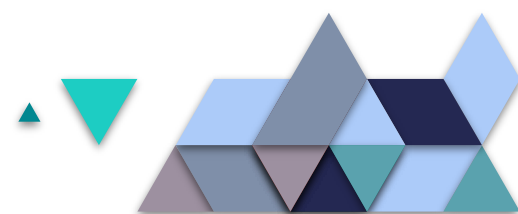




*Trustable architectures with acceptable residual risk for the electric,  
 connected and automated cars*

<b>Deliverable</b>	<i>Report on requirements and specifications for residual risk in connectivity systems.</i>		
<b>Deliverable File</b>	<i>D1.3</i>		
<b>Project</b>	ArchitectECA2030	<b>Grant Agreement Number</b>	877539
<b>Lead Beneficiary</b>	SINTEF	<b>Dissemination Level</b>	Public
<b>Involved SCs</b>	SC3	<b>Related Task/s</b>	T1.03
<b>Due Date</b>	June 2021 (m12)	<b>Actual Submission Date</b>	m13
<b>Status</b>	Final	<b>Version</b>	V1.0
<b>Contact Person</b>	Ovidiu Vermesan	<b>Organisation</b>	SINTEF
<b>Phone</b>	+47 930 59 322	<b>E-Mail</b>	Ovidiu.Vermesan@sintef.no



<b>Document history</b>			
<b>V</b>	<b>Date</b>	<b>Author</b>	<b>Description</b>
0.01	01.12.2020	SINTEF	Initial Version
0.02	02.12.2020	SINTEF	Draft structure
0.03	04.02.2021	SINTEF	Structure update and input SSC 3.1
0.04	19.02.2021	ALL SC3 partners	Agreement on the final document structure.
0.05	20.05.2021	SINTEF	Structure/title updates.
0.06	07.06.2021	SINTEF, IFAG	Update SC3 overview
0.07	16.06.2021	SINTEF	Contribution on introduction and scope.
0.08	18.06.2021	SINTEF, TSENSE, NXT	Contribution on SSC 3.1.
0.09	18.06.2021	TSENSE	SSC 3.1 updates on NFRs and FRs.
0.10	18.06.2021	NXP	Contribution on SSC 3.3.
0.11	21.06.2021	INRIA	Contribution and updates on SSC 3.3.
0.12	23.06.2021	SINTEF	Structure update (Treatment of residual risk).
0.13	23.06.2021	NXP, TUDE	Contribution on SSC 3.2.
0.14	25.06.2021	DATA	Additional inputs and updates on SSC 3.3.
0.15	25.06.2021	TSENSE	Additional inputs and updates on SSC 3.1.
0.16	27.06.2021	NXP, TUDE	Additional inputs and updates on SSC 3.2.
0.17	29.06.2021	SINTEF	Contribution on SSC 3.1.
0.18	30.06.2021	SINTEF	Additional contribution on SSC 3.1.
0.19	02.07.2021	NXP	Additional contribution on SSC 3.3.
0.20	02.07.2021	SINTEF	Overall updates.
0.21	05.07.2021	INRIA	Updates on SSC 3.3.
0.22	05.07.2021	NXP, TUDE	Updates and new inputs on SSC 3.2, plus contribution on the conclusions.
0.23	06.07.2021	INRIA	Updates and new inputs on SSC 3.3, plus contribution on the conclusions.
0.24	07.07.2021	SINTEF	Inputs/updates on introduction, SC3 overview, SSC 3.1 demonstrator and conclusions.
0.25	08.07.2021	DATA	Update 10.2, 10.3, 10.4, 10.5.
0.26	09. 07.2021	NXP	Inputs/updates on introduction SSC 3.3. demonstrator, and conclusions.
0.27	09. 07.2021	SINTEF	Final check
1.00	09. 07.2021	IFAG	Final and reviewed 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).

