, and interoperability. It also contains recommended methods for evaluating electromagnetic emissions.**
Technologies/methods/processes covered	**Focus on safety, EMF, performance and interoperability.**
Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE	**Applicable for vehicles with a coil ground clearance less than 250 mm and for a maximum grid input power of 11.1 kVA.**

[11] https://www.sae.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')		
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [ ] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**Wireless charging is a way to transfer energy to an electric vehicle automatically. The charging system is typically formed by two components – one as part of the vehicle and one external component – provided by independent parties. This will lead to many combinations that were never used together in the field before. All components have to comply with a minimum set of functionalities that makes it possible to check interoperability and safety at runtime.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar)	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**SC1 / Foreign object detection system within a wireless charging system** **Partners: TU Dresden (TUDR)**

6.4.5 Demo 3.1 - IEC 61508

IEC 61508: **Functional safety of electrical/electronic/programmable electronic safety-related systems.**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IEC 61508 "Functional safety of electrical/ electronic/ programmable electronic safety-related systems", (April 2010).** **The international standards consist of seven parts (see below).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IEC - International Electrotechnical Commission.**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**TC 65/SC 65A - System aspects.** **The IEC has a dedicated technical advisory committee on safety (ACOS) which guides and coordinates IEC work on safety and ensures that all IEC Standards address safety issues.**
Content / Coverage	

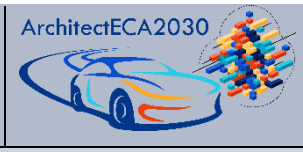
This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Assessment and quantification of possible failures according to ISO 61508, (together with IEC 26262 and ISO/PAS 21448).** **IEC 61508 address aspects to be considered when electrical/ electronic/ programmable electronic (E/E/PE) systems are used to carry out safety functions. Requirements for ensuring that systems are designed, implemented, operated, and maintained to provide the required safety integrity level (SIL). ISO 26262 is the adaptation of the IEC 61508 series of standards to address the sector-specific needs of E/E systems within road vehicles.** **This standard consists of seven parts:** • **IEC 61508-1: 2010: General requirements.** • **IEC 61508-2: 2010: Requirements for E/E/PE safety-related systems.** • **IEC 61508-3: 2010: Software requirements.** • **IEC 61508-4: 2010: Definitions and abbreviations.** • **IEC 61508-5: 2010: Examples of methods for the determination of safety integrity levels.** • **IEC 61508-6: 2010: Guidelines on the application of IEC 61508-2 and IEC 61508-3.** • **IEC 61508-7:2010: Overview of techniques and measures.** **In addition, the following related documents:** • **IEC 61508: 2010 CMV (Standard): Parts 1 to 7 together with a commented version.** • **IEC TR 61508-0: 2005 (Technical report): Functional safety and IEC 61508.** • **IEC TS 61508-3-1: 2016 (Technical specification): SW requirements - Reuse of pre-existing SW elements to implement all or part of a safety function.**
	Technologies/methods/processes covered	**The main purpose is to describe a (risk-based) methodology for specifying and realizing instrumented safety systems so that an acceptable level of functional safety is achieved.** **IEC 61508 is considered as a "basic or umbrella" standard for functional safety and covers the entire safety lifecycle of E/E/PE based systems.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**The pre-conditions are that we are dealing with E/E/PE based system. The standard is applicable to "all industries" and the constraints may be that the standard is too generic. However, it is acknowledged, and other sector specific application standards have adapted IEC 61508.**

6.4.6 Demo 3.1 - IPC 2551

IPC-2551: **International Standard for Digital Twins**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IPC-2551: "International Standard for Digital Twins", (Published January 2020, Release date January 2021).** **ISBN: 978-1-951577-82-7,** **Product ID: 2551-STD-0-D-0-EN-0**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IPC - IPC International Inc.**[12] **(The former names "Institute of Printed Circuits" and "Institute for Interconnecting and Packaging Electronic Circuits" are no longer in use.)**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**IPC is a trade/industry association whose aim is to standardize the assembly and production requirements of electronic equipment and assemblies.** **IPC is a non-profit, member-driven organization and leading source for industry standards, training, industry intelligence and public policy advocacy, IPC is a global association that helps OEMs, EMS, PCB manufacturers and suppliers build electronics better.**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The IPC-2551 standard is part of the IPC Factory of the Future standards establishing the IPC Digital Twin, which is comprised of the Digital Twin Product, Digital Twin Manufacturing and Digital Twin Lifecycle frameworks.**

[12] https://www.ipc.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		The standard stipulates and defines Digital Twin properties, types, complexities and readiness levels. The IPC Digital Twin includes historical information about a product, including the history of design in terms of revision and engineering changes, and manufacturing information, that many refer to as the Digital Thread. **Digital twins are defined at three different levels: Product definition, Manufacturing information and Lifecycle information.**

6.4.7 Demo 3.1 - ANSI/UL 4600

ANSI/UL 4600: **Standard for Evaluation of Autonomous Products**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ANSI/UL 4600: "Standard for Evaluation of Autonomous Products", (Edition 1, ANSI approved, April 2020).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ANSI: American National Standards Institute[13].** **UL: Underwriter Laboratories[14].**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**UL Standards developed this standard in partnership with Edge Case Research, (a recognized leader in development of autonomous systems).**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The ANSI/UL 4600 addresses safety principles and processes for evaluating fully autonomous products requiring no human driver supervision.** **In addition to autonomous vehicles, the standard can be applied to products used in mining, agriculture and maintenance as well as other products including unmanned aerial vehicles (UAVs).**

[13] https://ansi.org/

[14] https://ul.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Technologies/methods/processes covered	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**A standard that covers safety principles and processes for evaluating autonomous products. Main issues:** • **A set of weak prescriptive requirements.** • **OEM/Tier1 involvement is limited at this stage.** • **Areas of overlaps with ISO 26262 and ISO 21448.** • **Difficult and not clear how UL certification will work in the autonomous vehicle area.**

6.4.8 Demo 3.1 - ISO/SAE FDIS 21434

ISO/SAE FDIS 21434: Road vehicles - Cybersecurity engineering	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO/SAE FDIS 21434: "Road vehicles - Cybersecurity engineering", (under development. Stage 50.00, Final text received or FDIS[15] registered for formal approval).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO – International Organization for Standardization[16].** **SAE - SAE International[17].**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/TC 22/SC 32 Electrical and electronic components and general system aspects.**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Specifies requirements for cybersecurity risk management regarding engineering for concept, development, production, operation, maintenance, and decommissioning for road vehicle E/E systems, including their components and interfaces.** **Defines a framework that includes requirements for cybersecurity processes and**

[15] FDIS: Final Draft International Standard.

[16] https://www.iso.org/home.html

[17] https://www.sae.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		a common language for communicating and managing cybersecurity risk. **Does not prescribe specific technology or solutions related to cybersecurity.**
	Technologies/methods/processes covered	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Standard together developed by SAE and ISO:** • **Relevant to Road-vehicles.** • **Purpose of reasonably secure vehicles and systems.** • **Automakers and suppliers can use it to show "due diligence."** • **Focus on automotive cybersecurity engineering.** • **Based on the existing SoA for cybersecurity engineering.** • **Based on a risk-oriented approach** • **Addresses the management activities for cybersecurity.** • **Cybersecurity processes/activities for all phases of the vehicle lifecycle.** **Main issues:** • **Addresses the topics at a high-level.** • **It not considering the interaction with safety.**

6.4.9 Demo 3.1 - SAE J3061

SAE J3061: **Cybersecurity Guidebook for Cyber-Physical Vehicle Systems**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**SAE J3061: "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", (January 2016).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**SAE - SAE International**[18].
Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Guides vehicle cybersecurity and was created based on and expanded on from existing practices implemented or reported in industry, government, and conference papers. Main issues:** • **The standard is a collection of guidance.**

[18] https://www.sae.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		• **The standard is not considering the interaction with safety.**

6.4.10 Demo 3.1 - IEEE P2846

IEEE P2846: **Assumptions for Models in Safety-Related Automated Vehicle Behavior**	ArchitectECA2030
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IEEE P2846: "Assumptions for Models in Safety-Related Automated Vehicle Behavior", (PAR[19] approval September 2020).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IEEE SA - Institute of Electrical and Electronics Engineers Standard Association[20].**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	• **Society: IEEE Vehicular Technology Society.** • **Standard committee: VT/ITS - Intelligent Transportation Systems.** • **Co-standard committee: C/SAB, VT/AVSC.** • **Working Group: AV Decision Making - Formal Model for Safety Considerations in Automated Vehicle Decision Making.** • **Sponsor: IEEE Computer Society Standards Activity Board Standards Committee.**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Formal Model for Safety Considerations in Automated Vehicle Decision Making.** **Scope: This standard defines a formal rules-based mathematical model for automated vehicle decision-making using discrete mathematics and logic. The model applies to the planning and decision-making functions of an SAE Level 3-5 automated vehicle. The model is formally verifiable, technology-neutral, and parameterized to allow regional customization by governments as desired. The standard applies to specified driving scenarios and cases. For example, several scenarios/procedures include highway driving and potentially full urban driving. The standard describes a test methodology and the tools**

[19] PAR: Project Authorization Request

[20] https://standards.ieee.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		necessary to verify an automated vehicle to assess conformance with the standard. The standard is not addressing the host vehicle navigation system implementing the logic or anything relating to perception, object detection, recognition, verification and or classification, free space detection, etc. **Describes the minimum set of reasonable assumptions used in foreseeable scenarios to be considered for road vehicles in the development of safety-related models that are part of automated driving systems (ADS). However, is not necessarily exhaustive to guarantee the safety of the ADS. Includes consideration of rules of the road and their regional and temporal dependencies.**
	Technologies/methods/processes covered	**The standard focus on describing a minimum set of reasonable assumptions used in foreseeable scenarios to be considered for road vehicles in the development of safety-related models that are part of ADS. The standard includes consideration of rules of the road and their regional and temporal dependencies.**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**The algorithms or technologies in an ADS that the assumptions and attributes defined are not part of the scope if this standard.**

6.4.11 Demo 3.1 - IEEE P2851

IEEE P2851: **Exchange/ Interoperability Format for Safety Analysis and Safety Verification of IP, SoC and Mixed Signal ICs**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IEEE P2851: "Exchange/ Interoperability Format for Safety Analysis and Safety Verification of IP, SoC and Mixed Signal ICs", (PAR[21] approval November 2019).**

[21] PAR: Project Authorization Request

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IEEE SA - Institute of Electrical and Electronics Engineers Standard Association[22].**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	• **Society: IEEE Computer Society.** • **Standard committee: C/DA - Design Automation.** • **Working Group: Functional Safety Format - Exchange/Interoperability format for functional safety analysis and safety verification of IP, SoC and mixed signal ICs.** • **Sponsor: IEEE Computer Society Standards Activity Board Standards Committee.**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Defines a data format with which results of functional safety analyses such as Failure Mode and Effects Analysis (FMEA), Failure Modes, Effects and Diagnostic Analysis (FMEDA), Failure Mode, Effects and Criticality analysis (FMECA), and Fault Tree analysis (FTA).** **Related functional safety verification activities such as fault injection executed for Intellectual Properties (IPs), SoCs and mixed signal ICs can be exchanged and made available to system integrators.** **The format will define languages, data fields and parameters in a technology independent way.** **The goal of the standard is to provide a common ground for Electronic Design Automation (EDA), SoC and IP vendors in needs of developing tools for functional safety critical applications.**

6.4.12 Demo 3.1 - IATF 16949:2016 (replace ISO/TS 16949:2009)

IATF 16949: **Technical specification - Quality management systems for automotive production and relevant service parts organisations**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IATF 16949:2016 "Technical specification - Quality management systems for automotive production and relevant service parts organisations", (1st edition, October 2016).**

[22] https://standards.ieee.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	IATF 16949:2016 is aligned with structure and requirements of ISO 9001:2015. **IATF 16949:2016 replace ISO/TS 16949:2009 which is withdrawn.**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IATF - International Automotive Task Force[23].**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**IATF 16949:2016 is coupled with the applicable customer-specific requirements, defines the quality management system (QMS) requirements for automotive production, service, and accessory parts.** **IATF 16949:2016 is an autonomous QMS standard that is fully aligned with the structure and requirements of ISO 9001:2015. However, it is not a stand-alone document, but is implemented as a supplement to, and in conjunction with, ISO 9001:2015.** **Related document is "Automotive certification scheme for IATF 16949 - Rules for achieving IATF recognition" (5th edition November 2016).**

6.4.13 Demo 3.1 - AEC Q100

AEC Q100 **Failure mechanism based stress test qualification for integrated circuits**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**AEC Q100 "Failure mechanism based stress test qualification for integrated circuits", (Rev-H, September 2014).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**AEC - Automotive Electronics Council[24].**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization	**AEC/Component Technical Committee.** **The AEC was originally established by Chrysler, Ford, and GM for the purpose of establishing**

[23] https://www.iatfglobaloversight.org/

[24] http://www.aecouncil.com/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

and/or writers of the (initial) specification/standard proposal, etc.)	**common part-qualification and quality-system standards.** **Today, the committees are composed of representatives from the Sustaining Members, currently: Aptiv, Bose Corporation, Continental Corporation, Cummins, Delphi Technologies, Denso International America, Gentex Corporation, Harman, Hella, John Deere Electronics Solutions (Phoenix International), Kostal Automotive, Lear Corporation, Magna Electronics, Sirius XM, Valeo, Veoneer, Visteon Corporation, and ZF (plus other Technical, Associate, and Guest Members).**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**AEC Q100 covers failure mechanism-based stress tests, minimum stress test driven qualification requirements and test conditions for qualifying Integrated Circuits (ICs).** **The idea is to determine devices which can pass the defined stress tests, and provide devices which can offer certain level of quality and reliability in the application.** **AEC Q100 defines four temperature ranges based on the operating range of ICs.** **Other related documents are:** • **AEC Q101 (Discrete semiconductors such as diodes, transistors, etc.)** • **AEC Q102 (Opto-electronic semiconductors).** • **AEC Q103 (MEMS pressure sensor devices).** • **AEC Q104 (Multichip modules).** • **AEC Q200 (Passive components).**

6.4.14 Demo 3.1 - EN ISO 24534

EN ISO 24534:

Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles

Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**EN ISO 24534: "Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles". 4 Parts published between 2010-2019.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**CEN - European Committee for Normalization[25]. ISO - International Organization for Standardization[26].**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Provides requirements for electronic registration identification (ERI) that are based on an identifier assigned to a vehicle (e.g., for recognition by national authorities), and adheres to privacy and data protection regulations. Part 1 (Architecture) provides an overview of the ERI system concept regarding the onboard vehicle components and the external off-vehicle components required for an operational system. The detailed requirements are defined in Part 2 (operational requirements), Part 3 (intelligent transport systems), and Part 4 (secure communications using asymmetrical techniques).**

6.4.15 Demo 3.1 - IEEE 802.11p

IEEE 802.11p: **IEEE Standard for Information technology -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Wireless Access in Vehicular Environments.**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IEEE 802.11p: IEEE Standard for Information technology -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Wireless Access in Vehicular Environments, (2010).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IEEE SA - Institute of Electrical and Electronics Engineers Standard Association[27].**

[25] https://www.cen.eu/Pages/default.aspx

[26] https://www.iso.org/home.html

[27] https://standards.ieee.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Amendment 6 specifies the extensions to IEEE 802.11 standard for wireless local area networks (WLANs) providing wireless communications while in a vehicular environment.**

6.4.16 Demo 3.1 - IEEE 802.11bd

IEEE 802.11bd:

Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment: Enhancements for Next Generation V2X.

Formalia		
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).		**IEEE 802.11bd: Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment: Enhancements for Next Generation V2X.**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')		**IEEE SA - Institute of Electrical and Electronics Engineers Standard Association[28].**
Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**This amendment provides enhancements for the next generation V2X.**

[28] https://standards.ieee.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6.4.17 Demo 3.1 - IEEE P2020

IEEE P2020: **Standard for Automotive System Image Quality**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IEEE P2020: "Standard for Automotive System Image Quality", (Project 2016).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IEEE SA - Institute of Electrical and Electronics Engineers Standard Association[29].**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Address fundamental attributes that contribute to image/ quality for automotive Advanced Driver Assistance Systems (ADAS) applications and identifying existing metrics and other useful information relating to these attributes. Define a standardized suite of objective and subjective test methods for measuring automotive camera image quality attributes. Specify tools and test methods to facilitate standard-based communication and comparison among Original Equipment Manufacturer (OEM) and Tier 1 system integrators and component vendors.**

6.4.18 Demo 3.1 - SAE J2735

SAE J2735: **V2X Communication Message Set Dictionary**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**SAE J2735: "V2X Communication Message Set Dictionary", (2007).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**SAE - SAE International[30].**

[29] https://standards.ieee.org/

[30] https://www.sae.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Specifies a message set, and its data frames and elements, for use by vehicle-to-everything (V2X) communications system applications. The data dictionary was initially designed for use over DSRC, but this document is intended to be independent of the underlying communications protocols used to exchange data between participants in V2X applications.**

6.4.19 Demo 3.1 - SAE J3016

SAE J3016: **Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**SAE J3016: "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles", (2018).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**SAE - SAE International[31].**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Describes vehicle driving automation systems that perform part or all the dynamic driving tasks on a sustained basis. It provides a taxonomy with detailed definitions for six driving automation levels, ranging from Level 0 (no driving automation) to Level 5 (full driving automation).**

6.4.20 Demo3.1 - Other comments

ISO/SAE FDIS 21434

Potential gaps for an integrated safety-security approach for autonomous vehicles combining ISO 26262, SAE J3061, and ISO 21448.

- Common language/structure used to perform HARA and TARA.

[31] https://www.sae.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

- Define safety and cybersecurity concepts.
- Define safety and cybersecurity requirements.
- Make safety and cybersecurity analyses perform safety and cybersecurity verification.
- Requirements for Interactions between safety and cybersecurity.
- Safety affecting cybersecurity, and vice versa.
- Safety supporting cybersecurity, and vice versa.

6.4.21 Demo 3.2 - IPC 2551

IPC-2551: **International Standard for Digital Twins**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IPC-2551: "International Standard for Digital Twins", (Published January 2020, Release date January 2021).** **ISBN: 978-1-951577-82-7,** **Product ID: 2551-STD-0-D-0-EN-0**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IPC - IPC International Inc.**[32] **(The former names "Institute of Printed Circuits" and "Institute for Interconnecting and Packaging Electronic Circuits" are no longer in use.)**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**IPC is a trade/industry association whose aim is to standardize the assembly and production requirements of electronic equipment and assemblies.** **IPC is a non-profit, member-driven organization and leading source for industry standards, training, industry intelligence and public policy advocacy, IPC is a global association that helps OEMs, EMS, PCB manufacturers and suppliers build electronics better.**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The IPC-2551 standard is part of the IPC Factory of the Future standards establishing the IPC Digital Twin, which is comprised of the Digital Twin Product, Digital Twin Manufacturing and Digital Twin Lifecycle frameworks.** **The standard stipulates and defines Digital Twin properties, types, complexities and**

[32] https://www.ipc.org/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		readiness levels. The IPC Digital Twin includes historical information about a product, including the history of design in terms of revision and engineering changes, and manufacturing information, that many refer to as the Digital Thread. **Digital twins are defined at three different levels: Product definition, Manufacturing information and Lifecycle information.**	
	Technologies/methods/processes covered	**Focus on the following:** • **Hierarchical structure of IPC Digital Twin** • **Definitions of its various aspects** • **Interoperability among various Digital Twin instances of these aspects** • **Structured definition of attributes of each aspect** • **Readiness level and assessment (categorization of application field) of the Digital Twin**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Applicable to all aspects of product lifecycle (from initial concept to final end-of-life) with no restrictions on product classification sector, size of operation, or location.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [ ] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** **Research and development**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance		
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly')	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator: SC3 (Demonstrator SSC3.2 DigiPack)** **Partners: NXP and TUDE** **(Use of standard is tentative)**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [ ] No [**X**] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			[ ] Partly [**X**] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**IPC-2551 only addresses the structure of Digital Twin. ISO-26262 could be utilized for safety level.**
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**Residual risk in the following aspects – hardware, software, data, and connectivity would be considered.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [**X**] No
		If **partly**: What is missing?	**No section on application of Digital Twin (only the structure is described), thus no section related to safety and residual risk.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**ISO-26262 and SOTIF (ISO/PAS-21448) could be utilized for residual risk.**

6.4.22 Demo 3.2 - ISO 26262

ISO 26262 **Road Vehicles – Functional Safety**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO26262:2018 Road Vehicles – Functional Safety. 12 Parts, ISO2626-1:2018 – ISO2626-12:2018. Published 12/2018.**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO – International Organization for Standardization[33].**

[33] https://www.iso.org/home.html

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/TC 22, SC 32 Electrical and electronic components and general system aspects[34,35].**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Assessment and quantification of possible failures according to ISO 26262, (together with IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" and ISO/PAS 21448).** **ISO 26262 address safety-related systems that include one or more electrical/electronic (E/E) systems. The risk classification scheme ASIL (automotive safety integrity level) is a key component of ISO 26262 and defined in part 9. The ASIL scheme is focusing on the harm to the driver and other road users but is not addressing the technologies used in the system. Each safety requirement is assigned an ASIL of A, B, C, or D, where D is the most safety critical processes/ strictest testing regulations.** **Engineering processes and methods (and some organizational issues) to ensure functional safety of E/E systems installed in road vehicles (trucks, cars, etc.), excluding mopeds by prescribing a certain design, implementation, and test (incl. validation and verification) methodology.** **The 12 parts of the standard deal with:** **25) Vocabulary** **26) Management of functional safety** **27) Concept phase** **28) Product development at the system level** **29) Product development at the hardware level** **30) Product development at the software level** **31) Production, operation, service, and decommissioning** **32) Supporting processes** **33) Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis** **34) Guidelines on ISO 26262**

[34] TC: Technical Committee

[35] SC: Sub Committee

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		35) Guidelines on application of ISO 26262 to semiconductors **36) Adaptation of ISO 26262 for motorcycles**	
	Technologies/methods/processes covered	**Focus on hazard and risk analysis, verification, validation, and test.**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**An established family of standards addressing functional safety management, HW random and systematic failures. Main issues:** • **Autonomous vehicle complexity (multiple items combined, thousands of safety requirements) requires a more agile development flow.** • **No autonomous vehicles system architecture references.** • **The PMHF targets do not match with modern technologies/components.** • **ISO 26262-6 is difficult/very challenging if applied to open-source SW.** • **Guidelines are missing on how to apply ISO 26262 to Artificial Intelligence.** **In principle, ISO26262 can (and should) be applied to any development of any E/E system. It ensures that – with a very high probability – the system behaves as specified. However, ISO26262 cannot answer the following questions:** **(5) Is the specification correct (i.e.., is a system that behaves according to this specification indeed functional safe)?** **(6) Is the specification complete (i.e.., are all situations/use-cases that the system might encounter during operation covered)?** **b) … even those where users deliberately misuse the system?**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [**X**] Other (pls. specify): Production, Decommissioning (see Part 7).	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[X] mandatory [ ] optional [ ] not done at all	**Your line of work is…** Research and development

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,		
	Short **description** of this relevance	**The question of whether an implementation fulfills a specification is a very important one also for L3+ cars and thus ISO26262 is an important part of their V&V&T. However, for L3+ cars applying only ISO26262 is not sufficient for showing functional safety.**
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [**X**] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is residual risk/probability of failure handled in this standard? If so, how?	**Each item (i.e., the system, each component, sub-component, software item, …) is assigned a set of 'hazardous events' (i.e., events in which the item will cause damage; example: failing brakes).** **Each 'hazardous event' is classified according to**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		g) S – Severity: The severity of the damage resp. the severity of the injuries caused by the item. **h) E – Exposure: Relative probability that the hazardous event occurs during operation.** **i) C – Controllability: If the hazardous event occurs, how likely is it that the driver can prevent the damage?** **Each is then assigned an 'automotive safety integrity (ASIL) level', ranging from QM (Quality Management, no safety risk) via ASIL A (very low risk) to ASIL D (very high risk), according to these three parameters.** **Much simplified, the ASIL of an item (i.e., the system, component, software…) is then the highest ASIL of the hazardous events identified for it.** **Simplified again, for each ASIL level, ISO 26262 defines the needed methods and processes (including definition of safety goals and safety architectures, types and amount of validation, verification and test, etc.) that need to be performed in order to guarantee that the remaining (residual) risk of an item with this ASIL level is below an acceptable threshold. For ASIL A items, only very few tests need to be done, for ASIL D an extensive safety case has to be devised and implemented. If properly done, at the end of the process each item has a sufficiently low residual risk of not being functional safe.**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator: SC3 (Demonstrator SSC3.2 DigiPack)** **Partners: NXP and TUDE**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [ ] No [**X**] Don't know yet
	If **Yes**:	
		Which Safety-Level is supposed to be achieved?
		Does this **standard actually help** with achieving this level? [ ] Yes

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			[ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**Residual risk in the following aspects – hardware, software, data, and connectivity would be considered.**
		Does the standard help you in considering residual risk/probability of failure?	[**X**] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