## Table of contents

<b>1</b>	<b>Executive/ Publishable summary</b> .....	<b>5</b>
<b>2</b>	<b>Non publishable information</b> .....	<b>5</b>
<b>3</b>	<b>Introduction &amp; Scope</b> .....	<b>5</b>
3.1	Purpose and target group .....	5
3.2	Contributions of partners .....	6
3.3	Relation to other activities in the project.....	6
3.4	Main objectives and key targets overview .....	6
3.4.1	Objective overview .....	6
3.4.2	Key target overview.....	7
<b>4</b>	<b>System level view</b> .....	<b>8</b>
<b>5</b>	<b>SC3 overview, structure, and demonstrators</b> .....	<b>9</b>
<b>6</b>	<b>SSC 3.1 Road condition detection and V2X connectivity (RCD-V2X)</b> .....	<b>11</b>
6.1	Target goals and achievements .....	11
6.2	Demonstrator structure.....	11
6.3	Demonstrator description.....	13
6.4	Treatment on residual risk.....	15
6.5	Demonstrator relations to the main objectives and key targets.....	16
6.5.1	Objectives .....	16
6.5.2	Key targets.....	17
6.6	Homologation framework mapping.....	17
6.7	Non-functional requirements, KPIs, and measures .....	18
6.8	Functional requirements, KPIs, and measures .....	20
6.9	Mapping to existing standards.....	21
6.10	Verification and validation.....	24
6.11	Demonstrator milestones .....	25
<b>7</b>	<b>SSC 3.2 Digital twin package monitoring (DigiPack)</b> .....	<b>25</b>
7.1	Target goals and achievements .....	25
7.2	Demonstrator structure.....	26
7.3	Demonstrator description.....	28
7.4	Treatment on residual risk.....	28
7.5	Demonstrator relations to the main objectives and key targets.....	29
7.5.1	Objectives .....	29

7.5.2	Key targets .....	30
7.6	Homologation framework mapping.....	30
7.7	Non-functional requirements, KPIs, and measures .....	30
7.8	Functional requirements, KPIs, and measures .....	32
7.9	Mapping to existing standards.....	34
7.10	Verification and validation.....	35
7.11	Demonstrator milestones .....	36
<b>8</b>	<b>SSC 3.3 Built-in Connectivity Component Ageing Monitoring (BIAM).....</b>	<b>36</b>
8.1	Target goals and achievements .....	36
8.2	Demonstrator structure.....	36
8.3	Demonstrator description.....	38
8.4	Treatment on residual risk.....	38
8.5	Demonstrator relations to the main objectives and key targets.....	39
8.5.1	Objectives .....	39
8.5.2	Key targets.....	39
8.6	Homologation framework mapping.....	39
8.7	Non-functional requirements, KPIs, and measures .....	40
8.8	Functional requirements, KPIs, and measures .....	41
8.9	Mapping to existing standards.....	43
8.10	Verification and validation.....	44
8.11	Demonstrator milestones .....	44
<b>9</b>	<b>SC3 demonstrators summarized .....</b>	<b>45</b>
<b>10</b>	<b>Conclusion .....</b>	<b>46</b>
10.1	Contribution to overall picture .....	46
10.2	Relation to the state-of-the-art and progress beyond it .....	46
10.3	Impacts to other WPs, Tasks and SCs .....	47
10.4	Contribution to demonstration.....	48
10.5	Other conclusions and lessons learned .....	48
<b>11</b>	<b>References.....</b>	<b>50</b>
<b>12</b>	<b>List of figures .....</b>	<b>52</b>
<b>13</b>	<b>List of tables .....</b>	<b>53</b>

## 1 Executive/ Publishable summary

The objective of the deliverable D1.3 is to define the non-functional (NFRs) and functional (FRs) requirements for the three demonstrators developed in the supply chain SC3 dealing with failure modes, fault detection and residual risk for safety analysis in autonomous vehicles connectivity systems. The demonstrators cover topics such as road condition detection and V2X connectivity (RCD-V2X), digital twin package monitoring (DigiPack) and a built-in connectivity component ageing monitoring (BIAM). The work in this deliverable is combined with a methodology for identifying residual risks in the connectivity domain and the interaction to automated and connected vehicles and linking with the standardisation framework provided by ISO/PAS 21448: Road Vehicles - Safety of the intended functionality (SOTIF). In this context, an overview of the existing standards relevant to the work is presented, and gaps are identified to address future standardisation work. The requirements and specifications expedite the integration of residual risk framework for connectivity systems connected with perception devices. To cover the different scenarios for identifying residual risk, the SC3 uses the idea of Operational Design Domain (ODD) as defined in SAE J3016 to indicate where the elements/components/systems of the autonomous and connected vehicle can operate safely.

The identification of the NFRs is based on the applicability of ISO/IEC 25010 characteristics and sub-characteristics for defining the NFRs and the selection of appropriate key performance indicators (KPIs) and measures these requirements. The features or the FRs of the systems developed in the demonstrators are evaluated using actions linked to KPIs related to SW/HW concerning a result of behaviour that a function of the system shall implement. FRs specify the function that the element/component/system implemented in the demonstrators can perform.