6.4.23 Demo 3.2 - ISO/PAS 21448

ISO/PAS 21448 **Road Vehicles – Safety of the intended functionality**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO/PAS 21448:2019 Road Vehicles – Safety of the intended functionality** **(PAS: Publicly Available Specification; Under development is ISO/DIS 21448, to appear, with DIS: Draft International Standard)** **Published 11/2019.**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO – International Organization for Standardization[36].**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization	**ISO/TC (Technical Committee) 22/SC (Subcommittee) 32**

[36] https://www.iso.org/home.html

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

and/or writers of the (initial) specification/standard proposal, etc.)		**Electrical and electronic components and general system aspects**
Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Requirements and specifications for defining the methodology for identifying residual risks for connectivity systems for automated and connected vehicles in link with the ISO/PAS 21448 framework. Propose a methodology for risk estimations of connectivity systems considering the planned system integrity and dependability measures based on the framework. Assessment and quantification of possible failures according to ISO/PAS 21448, (together with ISO 26262 and IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems").** **ISO/PAS 21448 provides guidance on the applicable design, verification and validation measures needed to achieve the safety of the intended functionality (SOTIF). Examines whether a needed safety functionality is successfully delivered in the absence of a failure, such as performance limitations (e.g., systems, subsystems, sensors, unexpected road environment changes).** **The absence of unreasonable risks due to hazards resulting from functional insufficiencies of the intended functionality [of the E/E system/product] or by reasonably foreseeable misuse is referred to as Safety of the Intended Functionality (SOTIF). ISO 21448 provides guidance on the applicable design, verification and validation measures needed to achieve the SOTIF.**
	Technologies/methods/processes covered	**Focus on design processes, verification, and validation methods**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**New standard targeting:** • **The inadequacy/inefficiency of the function to correctly comprehend the situation and operate safely.** • **Insufficient robustness of the procedure/function concerning sensor input variations or diverse environmental conditions.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		Main issues: • **The standard is at a high level to produce consistent/interoperable industry practices.** • **Not clear enough which are the different requirements between autonomous vehicle levels (L3/L4/L5).** • **Several annexes (e.g., machine learning) needs extra work.** **ISO 21448 is applied when ISO 26262 alone is not sufficient anymore (e.g., because the system behavior cannot fully be specified due to its complexity and/or its openness). Thus, ISO 21448 is aiming at (design and V&V of) L3+ cars.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [ ] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** Research and development
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**ISO 21448 provides a way to cope with (a) incomplete and (b) erroneous specifications. Whereas ISO 26262 solves the problem of whether the systems functions are correct according to the specification, ISO 21448 also asks whether the functions are sufficient to guarantee safety in any scenario of any use-case for which the system was build. Thus, it is highly relevant for L3+ cars.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly')	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro-magnetic interference), ageing, accidental mechanical stress, etc. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).

	Is **residual risk/probability of failure** handled in this standard? If so, how?	**ISO 21448 considers four types of scenarios to handle:**
		
		5. **Known scenarios (i.e., scenarios of which the engineers know that they can occur within an intended Use-Case of the system/product) in which the system is known to behave safe.**
		  ○ **Need not be handled.**
		6. **Known scenarios in which the system is not known to behave safe.**
		  ○ **These are handled via methods from e.g., ISO 26262 (slightly extended to include intended functionality and foreseeable misuse) to achieve safe behavior and a sufficient low residual risk.**
		  ○ **Scenarios in this class thus 'move into class 1' above, leaving this class (ideally) empty (or at least with only a**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		few, highly improbable scenarios). ○ This class also (typically) includes. ▪ Sensor faults or other causes of misperception of the environment ▪ Foreseeable misuse 7. Unknown scenarios (i.e., scenarios that were unknown to engineers at design time) for which the system is not known to behave safe. ○ This case is typically handled by either or both of ▪ Employment of methods similar to fail-aware and fail-operational concepts ('Recognizing that the system is in an unknown scenario (fail-aware) leads to safe (probably degraded) behavior (fail-operational) ▪ Restriction of the Use-Cases ○ With this argument, also Class 3 scenarios are 'moved to' classes 2 and 1. 8. The fourth case, unknown scenarios with known safe behavior is not considered. **A safety case with ISO 21448 typically includes am argument that the residual risk of a system is acceptable because it has been proven to have this residual risk in Class 1 above (using ISO 26262 methods) and Class 2 and Class 2 are small enough so that there is no relevant residual risk there, either.**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator: SC3 (Demonstrator SSC3.2 DigiPack)** **Partners: NXP and TUDE** **(Use of standard is tentative)**
If the Standard is used for a Use-Case/Demonstrator:		

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [ ] No [**X**] Don't know yet
	If **Yes**:		
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**Residual risk in the following aspects – hardware, software, data, and connectivity would be considered.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No
		If **partly**: What is missing?	**We intend to use machine learning in the demonstrator and the corresponding annex in ISO/PAS 21448 is awaiting an update.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**We are not aware of any.**

6.4.24 Demo 3.2 - AEC Q100

AEC Q100

Failure mechanism based stress test qualification for integrated circuits

Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication**	**AEC Q100 "Failure mechanism based stress test qualification for integrated circuits", (Rev-H, September 2014).**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

date of the standard (if these can not be derived from the name already).	
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**AEC - Automotive Electronics Council[37].**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**AEC/Component Technical Committee.** **The AEC was originally established by Chrysler, Ford, and GM for the purpose of establishing common part-qualification and quality-system standards.** **Today, the committees are composed of representatives from the Sustaining Members, currently: Aptiv, Bose Corporation, Continental Corporation, Cummins, Delphi Technologies, Denso International America, Gentex Corporation, Harman, Hella, John Deere Electronics Solutions (Phoenix International), Kostal Automotive, Lear Corporation, Magna Electronics, Sirius XM, Valeo, Veoneer, Visteon Corporation, and ZF (plus other Technical, Associate, and Guest Members).**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**AEC Q100 covers failure mechanism-based stress tests, minimum stress test driven qualification requirements and test conditions for qualifying Integrated Circuits (ICs).** **The idea is to determine devices which can pass the defined stress tests, and provide devices which can offer certain level of quality and reliability in the application.** **AEC Q100 defines four temperature ranges based on the operating range of ICs.** **Other related documents are:** • **AEC Q101 (Discrete semiconductors such as diodes, transistors, etc.)** • **AEC Q102 (Opto-electronic semiconductors).** • **AEC Q103 (MEMS pressure sensor devices).** • **AEC Q104 (Multichip modules).** • **AEC Q200 (Passive components).**
Technologies/methods/processes covered	**A set of failure mechanism based stress tests capable of stimulating and precipitating**

[37] http://www.aecouncil.com/

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		semiconductor device and package failures. They are categorized into following 6 test groups: • **Accelerated environment stress tests** • **Accelerated lifetime simulation tests** • **Package assembly integrity tests** • **Die fabrication reliability tests** • **Electrical verification tests** • **Defect screening tests** • **Cavity package integrity tests** **It also includes definitions of the minimum stress test driven qualification requirements and references test conditions for qualification of integrated circuits (ICs). The objective is to precipitate failures in an accelerated manner compared to use conditions.**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**The document states that each qualification project should be examined for the following:** • **Any potential new and unique failure mechanisms** • **Any situation where these tests/conditions may induce failures that would not be seen in the application** • **Any extreme use condition and/or application that could adversely reduce the acceleration.** **Additionally, use of this standard does not relieve the IC supplier of their responsibility to meet their own company's internal qualification program.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [ ] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[**X**] mandatory [ ] optional [ ] not done at all	**Your line of work is…** Research and development
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance		

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [**X**] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**Residual risk is not handled by this standard. Probability of failure is handled by the acceptance criteria of standard accelerated stress tests.**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator: SC3 (Demonstrator SSC3.2 DigiPack)** **Partners: NXP and TUDE** **(Use of standard is tentative)**
If the Standard is used for a Use-Case/Demonstrator:		

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [ ] No [**X**] Don't know yet
	If **Yes**:		
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**Residual risk in the following aspects – hardware, software, data, and connectivity would be considered.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No
		If **partly**: What is missing?	**Residual risk is not mentioned in this standard.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**ISO-26262 and SOTIF (ISO/PAS-21448) could be utilized for residual risk.**

6.4.25 Demo 3.2 - ISO/TR 18161

ISO/TR 18161 **Automation systems and integration – Applications integration approach using information exchange requirements modelling and software capability profiling**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication**	**ISO/TR 18161: "Automation systems and integration – Applications integration approach using information exchange**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

date of the standard (if these can not be derived from the name already).		**requirements modelling and software capability profiling", (Published July 2013).**	
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')		**ISO – International Organization for Standardization.**	
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)		**ISO/TC 184/SC 5 Interoperability, integration, and architectures for enterprise systems and automation applications.**	
Content / Coverage			
Scope of the Standard			
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**This standard describes an approach for using ISO 16100 and ISO 18435 to specify information exchange requirements between applications. This approach is based on the use of ISO 18435 application interaction matrix element (AIME)/application domain matrix element (ADME) templates in conjunction with ISO 16100 manufacturing software unit (MSU) capability profiles.**	
	Technologies/methods/processes covered	**This standard describes method for data exchange among physical product equipped with sensors, control and acquisition software, and diagnostics software. It includes an example of this approach as applied to describing the interoperability requirements of an integrated smart pump application.**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**No specific constraint has been mentioned for the applicability of this standard. At the same time, it bridges the ISO 18435 and ISO 16100 standards, so it follows the constraints therein.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[ ] Requirements [**X**] Development and Implementation [ ] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [**X**] not done at all	**Your line of work is…** **Research & development**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Short **description** of this relevance	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator: SC3 (Demonstrator SSC3.2 DigiPack)** **Partners: NXP and TUDE**
If the Standard is used for a Use-Case/Demonstrator:		

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [ ] No [**X**] Don't know yet
	If **Yes**:		
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**Residual risk in the following aspects – hardware, software, data, and connectivity would be considered.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [**X**] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**ISO-26262 and SOTIF (ISO/PAS-21448) could be utilized for residual risk.**

6.4.26 Demo 3.3 - ISO 26262

ISO 26262 **Road Vehicles – Functional Safety**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO26262:2018 Road Vehicles – Functional Safety** **(12 Parts, ISO2626-1:2018 – ISO2626-12:2018)** **Published 12/2018 (previous version '…:2011')**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')		**ISO – International Organization for Standardization**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)		**ISO/TC (Technical Committee) 22/SC (Subcommittee) 32** **Electrical and electronic components and general system aspects**
Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Engineering processes and methods (and some organizational issues) to ensure functional safety of E/E systems installed in road vehicles (trucks, cars, etc.), excluding mopeds by prescribing a certain design, implementation, and test (incl. validation and verification) methodology.** **The 12 parts of the standard deal with:** **37) Vocabulary** **38) Management of functional safety** **39) Concept phase** **40) Product development at the system level** **41) Product development at the hardware level** **42) Product development at the software level** **43) Production, operation, service, and decommissioning** **44) Supporting processes** **45) Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis** **46) Guidelines on ISO 26262** **47) Guidelines on application of ISO 26262 to semiconductors** **48) Adaptation of ISO 26262 for motorcycles**
	Technologies/methods/processes covered	**Focus on hazard and risk analysis, verification, validation, and test.**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**In principle, ISO26262 can (and should) be applied to any development of any E/E system. It ensures that – with a very high probability – the system behaves as specified. However, ISO26262 cannot answer the following questions:** **(7) Is the specification correct (i.e.., is a system that behaves according to this specification indeed functional safe)?**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		(8) Is the specification complete (i.e.., are all situations/use-cases that the system might encounter during operation covered)? **c) … even those where users deliberately misuse the system?**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [?] Homologation [**X**] Operation in the field [**X**] Other (pls. specify): Production, Decommissioning (see Part 7).	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**The question of whether an implementation fulfills a specification is a very important one also for L3+ cars and thus ISO26262 is an important part of their V&V&T. However, for L3+ cars applying only ISO26262 is not sufficient for showing functional safety.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[X] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [X] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [X] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**Each item (i.e., the system, each component, sub-component, software item, …) is assigned a set of 'hazardous events' (i.e., events in which the item will cause damage; example: failing brakes).** **Each 'hazardous event' is classified according to** **j) S – Severity: The severity of the damage resp. the severity of the injuries caused by the item.** **k) E – Exposure: Relative probability that the hazardous event occurs during operation.** **l) C – Controllability: If the hazardous event occurs, how likely is it that the driver can prevent the damage?** **Each is then assigned an 'automotive safety integrity (ASIL) level', ranging from QM (Quality Management, no safety risk) via ASIL A (very low risk) to ASIL D (very high risk), according to these three parameters.** **Much simplified, the ASIL of an item (i.e., the system, component, software…) is then the highest ASIL of the hazardous events identified for it.** **Simplified again, for each ASIL level, ISO 26262 defines the needed methods and processes (including definition of safety goals and safety architectures, types and amount of validation, verification and test, etc.) that need to be performed in order to guarantee that the**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		remaining (residual) risk of an item with this ASIL level is below an acceptable threshold. For ASIL A items, only very few tests need to be done, for ASIL D an extensive safety case has to be devised and implemented. If properly done, at the end of the process each item has a sufficiently low residual risk of not being functional safe.

6.4.27 Demo 3.3 - ISO/PAS 21448

ISO/PAS 21448 **Road Vehicles – Safety of the intended functionality**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO/PAS 21448:2019 Road Vehicles – Safety of the intended functionality** **(PAS: Publicly Available Specification; Under development is ISO/DIS 21448, to appear, with DIS: Draft International Standard)** **Published 11/2019.**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO – International Organization for Standardization.**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/TC (Technical Committee) 22/SC (Subcommittee) 32** **Electrical and electronic components and general system aspects**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The absence of unreasonable risks due to hazards resulting from functional insufficiencies of the intended functionality [of the E/E system/product] or by reasonably foreseeable misuse is referred to as Safety of the Intended Functionality (SOTIF). ISO 21448 provides guidance on the applicable design, verification and validation measures needed to achieve the SOTIF.**
Technologies/methods/processes covered	**Focus on design processes, verification and validation methods**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**ISO 21448 is applied when ISO 26262 alone is not sufficient anymore (e.g., because the system behavior cannot fully be specified due to its complexity and/or its openness). Thus, ISO 21448 is aiming at (design and V&V of) L3+ cars.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [ ] Development and Implementation [**X**] Verification, Validation, Test [Not yet, but high potential] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**ISO 21448 provides a way to cope with (a) incomplete and (b) erroneous specifications. Whereas ISO 26262 solves the problem of whether the systems functions are correct according to the specification, ISO 21448 also asks whether the functions are sufficient to guarantee safety in any scenario of any use-case for which the system was build. Thus, it is highly relevant for L3+ cars.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro-magnetic interference), ageing, accidental mechanical stress, etc. These faults are typically not prevented, but	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [X] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**ISO 21448 considers four types of scenarios to handle:** **9. Known scenarios (i.e., scenarios of which the engineers know that they can occur within an intended Use-Case of the system/product) in which the system is known to behave safe.** **○ Need not be handled.** **10. Known scenarios in which the system is not known to behave safe.** **○ These are handled via methods from e.g., ISO 26262 (slightly extended to include intended functionality and foreseeable misuse) to achieve safe behavior and a sufficient low residual risk.** **○ Scenarios in this class thus 'move into class 1' above, leaving this class (ideally) empty (or at least with only a few, highly improbable scenarios).** **○ This class also (typically) includes.** **▪ Sensor faults or other causes of misperception of the environment** **▪ Foreseeable misuse** **11. Unknown scenarios (i.e., scenarios that were unknown to engineers at**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		design time) for which the system is not known to behave safe. **○ This case is typically handled by either or both of** **▪ Employment of methods similar to fail-aware and fail-operational concepts ('Recognizing that the system is in an unknown scenario (fail-aware) leads to safe (probably degraded) behavior (fail-operational)** **▪ Restriction of the Use-Cases** **○ With this argument, also Class 3 scenarios are 'moved to' classes 2 and 1.** **12. The fourth case, unknown scenarios with known safe behavior is not considered.** **A safety case with ISO 21448 typically includes am argument that the residual risk of a system is acceptable because it has been proven to have this residual risk in Class 1 above (using ISO 26262 methods) and Class 2 and Class 2 are small enough so that there is no relevant residual risk there, either.**

6.4.28 Demo 3.3 - IPC 2551

IPC-2551: **International Standard for Digital Twins**	

6.4.29 Demo 3.3 - ISO 4804

ISO/TR 4804 **Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation**	

Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can	**ISO/TR 4804:2020 Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

not be derived from the name already).	**(TR: Technical Report)** **Published 12/2020** **This standard is based upon a whitepaper titled "Safety first for Automated Driving" published by various OEMs, Tier Suppliers and Technology Providers (see below); the whitepaper is available – amongst others – at** **https://www.daimler.com/innovation/case/autonomous/safety-first-for-automated-driving.html . All information in this survey is taken from the whitepaper, not from the actual standard document. However, according to the table of contents of the standard from the ISO website, ~90% of the chapter names in the whitepaper and the standard are the same (and therefore presumably the content is quite similar, too).**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO – International Organization for Standardization**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ISO/TC (Technical Committee) 22** **Road Vehicles (no subcommittee assigned yet)** **Publishers/Authors of the whitepaper (see above):** **APTIV (was: Delphi Automotive), Audi, Baidu Apollo, BMW, Continental, Daimler, FCA (Fiat Crysler Automobiles), HERE (was: Smart2Go, Map24, Navteq, Ovi Maps and Nokia Maps), Infineon, Intel, VW**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Processes and methods – often based upon a combination of existing methods and standards, i.e., ISO26262, ISO21448 SOTIF and similar – for a comprehensive approach to safety and security for L3 and L4 automated cars.**
Technologies/methods/processes covered	**The followed approach is to break down safety principles into safety by design capabilities, elements and architectures, each of which should be validated by existing approaches (i.e., by methods from ISO 26262, ISO21448, and others) and which together are meant to guarantee safety (and security). The standard defines:** - **12 (safety and security) principles of automated driving.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		- **7 fail-safe and 6 fail-degraded capabilities that the ECA must implement (capabilities are mapped to the 12 principles.** - **5 challenges for V&V and Test; each challenge defines what must be shown by which means/methods during V&V&Test (in addition to what must be shown by application of the existing standards anyway) in order for the 12 principles to hold (and thus for the system to be safe and secure).**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Aims at SAE Level 3 and Level 4 cars.**
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [?] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all **Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,		
	Short **description** of this relevance	**The approach outlined in this standard (see above under 'technologies covered') will be highly relevant for V&V&Test of L3 and L4 ECAs; it has the potential to become THE one standard that is needed for showing safety and security for L3 and L4 cars (with the disclaimer that it references and builds upon other, existing standards, and thus the referenced standards will be needed, too).**
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [**X**] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**.

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[X] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [X] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [X] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**Not directly, but indirectly by relying upon other existing standards.**

6.4.30 Demo 3.3 - SAE J2954

SAE J2954 **Surface Vehicle – Wireless Power Transfer for Light-Duty Plug-in/Electric Vehicles and Alignment Methodology**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**SAE J2954:2020 Surface Vehicle – Wireless Power Transfer for Light-Duty Plug-in/Electric Vehicles and Alignment Methodology** **(Standard / Published: 2020-10-20 / Previous Versions: 2019-04-23, 2017-11-27, 2016-05-26)**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**SAE International**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**Motor Vehicle Council / Hybrid - EV Committee**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology,	**The SAE J2954 standard establishes an industry-wide specification that defines**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	(engineering) processes and/or organization):	**acceptable criteria for interoperability, electromagnetic compatibility, EMF, minimum performance, safety, and testing for wireless power transfer (WPT) of light-duty plug-in electric vehicles.** **SAE J2954 addresses unidirectional charging, from grid to vehicle. This standard is intended to be used in stationary applications (charging while vehicle is not in motion). In this version, only above-ground (surface mounted) installations are covered.** **SAE J2954 contains requirements for safety, performance, and interoperability. It also contains recommended methods for evaluating electromagnetic emissions.**	
	Technologies/methods/processes covered	**Focus on safety, EMF, performance and interoperability.**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**Applicable for vehicles with a coil ground clearance less than 250 mm and for a maximum grid input power of 11.1 kVA.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [ ] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**Wireless charging is a way to transfer energy to an electric vehicle automatically. The charging system is typically formed by two components – one as part of the vehicle and one external component – provided by independent parties. This will lead to many combinations that were never used together in the field before. All components have to comply with a minimum set of functionalities that makes it possible to check interoperability and safety at runtime.**	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**SC1 / Foreign object detection system within a wireless charging system** **Partners: TU Dresden (TUDR)**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6.4.31 Demo 3.3 - ANSI/UL 4600

ANSI/UL 4600: **Standard for Evaluation of Autonomous Products**	

6.4.32 Demo 3.3 - ISO/SAE DIS 21434

ISO/SAE DIS 21434: **Road vehicles - Cybersecurity engineering**	

6.4.33 Demo 3.3 - IEEE P2846

IEEE P2846: **Assumptions for Models in Safety-Related Automated Vehicle Behavior**	

6.4.34 Demo 3.3 - IEEE P2851

IEEE P2851: **Exchange/ Interoperability Format for Safety Analysis and Safety Verification of IP, SoC and Mixed Signal ICs**	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6.5 MONITORING: SC4 Failure modes, fault detection and residual risk for safety security privacy on overall system "monitoring device" architecture

6.5.1 SAE JA6268TM

SAE JA6268TM **Design & Run-Time Information Exchange for Health-Ready Components, April 2018**			
Formalia			
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).		**SAE JA6268™ Design & Run-Time Information Exchange for Health-Ready Components, April 2018**	
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')		**SAE**	
Content / Coverage			
Scope of the Standard			
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Requirements for health-ready components, monitoring functionalities, prerequisites for PHM (prognostics and health management) system.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [ ] Development and Implementation [ ] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance		
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly')	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			[**X**] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [**X**] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
ArchitectECA2030			
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?			**WP/SC/Demonstrator: SC4** **Partners: IFAT**
If the Standard is used for a Use-Case/Demonstrator:			
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes**:		
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	Failure turns into a maintenance action.
		Does the standard help you in considering residual risk/probability of failure?	[**X**] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

6.5.1 SAE J3016

SAE J3016 **Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**SAE J3016 – Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles** **Version: June 2018**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**SAE International**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**This SAE Recommended Practice describes *motor vehicle driving automation systems* that perform part or all of the *dynamic driving task* (*DDT*) on a *sustained* basis. It provides a taxonomy with detailed definitions for six levels of *driving automation,* ranging from *no driving automation* (level 0) to *full driving automation* (level 5), in the context of *motor***

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		vehicles **(hereafter also referred to as "*vehicle*" or "*vehicles*") and their *operation* on roadways. These level definitions, along with additional supporting terms and definitions provided herein, can be used to describe the full range of *driving automation features* equipped on *motor vehicles* in a functionally consistent and coherent manner. "On-road" refers to publicly accessible roadways (including parking areas and private campuses that permit public access) that collectively serve *users* of *vehicles* of all classes and *driving automation* levels (including no *driving automation*), as well as motorcyclists, pedal cyclists, and pedestrians**.	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [ ] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** Research
ArchitectECA2030			
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		WP/SC/Demonstrator: **SC4:** *Monitoring Fail Operationality and Robustness of ADAS/AD Functions* Partners: VIF, DATA	
If the Standard is used for a Use-Case/Demonstrator:			
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [**X**] No [ ] Don't know yet	
	If **Yes**:		
	Which Safety-Level is supposed to be achieved?		
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	It has not been defined yet.
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [**X**] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

6.5.2 J3018

J3018 **Guidelines for Safe On-Road Testing of SAE Level 3, 4 and 5 Prototype Automated Driving Systems (ADS)**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these cannot be derived from the name already).	**J3018 - Guidelines for Safe On-Road Testing of SAE Level 3, 4 and 5 Prototype Automated Driving Systems (ADS)** **Version: March 2015**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**SAE International**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**This document provides guidelines for the safe conduct of on-road tests of vehicles equipped with prototype conditional, high, and full (levels 3-5) *automated driving systems* (*ADSs*), as defined by SAE J3016. It does not include guidance for testing production *ADSs* intended for sale to the general public. The scope is**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		further limited to testing of automated prototype vehicles on public roads. **These guidelines do not address:** **• Testing of driver assist (Level 1) or partial (Level 2) automation systems, which rely on a *human driver* to *monitor* the environment. (See SAE J3016 for Definitions of Levels of Automated Systems.)** **• Closed-course testing.** **• Component-level testing.** **The precise regime of road testing for a particular prototype will depend on the intended level of automation and the targeted capabilities of the prototype (see SAE J3016 for more information).** **A prototype suitable for testing on public roadways is presumed to have already passed laboratory and/or closed-course testing, which are not addressed by this document.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[ ] Requirements [ ] Development and Implementation [x] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** Research
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance		
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad'	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator:** **SC4:** ***Monitoring Fail Operationality and Robustness of ADAS/AD Functions*** **Partners: VIF, DATA**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
	If **partly**: What is missing?	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	This has not been defined yet.
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [**X**] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Safety guidelines for the on-road testing of vehicles equipped with prototype ADSs do not currently exist. The information given in this report will assist interested parties in the creation of guidelines for the on-road testing of such prototypes.**