The summary and conclusions provide an overview of the FRs and NFRs used in the three demonstrators in SC3 and discuss the issue related to residual risk identification and the approach to support the homologation framework for connected autonomous vehicles.

## 2 Non publishable information

N.A. (The dissemination level of this deliverable is public).

## 3 Introduction & Scope

### 3.1 Purpose and target group

This report is the outcome of task T1.03 (Requirements and specifications for residual risk in connectivity systems). The purpose is the requirements and specifications for defining the methodology for identifying residual risks in the perception and connectivity domains, and their interaction for automated and connected vehicles and link with the standardisation framework provided by ISO/PAS 21448: Road Vehicles - Safety of the intended functionality (SOTIF) [12]. The requirements and specifications facilitate the residual risk framework integration for connectivity systems connected with perception devices.

The document containing the functional and non-functional requirements, the KPIs and measures for the demonstrators provided in SC3 and the methodology for identifying residual risks in connectivity domain and its relation to connected perception systems.

## 3.2 Contributions of partners

**TABLE 1: CONTRIBUTIONS OF PARTNERS**

Chapter	Partner	Contribution
1; 2; 3; 4; 5; 6; 9; 10	SINTEF	Filled the roles as both SC3, SSC3.1 and D1.03 leader and coordinated the work accordingly. Contribution on the overall document and SSC 3.1: Road condition detection and V2X connectivity (RCD-V2X) in particular.
8; 10	DATA	Contribution on SSC 3.3 in Chapter 8.3, 8.4, 8.7 and 8.8.
8; 10	INRIA	Contribution on demonstrator in SSC 3.3.
7; 8; 10	NXP	Contribution on SSC 3.2 in Chapter 7.4, 7.7, 7.8, 7.11. Contribution on SSC 3.3 in Chapter 8.1, 8.2, 8.3, 8.5 and 8.7.
6; 10	NXT	Contribution on SSC 3.1: Road condition detection and V2X connectivity (RCD-V2X), with focus on residual risk, multi-sensor solutions and V2X communication.
6; 10	TSENSE	Contribution on SSC 3.1: Road condition detection and V2X connectivity (RCD-V2X), with focus on residual risk, functional and non-functional requirements related to friction prediction and the road surface conditions monitoring system.
7; 10	TUDE	Contribution on SSC 3.2 in Chapter 7.1, 7.2, 7.3, 7.5, 7.6, 7.9, and 7.10.

## 3.3 Relation to other activities in the project

All three sub-supply chains (SSCs) and their targeted demonstrators in supply chain 3 (SC3) are represented in this work. The results of this WP1 work will be used as guidelines in the work for the consecutive work packages. In particular; task T4.1 "Identification and management of risks in automotive ECS in the connectivity and perception interacting domains", task T5.1 "Integration of the residual risk framework in connectivity and perception systems", and task T6.1 "Validation of mission oriented ECS in the connectivity and perception interacting domains" in WP4, WP5, and WP6, respectively.

The work reflected in this deliverable report is part of milestone MS1 "Requirements and targets available initial concept for monitoring device prepared".

## 3.4 Main objectives and key targets overview

### 3.4.1 Objective overview

The mission of the Architect ECA 2030 project is to define a harmonized pan-European validation framework for electronic components and systems (ECS), and the methods, tools, metrics around it, coordinated with global, and regional activities for electric, connected, and automated (ECA) vehicles including periodical re-validation and certification.

Increased safety and reliability of ECS-defined ECA vehicles given a well-defined and acceptable residual risk shall be achieved by addressing the system architecture, the system components and the semiconductors along the entire development and value chain.

To achieve that, the following five overall objectives (O) are focused on and addressed in this project:

**O1 - Continuous robust design optimization for each part in the ECS value chain (Technical):** Related to ensuring secure connected, cooperative, and automated mobility and transportation; and managing critical, autonomous, cooperating evolvable systems. The outcome is robust mission validated design. The objective's KPI addresses coverage components.

**O2 - Framework for safety validation of ECS value chain (Technical):** Related to managing critical, autonomous, cooperating, evolvable systems; managing complexity; and increasing compactness and capabilities by functional and physical systems integration. The outcome is accepted residual risk in ACS for HAD to enable type approval. The objective's KPI addresses coverage validation.