6.5.3 UNECE Regulation 157 (ALKS) --> link

UNECE Regulation 157 **Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**UNECE Regulation 157** **Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems** **6 April 2020**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**United Nations (UN) / Economic and Social Council / Economic Commission for Europe (ECE)**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**ECE / Inland Transport Committee / World Forum for Harmonization of Vehicle Regulations / Working Party on Automated/autonomous and Connected Vehicles**
Content / Coverage	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The intention of the Regulation is to establish uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems (ALKS). It contains administrative provisions suitable for type approval, technical requirements, audit and reporting provisions and testing provisions.**
	Technologies/methods/processes covered	**This Regulation includes general requirements regarding the system safety and the failsafe response. When the ALKS is activated, it shall perform the driving task instead of the driver, i.e. manage all situations including failures, and shall not endanger the safety of the vehicle occupants or any other road users. There is however always the possibility for the driver to override the system, at any time.** **The Regulation also lays down requirements on how the driving task shall be safely handed over from the ALKS to the driver including the capability for the system to come to a stop in case the driver does not reply appropriately.** **Finally, the Regulation includes requirements on the Human-Machine Interface (HMI) to prevent misunderstanding or misuse by the driver. The Regulation for instance requires that on-board displays used by the driver for other activities than driving when the ALKS is activated, shall be automatically suspended as soon as the system issues a transition demand. These measures are without prejudice to driver behavior rules on how to use these systems in the Contracting Parties as currently being discussed by the Global Forum for Road Traffic Safety (WP.1) at the time of drafting this document.**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**This Regulation applies to the type approval of vehicles of Category M11 with regards to their Automated Lane Keeping System.** **ALKS can be activated under certain conditions on roads where pedestrians and cyclists are prohibited and which, by design, are equipped with a physical separation that divides the traffic moving in opposite directions and prevent traffic from cutting across the path of the vehicle. In a first step, the original text of this Regulation limits the operational speed to**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		60 km/h maximum and passenger cars (M1 vehicles).	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [**X**] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** **Research**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance		
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [**X**] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [**X**] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP2/SC1/SC4 Automated Vehicle Demonstrator (VIF)** Partners: **VIF, DATA, IFAT**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
	If **partly**: What is missing?	**Standard compliance of ALKS for the demonstration purposes is not required.**
	If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There are also relevant standards ISO17361:2007, ISO17387:2008, ISO11270:2014 on this topic. However, standard compliance of ALKS function utilized for the use-case is not required for the demonstration purposes.**
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?	[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**	
	Shortly **describe** how residual risk/probability of failure will be considered:	**In the corresponding VIF demonstrators, the propagation and evaluation of different systemic and synthetically generated faults during the functioning of the ALKS operation will be emulated.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No
		If **partly**: What is missing?	**The information on quantifying how the residual risk accumulates is not described.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There are also relevant standards ISO17361:2007, ISO17387:2008, ISO11270:2014 on this topic. However, standard compliance of ALKS function utilized for the use-case is not required for the demonstration purposes.**

6.5.4 IEEE P2846

IEEE P2846 **Assumptions for Models in Safety-Related Automated Vehicle Behavior**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**IEEE P2846 - Assumptions for Models in Safety-Related Automated Vehicle Behavior; Version: ongoing**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**IEEE**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	IEEE SA WG: VT/ITS/AV Decision Making
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The standard identifies reasonable assumptions for automated driving system about the rules of the road and their regional dependencies. The standard is not exhaustive to guarantee the safety of automated driving systems. Furthermore, the standard defines a method to verify if a automated driving system conforms to these assumptions.**
Technologies/methods/processes covered	**Reasoning of automated driving systems**
Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE	**Only for automated driving systems**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')		
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all	**Your line of work is…** **CPS V&V**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**The standard specifies a method to test automated driving systems' conformance to a set of assumptions about the rules of the road.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[**X**] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [**X**] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time)	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP/SC/Demonstrator: Maybe in the SC4 Demonstrator "Virtual Validation and Verification Framework"** Partners:
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
	If **partly**: What is missing?	
	If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?	[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**	
	Shortly **describe** how residual risk/probability of failure will be considered:	**The Demonstrator will be concerned with V&V of MonDevs and ADAS functions. In the V&V process also metrics for residual risk and predictive maintenance will be considered.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [**X**] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

6.5.5 ISO 17361:2007(E)

ISO 17361:2007(E) **Lane departure warning systems —** **Performance requirements and test procedures**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO17361:2007(E)** **Intelligent transport systems — Lane departure warning systems — Performance requirements and test Procedures** **01-02-2007**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ISO (the International Organization for Standardization)**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)	**Technical Committee ISO/TC 204, Intelligent transport systems**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**Lane departure warning systems (LDWS) are based on fundamental traffic rules. The main focus of an** **LDWS is to help the driver keep the vehicle in the lane on highways and highway-like roads. Accordingly, a warning is issued to alert the driver in case of lane departure caused by, for example, inattention. This standard provides references to technological and engineering requirements as well as test procedures of such systems.**
Technologies/methods/processes covered	**This International Standard specifies the definition of the system, classification,**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		functions, human–machine interface (HMI) and test methods for lane departure warning systems.	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**These are in-vehicle systems that can** **Warn the driver of a lane departure on highways and highway-like roads. The subject system, which may utilize optical, electromagnetic, GPS or other sensor technologies, issues a warning consistent with the visible lane markings. The issuance of warnings at roadway sections having temporary or irregular lane markings (such as roadwork zones) is not within the scope of this International Standard. This International Standard** **Applies to passenger cars, commercial vehicles and buses. The system will not take any automatic action to prevent possible lane departures. Responsibility for the safe operation of the vehicle remains with the driver. LDWS are not intended to issue warnings with respect to collisions with other vehicles or to control vehicle motions.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [**X**] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [X] optional [ ] not done at all	**Your line of work is…** **Research**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance		
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[X] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly')	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [X] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP2/SC1/SC4 Automated Vehicle Demonstrator (VIF)** Partners: **VIF, DATA, IFAT**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [X] No [ ] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			[ ] No
		If **partly**: What is missing?	**Standard compliance of LDWS for the demonstration purposes is not required.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There are also relevant standards and regulations (UNECE Regulations 157), ISO17387:2008, ISO11270:2014 on this topic. However, standard compliance of LDWS function utilized for the use-case is not required for the demonstration purposes.**
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**In the corresponding VIF demonstrators, the propagation and evaluation of different systemic and synthetically generated faults during the functioning of the ALKS operation will be emulated.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No
		If **partly**: What is missing?	**The information on quantifying how the residual risk accumulates is not described.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There are also relevant standards and regulations (UNECE Regulations 157), ISO17387:2008, ISO11270:2014 on this topic. However, standard compliance of LDWS function utilized for the use-case is not required for the demonstration purposes.**

6.5.6 ISO 11270:2014(E)

ISO 11270:2014(E) **Lane keeping assistance systems (LKAS) —** **Performance requirements and test procedures**	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ISO 11270:2014(E)** **Intelligent transport systems — Lane keeping assistance systems (LKAS) —Performance requirements and test procedures** **15-05-2014**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')		**ISO (the International Organization for Standardization)**
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)		**Technical Committee ISO/TC 204, Intelligent transport systems**
Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The main system function of a Lane Keeping Assistance System (LKAS) is to support the driver in** **Keeping the vehicle within the current lane. LKAS acquires information on the position of the vehicle** **Within the lane and, when required, sends commands to actuators to influence the lateral movement of the vehicle. LKAS provides status information to the driver. This standard provides references to technological and engineering requirements as well as test procedures of such systems.**
	Technologies/methods/processes covered	**This International Standard contains the basic control strategy, minimum functionality requirements, basic driver interface elements, minimum requirements for diagnostics and reaction to failure, and performance test procedures for Lane Keeping Assistance Systems.**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**LKAS provide support for safe lane keeping operations by drivers and do not perform automatic driving nor prevent possible lane departures. The responsibility for the safe operation of the vehicle always remains with the driver. LKAS is intended to operate on highways and equivalent roads. LKAS consist of means for recognizing the location of the vehicle inside its lane and means for influencing lateral vehicle movement. LKAS should react consistently with the driver expectations with respect to the visible lane markings. The support at roadway sections having temporary or irregular lane markings (such as roadwork zones) is not within the scope of this International Standard. This**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		International Standard is applicable to passenger cars, **Commercial vehicles, and buses.** **Issues such as specific requirements for the detection sensor function and its performance, or the communication links for co-operative solutions, is not part of this standard.**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[**X**] Requirements [**X**] Development and Implementation [**X**] Verification, Validation, Test [**X**] Homologation [**X**] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [X] optional [ ] not done at all	**Your line of work is…** **Research**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance		
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[X] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar)	

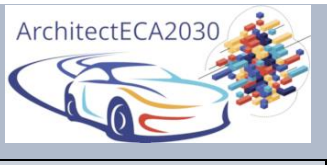
This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		[X] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	**No**
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?		**WP2/SC1/SC4 Automated Vehicle Demonstrator (VIF)** Partners: **VIF, DATA, IFAT**
If the Standard is used for a Use-Case/Demonstrator:		
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?	[ ] Yes [X] No [ ] Don't know yet
	If **Yes**:	
	Which Safety-Level is supposed to be achieved?	
	Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
	If **partly**: What is missing?	**Standard compliance of LKAS for the demonstration purposes is not required.**
	If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There are also relevant standards and regulations (UNECE Regulations 157), ISO17361:2007, ISO17387:2008 on this topic. However, standard compliance of LKAS function utilized for the use-case is not required for the demonstration purposes.**
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?	[X] Yes [ ] No

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			[ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**In the corresponding VIF demonstrators, the propagation and evaluation of different systemic and synthetically generated faults during the functioning of the ALKS operation will be emulated.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [**X**] Partly [ ] No
		If **partly**: What is missing?	**The information on quantifying how the residual risk accumulates is not described.**
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	**Yes. There are also relevant standards and regulations (UNECE Regulations 157), ISO17361:2007, ISO17387:2008 on this topic. However, standard compliance of LKAS function utilized for the use-case is not required for the demonstration purposes.**

6.5.7 ASAM OpenDRIVE

ASAM OpenDRIVE	
Formalia	
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).	**ASAM OpenDRIVE (Open Dynamic Road Information for Vehicle Environment); Version: 1.6.0; Release Date: 12 Mar 2020**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')	**ASAM**
Content / Coverage	
Scope of the Standard	
Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The standard defines a formal XML schema used to define road networks and static objects. In addition, the objects can have different properties, for example, lane width. The XML file can be used to reproducible generate 3D road network for a simulation.**
Technologies/methods/processes covered	**Mostly used for simulation.**
Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE	**None**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')		
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[ ] Requirements [ ] Development and Implementation [**X**] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** **CPS V&V**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**Having a standardized format to represent road networks is necessary for testing, validating and certifying ADAS functions. However, the standard does not directly relate to V&V, test or homologation.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?		No
ArchitectECA2030			
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?			WP/SC/Demonstrator: SC4 Demonstrator "Virtual Validation and Verification Framework" Partners: AVL, SBA
If the Standard is used for a Use-Case/Demonstrator:			
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes**:		
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**The Demonstrator will be concerned with V&V of MonDevs and ADAS functions. In the V&V process also metrics for residual risk and predictive maintenance will be considered.**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [X] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

6.5.8 ASAM OpenSCENARIO

ASAM OpenSCENARIO		
Formalia		
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).		**ASAM OpenSCENARIO; Version: 1.0.0; Release Date: 13 Mar 2020**
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')		**ASAM**
Content / Coverage		
Scope of the Standard		
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**The standard defines an XML schema used to create dynamic driving and traffic scenarios. These scenarios contain road participants and their corresponding maneuvers. Multiple ways to define these maneuvers exist. The XML file can be used in a simulator to reproducible simulate a driving scenario.**
	Technologies/methods/processes covered	**Mostly used for simulation.**
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**None**
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[ ] Requirements [ ] Development and Implementation [X] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

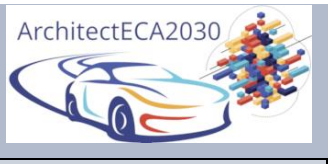
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [**X**] optional [ ] not done at all	**Your line of work is…** **CPS V&V**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			
	Short **description** of this relevance	**Having a standardized format to represent driving situation is necessary for testing, validating and certifying ADAS functions. However, the standard does not directly relate to V&V, test or homologation.**	
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Is **residual risk/probability of failure** handled in this standard? If so, how?		No
ArchitectECA2030			
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project partner(s)) will this standard be used within ArchitectECA2030?			WP/SC/Demonstrator: SC4 Demonstrator "Virtual Validation and Verification Framework" Partners: AVL, SBA
If the Standard is used for a Use-Case/Demonstrator:			
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes**:		
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**The Demonstrator will be concerned with V&V of MonDevs and ADAS functions. In the V&V process also metrics for residual risk and predictive maintenance will be considered.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [**X**] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

6.5.9 ASAM OpenXOntology

ASAM OpenXOntology	

Formalia			
Name of the Standard (incl. Nr., Shorthand ID, etc.). Please also include **version** and **publication date** of the standard (if these can not be derived from the name already).		**ASAM OpenX Ontology; Version: ongoing; Release Date: Jul 2021**	
Standardization Organization / Organization that owns the standard (i.e., ISO, IEC, DIN, UL, ETSI, ASAM,… or 'none yet')		**ASAM**	
(Group of) **Organization(s) that push** this standard (i.e., Members/Leaders of Technical Committee within the Owning Organization and/or writers of the (initial) specification/standard proposal, etc.)		**AVL – Project Lead**	
Content / Coverage			
Scope of the Standard			
	Short **description of scope** (including: does the standard refer to technology, (engineering) processes and/or organization):	**This standard defines common elements of other ASAM OpenX standards, like, OpenDRIVE, OpenSCENARIO, etc. This makes it easier for humans and computers to process the data and establishes an additional layer of compatibility between the OpenX standards.**	
	Technologies/methods/processes covered	**Mostly used for simulation.**	
	Pre-conditions and/or constraints for applying this standard (i.e., 'only for SAE Autonomy level L2 and below systems', 'only for 'military-grade products', 'only for…')	**None**	
	To which **step(s) of the development and lifecycle process** does the standard (mostly) apply:	[ ] Requirements [ ] Development and Implementation [ ] Verification, Validation, Test [ ] Homologation [ ] Operation in the field [ ] Other (pls. specify): _____	
	In **your line of work** / for the business in which your company is active: Applying this standard resp. following this standard is…	[ ] mandatory [ ] optional [ ] not done at all	**Your line of work is…** **CPS V&V**
Is the standard relevant resp. used for **verification/validation/test of CPS** and/or for **homologation** of L3+ Cars (see question two lines up)? **If so**,			

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

	Short **description** of this relevance	**Having a common definition of concepts used in other standards makes it easier to consistently use the standards. However, this is not directly related to V&V, testing or homologation.**
	Which **types of errors/failures/faults** is (the application of) the standard supposed to prevent and/or mitigate?	[ ] **Systematic faults** (i.e., the methods/processes used for building (designing, implementing and testing) the system are insufficient or have been applied wrongly; Examples: Incomplete Specifications, Design bugs, production defects). Absence of these faults means 'the System operates correctly') [ ] **t-way faults** (i.e., the system behaves not according to its specification or has an undesired unspecified behavior, which is caused by an undesired interaction ('bad' combinations of valuations) of **multiple** (i.e., t) **parameters or settings**. [ ] **Random faults** (i.e., typically infrequent disturbances in normal operation, caused e.g. by EMI (electro magnetic interference), ageing, accidental mechanical stress, etc.. These faults are typically not prevented, but mitigated, by e.g., fail-aware/-safe/-operational concepts, redundancy or similar) [ ] **System (behavior) faults** (i.e., the system behaves correctly according to its specification, but the specification is incomplete, e.g., because of situations/scenarios that were not known/considered at design time) [ ] **Malicious faults** (i.e., The system behaves correctly according to its specification, but external actors with malicious intend try to 'hack in', feed incorrect information to the system and/or otherwise try to disturb system operation. Central questions here are 'is this malicious intent detected' and 'how are the consequences of these malicious actions prevented/mitigated).
	Is **residual risk/probability of failure** handled in this standard? If so, how?	No
ArchitectECA2030		
Where (i.e. in which WP, SC and/or in which Demonstrator) and **by whom** (i.e., project		**WP/SC/Demonstrator: Maybe in the SC4 Demonstrator "Virtual Validation and Verification Framework"**

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

partner(s)) will this standard be used within ArchitectECA2030?			Partners:
If the Standard is used for a Use-Case/Demonstrator:			
	Is the Use-Case/Demonstrator supposed to achieve a certain **Safety-Level**?		[ ] Yes [**X**] No [ ] Don't know yet
	If **Yes**:		
		Which Safety-Level is supposed to be achieved?	
		Does this **standard actually help** with achieving this level?	[ ] Yes [ ] Partly [ ] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	
	Will '**residual risk**'/'**probability of failure rate**' be considered in this Use-Case/Demonstrator?		[**X**] Yes [ ] No [ ] Don't know yet
	If **Yes:**		
		Shortly **describe** how residual risk/probability of failure will be considered:	**The Demonstrator will be concerned with V&V of MonDevs and ADAS functions. In the V&V process also metrics for residual risk and predictive maintenance will be considered.**
		Does the standard help you in considering residual risk/probability of failure?	[ ] Yes [ ] Partly [**X**] No
		If **partly**: What is missing?	
		If **partly** or '**no**': Is there another standard that you know of that covers this safety level?	

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

7 Evaluation of the survey's results

In the survey were identified 34 different standards (Figure 7 & Table 2). The standards that were addressed for more than one Supply Chain and important for the overall project are listed in Table 3 and all the others in Table 4 . To underline that ISO 26262 resulted absolutely the more relevant one. If we look to the standards per organizations, 47% are ISO (International Organization for Standardization) and 15% IEEE Standards Association and 15% SAE (Society of Automotive Engineers).

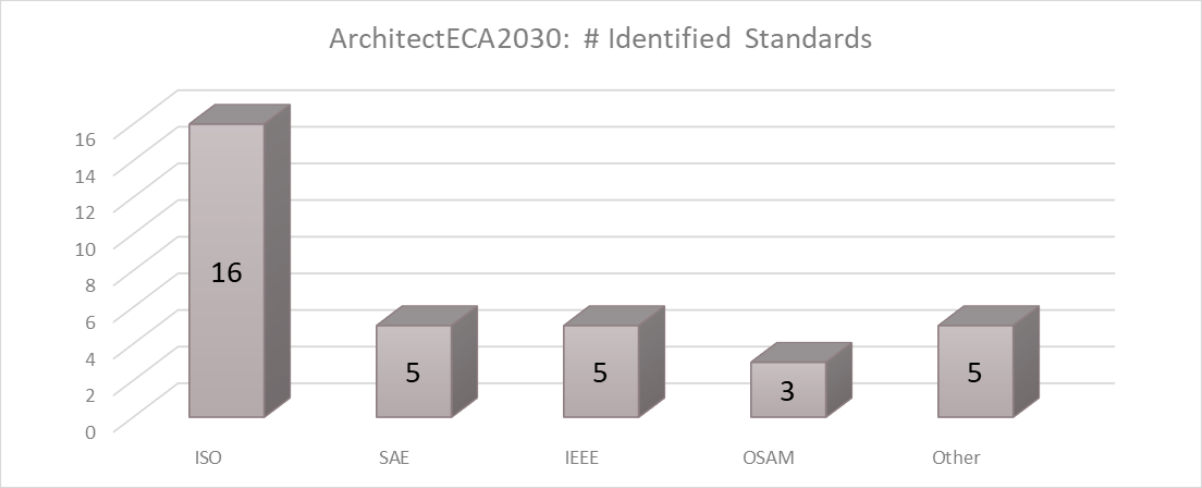


FIGURE 7 IDENTIFIED STANDARDS PER ORGANIZATION (E.G. ISO, SAE, IEEE, ETC.)

TABLE 2 ARCHITECTECA2030 RELEVANT STANDARDS PER ORGANIZATION

ISO	*SAE*	*IEEE*	*OSAM*	*Other*
ISO 17359:2018	SAE J2954	IEEE Std 1856TM-2017	ASAM OpenDRIVE	IEC 61508
ISO 18129:2015	SAE J3061	IEEE P2846	ASAM OpenSCENARIO	IPC-2551
ISO/IEC 25010	SAE J2735	IEEE P2851	ASAM OpenXOntology	ANSI/UL 4600
ISO/IEC TR 24028	SAE J3016	IEEE 802.11p		AEC Q100
ISO15622:2018	SAE JA6268TM	IEEE P2020		ECE/TRANS/WP.29/2020/81
ISO20035:2019				
ISO 17387:2008				
ISO26262				
ISO/PAS 21448				
ISO/TR 4804				
ISO/SAE FDIS 21434				
ISO/TS 16949:2016				
ISO/TR 18161				
ISO 17361:2007(E)				
ISO 11270:2014(E)				
EN ISO 24534				

TABLE 3 MORE FREQUENT STANDARDS

#	*Standards*	*Title*	*Short Description*
1	ISO 26262	Road Vehicles – Functional Safety	ISO 26262-6:2018 is the most recent version of the standard for the **development of software for safety-related systems installed in most road vehicles**. ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			series production passenger cars with a maximum gross vehicle mass up to 3 500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities. Engineering processes and methods (and some organizational issues) to ensure functional safety of E/E systems installed in road vehicles (trucks, cars, etc.), excluding mopeds by prescribing a certain design, implementation and Test (incl. validation and verification) methodology. The 12 parts of the standard deal with: 1) Vocabulary 2) Management of functional safety 3) Concept phase 4) Product development at the system level 5) Product development at the hardware level 6) Product development at the software level 7) Production, operation, service and decommissioning 8) Supporting processes 9) Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis 10) Guidelines on ISO 26262 11) Guidelines on application of ISO 26262 to semiconductors 12) Adaptation of ISO 26262 for motorcycles ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control). https://www.iso.org/standard/43464.html
2	ISO 17359:2018	Condition monitoring and diagnostics of machines — General guidelines	ISO 17359:2018 provides **guidelines for condition monitoring and diagnostics of machines** using parameters such as vibration, temperature, tribology, flow rates, contamination, power, and speed typically associated with performance, condition, and quality criteria. The evaluation of machine function and condition may be based on performance, condition or product quality.
3	ISO 18129:2015	Condition monitoring and diagnostics of machines — Approaches for performance diagnosis	ISO 18129:2015 provides an **introduction on how to apply performance monitoring and diagnostics** for machines, groups of machines, up to complete

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			industrial installation (equipment) typically covering the whole lifetime of the machines.
4	ISO/IEC 25010	Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models	The standard deals with **quality metrics for software engineering in general.** ISO/IEC 25010:2011 defines: 1.A quality in use model composed of five characteristics that relate to the outcome of interaction when a product is used in a particular context of use. This system model is applicable to the complete human-computer system, including both computer systems in use and software products in use. 2.A product quality model that relate to static properties of software and dynamic properties of the computer system. The model is applicable to both computer systems and software products. The characteristics defined by both models are relevant to all software products and computer systems. **Also of interest: ISO/IEC 25012** contains a model for data quality that is complementary to this model. https://www.iso.org/standard/35733.html
5	ISO/IEC TR 24028	Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence	The standard is concerned with the **general trustworthiness of AI applications.** This includes methods to establish trustworthiness (e.g., explainability, transparency, controllability, etc.), associated threads and risks, and methods to assess reliability and safety and approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems. The specification of levels of trustworthiness for AI systems is out of the scope of this document. https://www.iso.org/standard/77608.html
6	ISO/PAS 21448	Road Vehicles – Safety of the intended functionality	The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF). This document provides guidance on the applicable design, verification and validation measures needed to achieve the SOTIF. This document does not apply to faults covered by the ISO 26262 series or to hazards directly caused by the system technology (e.g. eye damage from a laser sensor). https://www.iso.org/standard/70939.html

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

7	ISO/TR 4804	Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation	ISO/TR 4804 **describes steps for developing and validating automated driving systems based on basic safety principles** derived from worldwide applicable publications. It considers safety- and cybersecurity-by-design, as well as verification and validation methods for automated driving systems focused on vehicles with level 3 and level 4 features according to SAE J3016:2018. In addition, it outlines cybersecurity considerations intersecting with objectives for safety of automated driving systems. https://www.iso.org/standard/80363.html
8	ISO/SAE DIS 21434	Road vehicles - Cybersecurity engineering	**Status: under development** Publication: 08/2021 Electrical and electronic components and general system aspect
9	SAE J2954	Surface Vehicle – Wireless Power Transfer for Light-Duty Plug-in/Electric Vehicles and Alignment Methodology	The SAE J2954 standard establishes an industry-wide specification that defines acceptable criteria for interoperability, electromagnetic compatibility, EMF, minimum performance, safety, and testing for wireless power transfer (WPT) of light-duty plug-in electric vehicles. SAE J2954 **addresses unidirectional charging, from grid to vehicle**. This standard is intended to be used in stationary applications (charging while vehicle is not in motion). In this version, only above-ground (surface mounted) installations are covered. SAE J2954 contains requirements for safety, performance, and interoperability. It also contains recommended methods for evaluating electromagnetic emissions.
10	SAE J3016	Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles	SAE J3016 **provides guidelines for the safe conduct of on-road tests of vehicles equipped with prototype conditional, high, and full (levels 3-5) automated driving systems (ADSs)**, as defined by SAE J3016. It does not include guidance for testing production ADSs intended for sale to the general public. The scope is further limited to testing of automated prototype vehicles on public roads. These guidelines do not address: • Testing of driver assist (Level 1) or partial (Level 2) automation systems, which rely on a human driver to monitor the environment. (See SAE J3016 for Definitions of Levels of Automated Systems.) • Closed-course testing. • Component-level testing. The precise regime of road testing for a particular prototype will depend on the intended level of automation and the targeted capabilities of the prototype (see SAE J3016 for more information).