**O3 - Identification and management of residual risks over the entire ECS value chain (Technical):** Related to ensuring secure connected, cooperative, and automated mobility and transportation; and reliability and functional safety. The outcome is accepted monitoring device methodologies. The objective's KPI addresses coverage qualification.

**O4 - End-user acceptance by trustworthy ECS value chain (Value):** Related to ensuring secure connected, cooperative, and automated mobility and transportation; and secure, safe, and trustable connectivity and infrastructure. The outcome is usability. The objective's KPI addresses coverage test.

**O5 - Zero emissions, crashes, and congestions by ECA2030 vehicle (Value):** Related to ensuring secure connected, cooperative, and automated mobility and transportation; and increasing compactness and capabilities by functional and physical systems integration. The outcome is sustainability. The objective's KPI addresses energy efficiency shorter validation time.

In addition, five supply chain specific objectives are defined:

**SC3-01:** Investigate the residual risks of subsystems, and systems. Analysis, assessment and quantification of fault modes and their consequences on communication systems.

**SC3-02:** Providing methods and tools for fault detection, localization, and repair.

**SC3-03:** Verification methodologies specifically adapted to ensure safety requirements.

**SC3-04:** Apply the planned system integrity and dependability measures into account (security, safety, reliability, resilience, maintainability, and availability) to create the basis for the homologation and validation of the connectivity functions for automated and connected vehicles as mission- and safety-critical systems.

**SC3-05:** Development of a demonstrator showing applicability of the proposed methods.

### 3.4.2 Key target overview

The five overall objectives of described above, together with the vision of mission-oriented qualification of ECA vehicles supported by lifecycle monitoring based upon monitoring devices gives rise to five key targets (KT).

Several key targets contribute to and support several objectives and supply chains (SC). The five key targets addressed are described below.

**KT1 - Architectures, components, sub-systems enabling virtual development and validation (monitoring device, failure risk):** Currently no agreed development framework exists to certify SAE L3+ automated driving functions in unstructured environments and adverse weather conditions using *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.*

virtual validation methods. The reduction of the validation process compared to a mileage accumulation driven approach will be shown. Additionally, the project will illustrate that the proposed framework is appropriate for certification of SAE L3+ automated driving functions on case studies within the project.

**KT2 - Methods and tools to validate the models used in virtual validation (lifetime monitoring, residual risk, methods, and tools):** The incorporation of real-world test data into the virtual V&V process, in combination with test data derived from a knowledge base, is most likely the key to develop, certify and re-certify automated vehicles with reasonable costs and efforts. As an assessment the project will provide a knowledge base that integrates pertinent data for safety validating and testing CAVs ECA vehicles and illustrate the alimentation of a corresponding data base with pilot test data generated by the monitoring device.

**KT3 - Metrics for quality assurance for ECS (mission-oriented qualification, residual risk):** Standardized safety, security and privacy metrics are of high relevance for type approval, vehicle operation residual risks (e.g., insurance) and homologation procedures. As an assessment, the project will illustrate the introduced coverage metrics by application of the homologation framework on case studies within the project. The project will show on case studies in a lab demonstrator within the project, proposed techniques keeping the residual risk less than  $10E-9/h$ .

**KT4 - Definition and understanding of test coverage (residual risk, design feedback, lifetime monitoring, aggregated risk):** The system understanding is the precondition to elaborate the homologation of automated vehicles. The functional safe design, system availability, and safe operation are mandatory to bring the vehicles into real traffic operation. As an assessment, the project will illustrate that the proposed processes and requirements enable to meet the expected increase of availability on case studies within the project. Reduction of homologation effort by virtual validation. Reduction of fatalities which might happen during homologation only occur in virtual environment and therefore issues are not perceived as severe as in real world driving. This increases customer acceptance.

**KT5 - Methods for shorter validation in respect to acceptable residual risk (methods):** The project's goal is to provide methods for shorter validation in respect to an acceptable residual risk. The project will bring together representative stakeholders from public authorities and reduce the heterogeneity of regulations to allow autonomous mode by introducing the developed homologation framework. As an assessment, the project will provide the list of propositions emanating from the project that found their way into international standards.

## 4 System level view

The demonstrators investigated in the supply chain are all to be found on the element and component level of the overall vehicle level hierarchy as illustrated in Figure 1.

The vehicle HW/SW partitioning describes the grouping of the elements, components, subsystems, systems, and functions in a vehicle assigned to the vehicle's respective functional areas and domains.