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			A prototype suitable for testing on public roadways is presumed to have already passed laboratory and/or closed-course testing, which are not addressed by this document.
11	IEEE P2846	Assumptions for Models in Safety-Related Automated Vehicle Behavior	The standard IEEE P2846 **identifies reasonable assumptions for automated driving system about the rules of the road and their regional dependencies**. The standard is not exhaustive to guarantee the safety of automated driving systems. Furthermore, the standard defines a method to verify if an automated driving system conforms to these assumptions.
12	IEEE P2851	Exchange/ Interoperability Format for Safety Analysis and Safety Verification of IP, SoC and Mixed Signal Ics	This standard **defines a data format** with which results of functional safety analyses (such as FMEA (Failure Mode and Effects Analysis), FMEDA (Failure Modes, Effects and Diagnostic Analysis), FMECA (Failure Mode, Effects and Criticality analysis), FTA (Fault Tree analysis) and related functional safety verification activities - such as fault injection - executed for IPs (Intellectual Property. See note in section 8.1), SoCs (System on Chip) and mixed signal ICs (Integrated Circuit) can be exchanged and made available to system integrators. The format will define languages, data fields and parameters with which the result of those analyses and verification activities can be represented, in a technology independent way. The goal of the standard is to provide a common ground for EDA (Electronic Design Automation), SoC and IP vendors in needs of developing tools, SoC and IP for functional safety critical applications. https://standards.ieee.org/project/2851.html
13	AEC Q100	Failure mechanism based stress test qualification for integrated circuits	AEC Q100 covers **failure mechanism-based stress tests, minimum stress test driven qualification requirements and test conditions for qualifying Integrated Circuits (ICs).** The idea is to determine devices which can pass the defined stress tests, and provide devices which can offer certain level of quality and reliability in the application. AEC Q100 defines four temperature ranges based on the operating range of ICs. Other related documents are: • AEC Q101 (Discrete semiconductors such as diodes, transistors, etc.) • AEC Q102 (Opto-electronic semiconductors). • AEC Q103 (MEMS pressure sensor devices).

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			• AEC Q104 (Multichip modules). • AEC Q200 (Passive components).
14	IPC-2551	International Standard for Digital Twins	The IPC-2551 **standard is part of the IPC Factory of the Future standards establishing the IPC Digital Twin**, which is comprised of the Digital Twin Product, Digital Twin Manufacturing and Digital Twin Lifecycle frameworks. The standard stipulates and defines Digital Twin properties, types, complexities and readiness levels. The IPC Digital Twin includes historical information about a product, including the history of design in terms of revision and engineering changes, and manufacturing information, that many refer to as the Digital Thread. Digital twins are defined at three different levels: Product definition, Manufacturing information and Lifecycle information.
15	IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems.	**Assessment and quantification of possible failures** according to ISO 61508, (together with IEC 26262 and ISO/PAS 21448). IEC 61508 address aspects to be considered when electrical/ electronic/ programmable electronic (E/E/PE) systems are used to carry out safety functions. Requirements for ensuring that systems are designed, implemented, operated, and maintained to provide the required safety integrity level (SIL). ISO 26262 is the adaptation of the IEC 61508 series of standards to address the sector-specific needs of E/E systems within road vehicles. This standard consists of seven parts.
16	ANSI/UL 4600	Standard for Evaluation of Autonomous Products	UL4600 **describes a safety case approach to ensuring autonomous product safety in general, and self-driving cars in particular.** Information is current as of June 2019. UL 4600 does not try to invent yet another V-cycle-based engineering process for computer-based system safety. Rather, it serves to take the information produced by existing and potentially new design and validation processes and standardizes how to organize the results into a coherent safety case. That safety case provides credible evidence that a highly autonomous vehicle is indeed appropriately safe for deployment. UL 4600 is specifically designed

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			to work well with existing automotive safety standards such as ISO 26262 and ISO/PAS 21448. However, it is generic enough that it can also play well with other standards as autonomy becomes adopted into other domains. (A revision to ISO/PAS 21448 is said to be expanding its scope to handle some of these areas. That new scope is being taken into account with an aim of avoiding unnecessary overlap in the development of UL 4600. Other potentially overlapping standards efforts are similarly being considered based on available information.) https://pr-97195.medium.com/an-overview-of-draft-ul-4600-standard-for-safety-for-the-evaluation-of-autonomous-products-a50083762591
17	IEEE 1856-2017	Standard Framework For Prognostics And Health Management Of Electronic Systems	Information for the implementation of prognostics and health management (PHM) for electronic systems is described in this standard IEEE 1856-2017. A normative framework for classifying PHM capability and for planning the development of PHM for an electronic system or product is also described in this standard. Manufacturers and end users can use this standard for planning the appropriate prognostics and health management techniques to implement and the associated life cycle operations for the system of interest. https://webstore.ansi.org/standards/ieee/ieee18562017

TABLE 4 OTHER IDENTIFIED STANDARDS

#	Standards	Title	Short Description
18	ISO15622:2018	Intelligent transport systems — Adaptive cruise control systems — Performance requirements and test procedures	ISO15622:2018 contains the basic control strategy, minimum functionality requirements, basic driver interface elements, minimum requirements for diagnostics and reaction to failure, and performance test procedures for Adaptive Cruise Control (ACC) systems. https://www.iso.org/standard/71515.html
19	ISO20035:2019	Intelligent transport systems — Cooperative adaptive cruise control systems (CACC) — Performance requirements and test procedures	The standard refers to the technological and engineering aspects of Cooperative Adaptive Cruise Control (CACC) which is an enhancement to the Adaptive Cruise Control (ACC) system by the addition of wireless communication with preceding vehicles and/or the infrastructure to augment the ACC active sensing capability. The document specifically discusses the performance requirements and test procedures for CACC systems.

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			https://www.iso.org/standard/66879.html
20	ISO 17387:2008	Intelligent transport systems — Lane change decision aid systems (LCDAS) — Performance requirements and test procedures	ISO 17387:2008 specifies system requirements and test methods for Lane Change Decision Aid Systems (LCDAS). LCDAS are fundamentally intended to warn the driver of the subject vehicle against potential collisions with vehicles to the side and/or to the rear of the subject vehicle, and moving in the same direction as the subject vehicle during lane change manoeuvres. This standardization addresses LCDAS for use on forward moving cars, vans and straight trucks in highway situations. https://www.iso.org/standard/43654.html
21	ISO/TS 16949:2016	Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations	ISO/TS 16949:2009, in conjunction with ISO 9001:2008, defines the quality management system requirements for the design and development, production and, when relevant, installation and service of automotive-related products. ISO/TS 16949:2009 is applicable to sites of the organization where customer-specified parts, for production and/or service, are manufactured. Supporting functions, whether on-site or remote (such as design centers, corporate headquarters and distribution centers), form part of the site audit as they support the site, but cannot obtain stand-alone certification to ISO/TS 16949:2009. ISO/TS 16949:2009 can be applied throughout the automotive supply chain. https://www.iso.org/standard/52844.html
22	ISO/TR 18161	Automation systems and integration — Applications integration approach using information exchange requirements modelling and software capability profiling	ISO/TR 18161:2013 describes an approach for using ISO 16100 and ISO 18435 to specify information exchange requirements between applications. https://www.iso.org/standard/60899.html This standard describes method for data exchange among physical product equipped with sensors, control and acquisition software, and diagnostics software. It includes an example of this approach as applied to describing the interoperability requirements of an integrated smart pump application.
23	ISO 17361:2007(E)		

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

24	ISO 11270:2014(E)	Intelligent transport systems — Lane departure warning systems — Performance requirements and test procedures	The main system function of a Lane Keeping Assistance System (LKAS) is to support the driver in keeping the vehicle within the current lane. LKAS acquires information on the position of the vehicle within the lane and, when required, sends commands to actuators to influence the lateral movement of the vehicle. LKAS provides status information to the driver. This standard provides references to technological and engineering requirements as well as test procedures of such systems. New Version 2017 https://www.iso.org/standard/72349.html
25	EN ISO 24534	Intelligent transport systems — Automatic vehicle and equipment identification — Electronic registration identification (ERI) for vehicles — Part 3: Vehicle data	Provides requirements for electronic registration identification (ERI) that are based on an identifier assigned to a vehicle (e.g., for recognition by national authorities), and adheres to privacy and data protection regulations. Part 1 (Architecture) provides an overview of the ERI system concept regarding the onboard vehicle components and the external off-vehicle components required for an operational system. The detailed requirements are defined in Part 2 (operational requirements), Part 3 (intelligent transport systems), and Part 4 (secure communications using asymmetrical techniques).
26	SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	This recommended practice provides guidance on vehicle Cybersecurity and was created based off of, and expanded on from, existing practices which are being implemented or reported in industry, government and conference papers. The best practices are intended to be flexible, pragmatic, and adaptable in their further application to the vehicle industry as well as to other cyber-physical vehicle systems (e.g., commercial and military vehicles, trucks, busses). https://www.sae.org/standards/content/j3061_201601/
27	SAE J2735	(R) Dedicated Short Range Communications (DSRC) Message Set Dictionary	Specifies a message set, and its data frames and elements, for use by vehicle-to-everything (V2X) communications system applications. The data dictionary was initially designed for use over DSRC, but this document is intended to be independent of the underlying communications protocols used to

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

			exchange data between participants in V2X applications.
28	SAE JA6268TM	Design & Run-Time Information Exchange for Health-Ready Components, April 2018	It provides standard templates for main components that can be found in a vehicle, describing their failure modes, the mechanism to monitor their heath, and run time data required to enable health monitoring. The standard templates are hosted by HRCSTM and will be made available to the public in in the spring of 2021.
29	IEEE 802.11p	IEEE Standard for Information technology -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Wireless Access in Vehicular Environments.	Amendment 6 specifies the extensions to IEEE 802.11 standard for wireless local area networks (WLANs) providing wireless communications while in a vehicular environment.
30	IEEE 802.11bp	Standard for Information technology-- Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment: Enhancements for Next Generation V2X.	This amendment provides enhancements for the next generation V2X.
31	IEEE P2020	Standard for Automotive System Image Quality	Address fundamental attributes that contribute to image/ quality for automotive Advanced Driver Assistance Systems (ADAS) applications and identifying existing metrics and other useful information relating to these attributes. Define a standardized suite of objective and subjective test methods for measuring automotive camera image quality attributes. Specify tools and test methods to facilitate standard-based communication and comparison among Original Equipment Manufacturer (OEM) and Tier 1 system integrators and component vendors.

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

32	UNECE Regulation 157	Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems	The intention of the Regulation is to establish uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems (ALKS). It contains administrative provisions suitable for type approval, technical requirements, audit and reporting provisions and testing provisions.
33	ASAM OpenDRIVE		The standard defines a formal XML schema used to define road networks and static objects. In addition, the objects can have different properties, for example, lane width. The XML file can be used to reproducible generate 3D road network for a simulation.
34	ASAM OpenSCENARIO		The standard defines an XML schema used to create dynamic driving and traffic scenarios. These scenarios contain road participants and their corresponding maneuvers. Multiple ways to define these maneuvers exist. The XML file can be used in a simulator to reproducible simulate a driving scenario.
35	ASAM OpenXOntology		This standard defines common elements of other ASAM OpenX standards, like, OpenDRIVE, OpenSCENARIO, etc. This makes it easier for humans and computers to process the data and establishes an additional layer of compatibility between the OpenX standards.

49% of the identified standards are from the SC3 *Failure modes, fault detection and residual risk for safety and security in* ***connectivity*** *systems*, followed by 22% of the SC4 *Failure modes, fault detection and residual risk for* ***safety security privacy on overall system "monitoring device" architecture.***

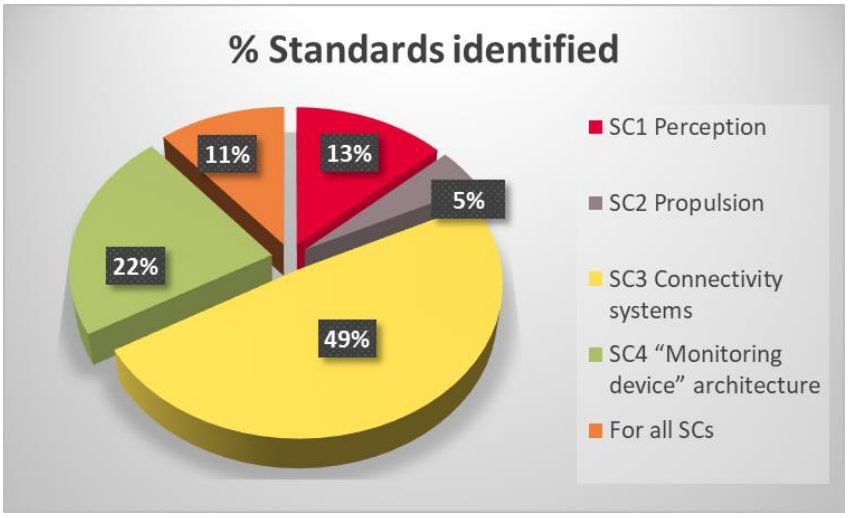


FIGURE 8 HISTOGRAM AND 3-D PIE OF THE NUMBER OF STANDARDS IDENTIFIED BY EACH SUPPLY CHAIN

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

Taking into consideration only the standards containing the information on which step(s) of the development and lifecycle process does the standard (mostly) apply, we see that 25% is assigned to both Requirements and verification, validation, test steps. Followed by 20% in the operation on the field and 19% for development and implementation.

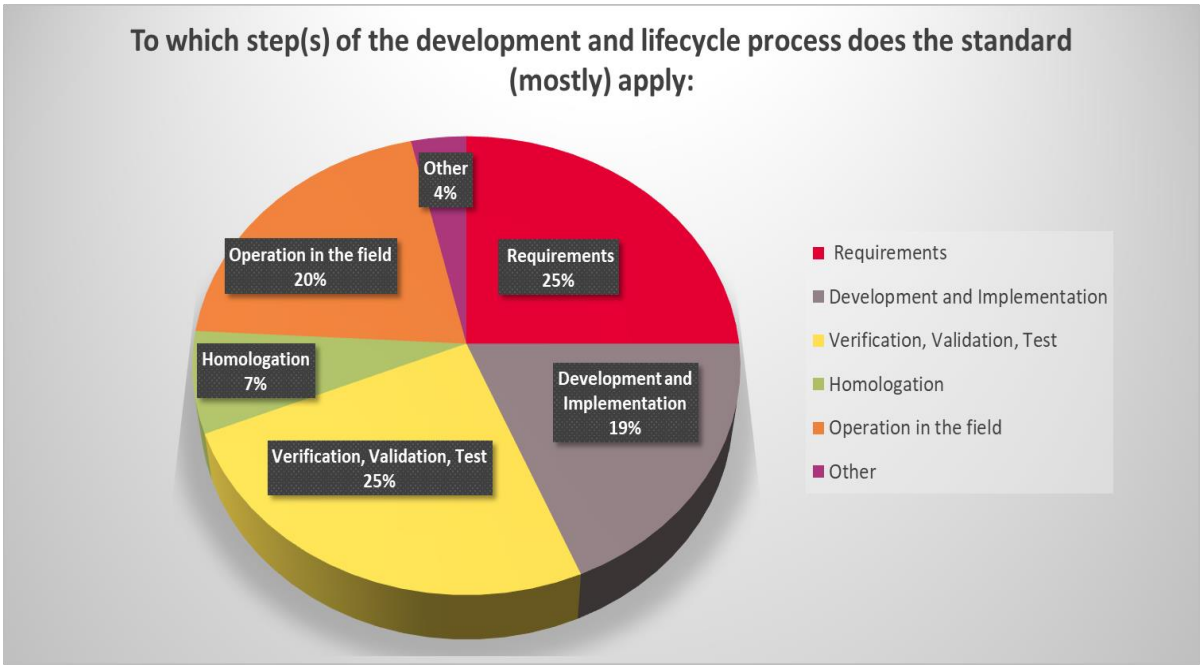


FIGURE 9 3-D PIE RELATED TO THE STEPS OF THE DEVELOPMENT AND LIFECYCLE PROCESS DOES THE STANDARD (MOSTLY) APPLY

Regarding the question "which type of errors/faults is the standard supposed to prevent and/or mitigate", the winner is ***systematic faults*** with 29% followed by 24% of ***random faults*** and 24% ***system (behaviour) faults.***

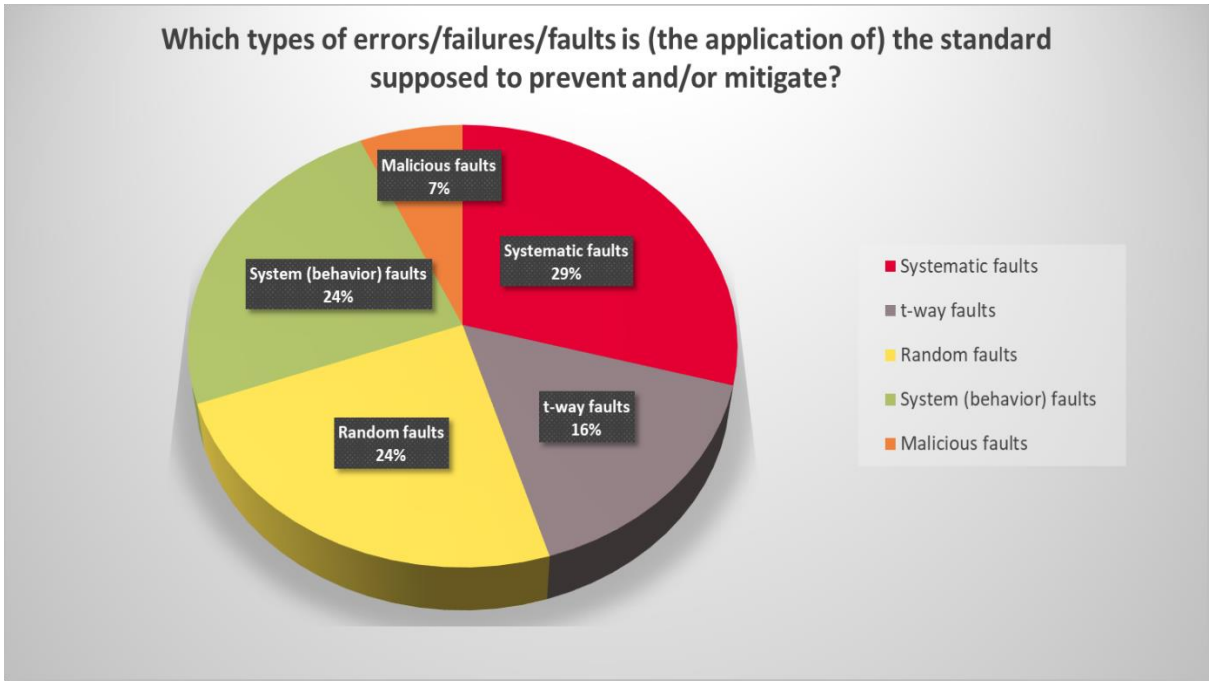


FIGURE 10 3-D PIE RELATED TO WHICH TYPES OF ERRORS/FAULTS IS THE STANDARD SUPPOSED TO PREVENT AND/OR MITIGATE

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

8 Conclusion

8.1 Contribution to overall picture

The deliverable describes the results of the survey on standards involvement in ArchitectECA2030 project, technologies concerned and standardization plan. This is the basis for **the ArchitectECA2030's framework** that shall cover the methods, tools, processes, and pilot data which are necessary to homologate as well as to periodically re-certificate ECS of ECA vehicles. The continuous application of existing standards and norms will be tackled to keep the pace with the fast advancements of automated driving functions.

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.

Taking into consideration only the standards containing the information on which step(s) of the development and lifecycle process does the standard (mostly) apply, we see that 25% is assigned to requirements and 25% to verification, validation, and test steps. Followed by 20% in the operation on the field and 19% for development and implementation. Regarding the question "which type of errors/faults is the standard supposed to prevent and/or mitigate", the winner is *systematic faults* with 29% followed by 24% of *random faults* and 24% *system (behaviour) faults.*

This deliverable together with D7.2 "***External Stakeholder Strategy",*** with which we have identified the stakeholder groups by categorizing organisations with respect to the role that they have in the value chain, lays the foundations for providing an implementation of an in-vehicle monitoring device that reliably measures the health status and takes appropriate actions in case of malfunctioning of subsystems in an autonomous and automated vehicle.

8.2 Contribution to demonstration

The present deliverable is fundamental for the demonstration, as it presents the identified standards of the ArhictectECA2030 demonstrators, together with initial ideas for their realization.

The mapping of existing standards, including why relevant and how to use them, are included in the deliverables D1.1 – D1.4 for each supply chain and demonstrator.

9 References & Good to Know

[1] "Taxonomy and Definitions for Terms Related to Driving Automation Systems for OnRoad Motor Vehicles," J3016_201806, SAE International, 15 June 2018. Available at https://www.sae.org/standards/content/j3016_201806/ (as of 7 May 2019).

[2] "Autonomous Vehicle Market by Level of Automation (Level 3, Level 4, and Level 5) and Component (Hardware, Software and Service) and Application (Civil, Robo Taxi, Self-driving Bus, Ride Share, Self-driving Truck, and Ride Hail)–Global Opportunity Analysis and Industry Forecast, 2019-

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

2026," industry report by Allied Market Research, May 2018. Summary available at https://www.alliedmarketresearch.com/autonomousvehicle-market (as of 7 May 2019).

[3] "Self-Driving Market Becomes a Reality in the U.S. by 2026, As 1 in 4 New Vehicles Sold Becomes Driverless," press release issued by Juniper Research in conjunction with the release of their report "Autonomous Vehicle & ADAS Readiness Index, Player Positioning & Forecast 2018-2026," 23 May 2018. Available at https://www. juniperresearch.com/press/press-releases/self-driving-market-becomes-a-reality (as of 7 May 2019).

[4] "Intel predicts a $7 trillion self-driving future," posted to the website The Verge, June 1, 2017. Available at https://www.theverge.com/2017/6/1/15725516/intel-7-trillion-dollarself-driving-autonomous-cars (as of 7 May 2019).

[5] "Cyber-Physical Systems," from the website of the U.S. National Institute of Standards and Technology (NIST). Available at https://www.nist.gov/el/cyber-physical-systems (as of 7 May 2019).

[6] "Framework document on automated/autonomous vehicles," prepared by the Secretariat of the United Nations World Forum for Harmonization of Vehicle Regulations, 15 April 2019. Available at https://www.unece.org/fileadmin/DAM/trans/ doc/2019/wp29/ECE-TRANS-WP29-2019-34e.pdf (as of 7 May 2019)

[7] https://www.tuvsud.com/en/e-ssentials-newsletter/automotive-essentials/e-ssentials-01-2020/status-of-homologation-of-autonomous-vehicles

[8] https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll

10 List of figures

Figure 1 Landscape of Bodies and committees 11
Figure 2 Type approval procedure for ECA vehicles. "Hochautomatisierte Systeme: Testen, Safety und Entwicklungsprozesse – Roadmap Forschungsfelder und Handlungsempfehlungen", SafeTRANS, November 2017 12
Figure 3 Standardization deliverables Plan 13
Figure 4 Representation of Standardization plan and certification 14
Figure 5 Example of V-Model Mapping. 14
Figure 6 Word-cloud of the standards' titles. 18
Figure 7 Identified standards per organization (e.g. ISO, SAE, IEEE, etc.) 149
Figure 8 Histogram and 3-D pie of the number of standards identified by each supply chain 159
Figure 9 3-D Pie related to the steps of the development and lifecycle process does the standard (mostly) apply 160
Figure 10 3-D Pie related to which types of errors/faults is the standard supposed to prevent and/or mitigate 160

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

11 List of Tables

Table 1 Template – Survey Description 15
Table 2 ArchitectECA2030 relevant standards per organization 149
Table 3 More frequent standards 149
Table 4 Other identified standards 155

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

12 GLOSSARY OF ACRONYMS

ADS – Automated Driving System

AV – Automated Vehicles CAGR

CAGR –Compound Annual Growth Rate

CATARC– China Automotive Technology and Research Center

CETRAN – Centre of Excellence for Testing and Research of AVs

C-NCAP – China New Car Assessment Program

DDT – Dynamic Driving Task Euro

NCAP – European New Car Assessment Program

IAMTS – International Alliance for Mobility Testing and Standardization

ITIC – International Transportation Innovation Center

ISO – International Organization for Standardization

JNCAP – Japan's New Car Assessment Program

NCAP – New Car Assessment Program

NHTSA – National Highway Traffic Safety Administration

ODD – Operational Design Domain

OEDR – Object and Event Detection and Response

OEM – Original Equipment Manufacturer

SOTIF – Safety of the Intended Functionality

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.

- Last page of the document is intended to be blank! -

This document and the information contained may not be copied, used or disclosed, entirely or partially, outside of the ArchitectECA2030 consortium without prior permission of the partners in written form.