The way the individual parts, features and resulting functions are implemented is achieved using the appropriate architecture. In this context, the term "system vehicle domains" defines a modular group architecture containing subsystems addressing specific vehicle functions (e.g., propulsion, perception, connectivity).

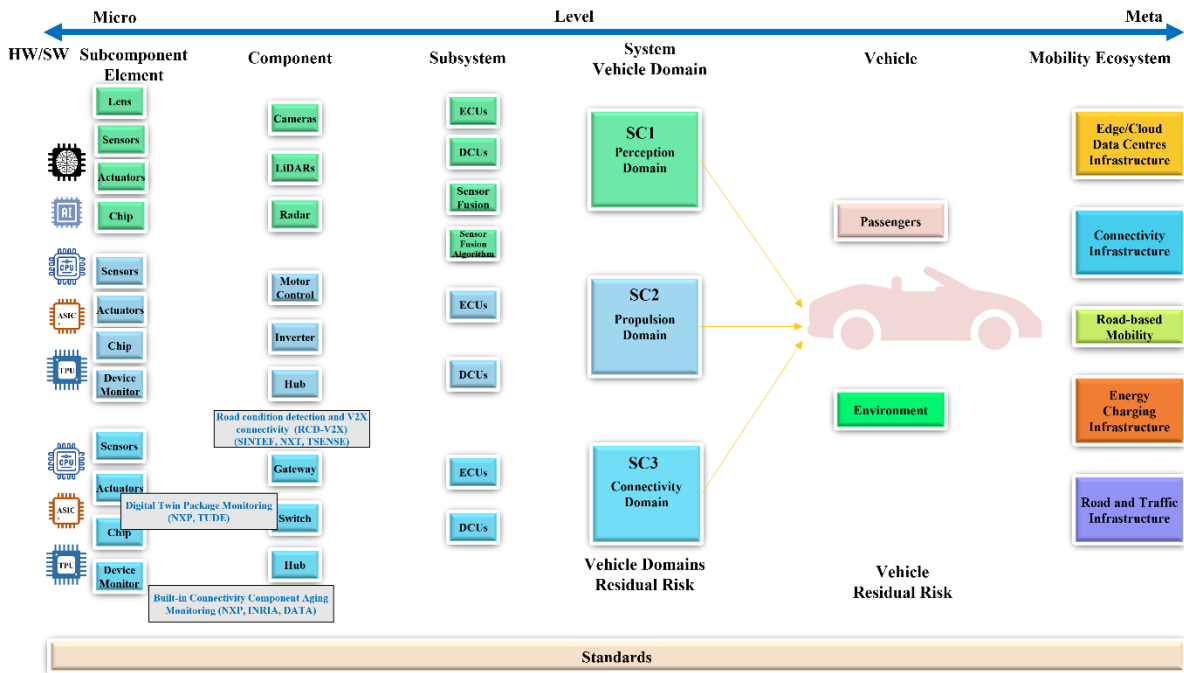


FIGURE 1: SC 3 DEMONSTRATORS

The following chapters provide detailed insight on the requirements per demonstrator.

## 5 SC3 overview, structure, and demonstrators

The system understanding is the precondition to elaborate the homologation of autonomous and connected vehicles.

The functional, safe design, system availability, and safe operation are mandatory to bring the vehicles into actual traffic conditions.

Supply chain SC3 is addressing failure modes, fault detection and residual risk for safety analysis in autonomous vehicles connectivity systems.

SC3 aims to investigate residual risks of subsystems, used to build the connectivity functions for autonomous vehicles, and identify the key elements needed to support building an overall methodology for risk estimations of connectivity systems.

The work is addressing the assessment and quantification of possible failures according to the standards ISO 26262 and ISO/PAS 21448: SOTIF.

The SC3 includes three demonstrators that cover topics such as road condition detection and V2X connectivity (RCD-V2X), digital twin package monitoring (DigiPack) and a built-in connectivity component ageing monitoring (BIAM).

The structure of the supply chain and the content addressed by the three demonstrators are illustrated in Figure 2.



### SSC3.1 (TSENSE, NXT, SINTEF):

Road condition detection and V2X connectivity

- Detect road condition and fusion the data for V2X communication
- Sensor model and prototype for road conditions and friction evaluation.
- On board unit (OBU) for information fusion and connectivity.
- Experimental set-up suitable for investigations of residual risks of systems and subsystems used to build the sensors and connectivity functions.



### SSC3.2 (NXP, TUDE):

Digital Twin Package Monitoring

- Method for monitoring IC packages
- Data-sensing module prototype for collecting environmental parameters such as temperature, humidity, vibrations.
- Evaluation of current state of degradation based on ageing mechanisms.
- Data-driven algorithms for prediction of remaining useful life of the degraded component

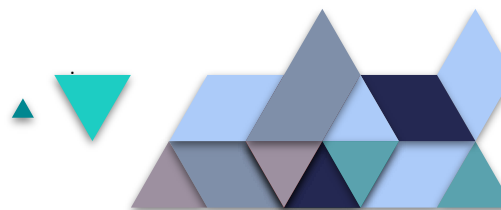


### SSC3.3 (NXP, INRIA, DATA)

Built-in Connectivity Component Aging Monitoring

- Method for built-in IC monitoring
- Monitor IC health condition in the field to make it possible for Fail-predication
- SW/HW communication infrastructure to handle monitoring data
- Evaluation of different types of ageing monitors, including monitoring of digital ICs and analogue components for different front-end processes.

FIGURE 2: SC 3 DEMONSTRATORS STRUCTURE AND CONTENT



The overall timeline for the three demonstrators is visualised in **Error! Reference source not found.**

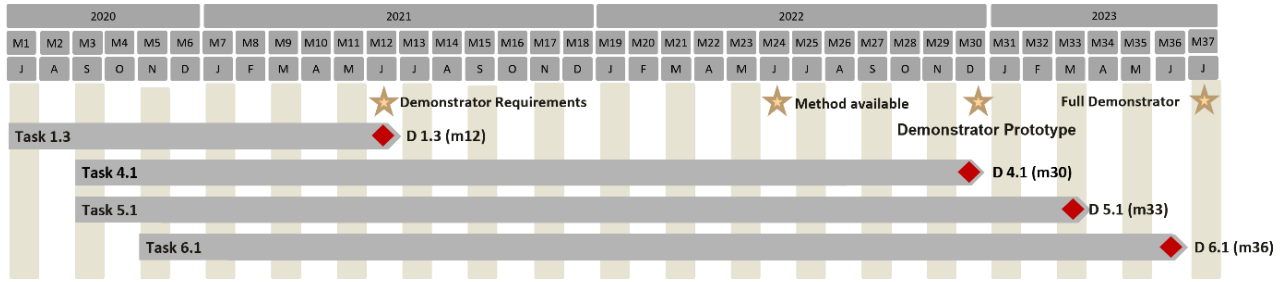


FIGURE 3: SC 3 DEMONSTRATORS TIMELINE

## 6 SSC 3.1 Road condition detection and V2X connectivity (RCD-V2X)

### 6.1 Target goals and achievements

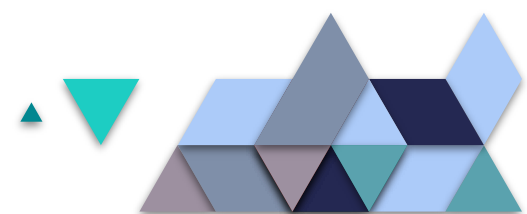
The general idea is that autonomous driving requires a transition from fail-safe, fail-aware to fail-operational and fail-prediction systems addressing predictive safety for dealing with security-safety issues. Safety is related to the environment conditions including road conditions and the capabilities of autonomous vehicles to communicate with other vehicles, infrastructure about these conditions. This demonstrator is aimed to develop methodology for quantification of remaining useful life based on the status of degradation.

As road surface conditions monitoring systems today are not part of automotive sensor suits, the demonstrator will provide the technology and methods beyond state of the art, to assess and mitigate the effects of varying surface conditions. The activities will address the interaction between the perception domain and the connectivity domain. Integration and interaction of the V2X connectivity and the perception for road conditions. Perform tests for the evaluation of residual risk that are aligned with the standard framework and use it as input to the methodology for risk estimations of connectivity systems to support virtual validation of automated and connected vehicles.

The targeted goals and achievements are identifying possible faults (sources of error), and analysis and quantification of the residual risk regarding the interaction between the perception domain and the V2X connectivity domain of automated vehicles. Quantification of uncertainty and residual risk calculation.

### 6.2 Demonstrator structure

This demonstrator focusses on interaction between the perception domain and the connectivity domain. The various aspects and the expected outcomes of the SSC 3.1 demonstrator are summarized in Figure 4.





## SSC 3.1

### Road condition detection and V2X connectivity

What

**What is developed in the demonstrators:**

- Safe and secure interaction between the perception domain and the connectivity domain.
- Trustable low latency V2X connectivity platform including near real-time vehicle embedded sensor monitoring units for road condition detection.
- The demonstrator should be suitable for investigations of residual risks of systems and subsystems used to build the connectivity and sensor functions for automated vehicles.

How

**How the demonstrators are designed and implemented:**

- V2X connectivity platform including gateways and V2D, V2V, V2I and GPS communications.
- AI based data collection through optical sensor with edge computing capabilities.
- Identifying relevance and gaps of standards, and mapping of relevant standards.
- Verification, validation and testing according to functional and non-functional requirements defined (KPIs, measures).

Why

**Why is the demonstrator relevant and why the demonstrators have chosen the approach and the technologies used:**

- Identifying possible sources of error in the interaction between the optical sensors (perception domain) and the V2X communication (connectivity domain) of the automated vehicles and associated infrastructure.
- Assessment and quantification of possible errors according to the relevant standards (e.g., ISO 26262, ISO/PAS 21448-SOTIF, IEC 61508).
- Methodology and methods for identifying security issues in communication protocols.

Results

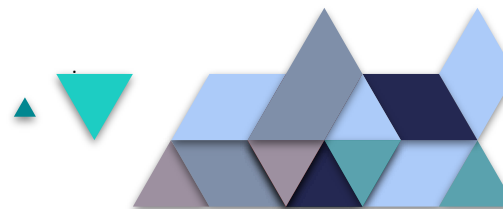
(FRs)

**Demonstrators results:**

- Methodology for risk estimations of connectivity systems.
- Analysis and quantification of the residual risk.
- Dynamic risk management in mission and safety critical systems.

**SC 3**  
 Failure modes, fault detection and residual risk for safety and security in connectivity systems.

FIGURE 4: DEMONSTRATOR SSC 3.1 STRUCTURE



### 6.3 Demonstrator description

The demonstrator collaborated partners are TSENSE, NXT and SINTEF, and their different roles are illustrated in Figure 5. Cooperation on the methodology for risk estimations of connectivity systems considering the planned system integrity and dependability to support virtual validation of automated and connected vehicles. Collaboration to quantify uncertainty and residual risk calculation and to develop a road surface conditions monitoring system. Provide the technology and methods to assess and mitigate the effects of varying surface conditions. Common tests to identify the road condition detection and V2X connectivity and evaluate residual risk. The demonstrator aims to cover different driving, road and weather condition scenarios and uses the idea of Operational Design Domain (ODD) as defined in SAE J3016 for the evaluation. ODD is defined by the SAE J3016 as the "operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics".

For addressing the scenarios for road condition detection, the interfaces with sensors/actuators and the integration with the connectivity domain, the autonomous vehicle system includes categories such as localisation, perception, and planning/control. Localisation handles locating the vehicle within geographic space, perception manages the detection and prediction of static/dynamic objects around the vehicle, roadways/environment conditions, and planning/control supervises the overall vehicle motion and path planning within the roads. In defining the scenarios, the degraded functionality of the autonomous driving system influences the ODD, and the ODD monitoring system should handle the degraded operation by modifying the ODD based on the current system capabilities. Integrated test sets and standards are significant for covering the ODD exploration area and allowing proper safety operational boundary conditions for the autonomous vehicle. The ISO 26262 functional safety (FuSa) and ISO 21448 SOTIF are relevant in this context. FuSa analyses technical failures such as software bugs that be traced back to the triggering signals. SOTIF considers concerns regarding nominal-performance-induced safety hazards, including the inherent limitations of sensor-and learning-based algorithms caused by conditions of the working environment, such as weather, light intensity or type, and transit from the open highway tunnel.

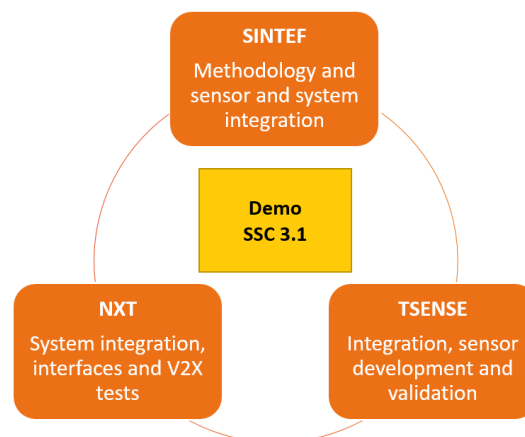
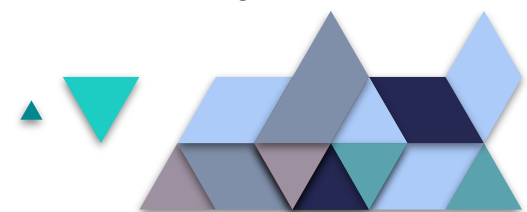
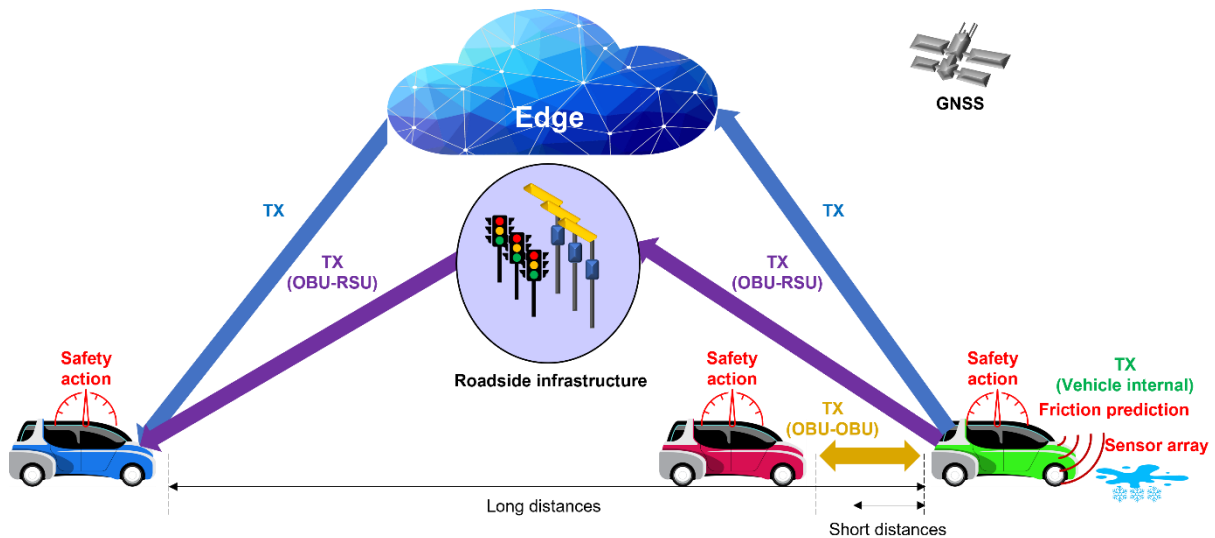


FIGURE 5: SSC 3.1 COOPERATION AND ROLES

As mentioned earlier, the road surface conditions monitoring systems today are not part of automotive sensor suits, the demonstrator will provide the technology and methods to assess and mitigate the effects of varying surface conditions.





**FIGURE 6: DEMONSTRATOR SSC 3.1 OVERVIEW**

The activities will address the interaction between the perception domain and the connectivity domain. These includes integration of the V2X connectivity domain (e.g., Gateway, V2V, V2I, GPS) and the perception domain (e.g., Camera, LiDAR); and performing tests for the evaluation of residual risk that are aligned with the standard framework (e.g., ISO/PAS 21448 [12], IEC 61508 [14]). Use these as input to the methodology for risk estimations of connectivity systems to support virtual validation of automated and connected vehicles.

An overview of the demonstrator and the block schematic are illustrated in Figure 6 and Figure 7 respectively. The demonstrator will provide a V2X connectivity system together with the technology and methods to assess and mitigate the effects of varying road surface conditions. The activities will address the interaction between the perception domain (cameras, sensors, etc.) and the connectivity domain (V2X, etc.), together with the quantification of uncertainty and residual risk calculation.

The perception domain will be established by cameras/sensors for surface condition detection mounted on the lower part of the vehicles, and the connectivity domain will be established by onboard and roadside units (OBUs, RSUs) for V2V and V2I communications together with different Gateways and GPS. The perception domain will include edge computing capabilities for road surface friction prediction. Quantification of uncertainty and residual risk calculation for road surface conditions monitoring and data transmission.

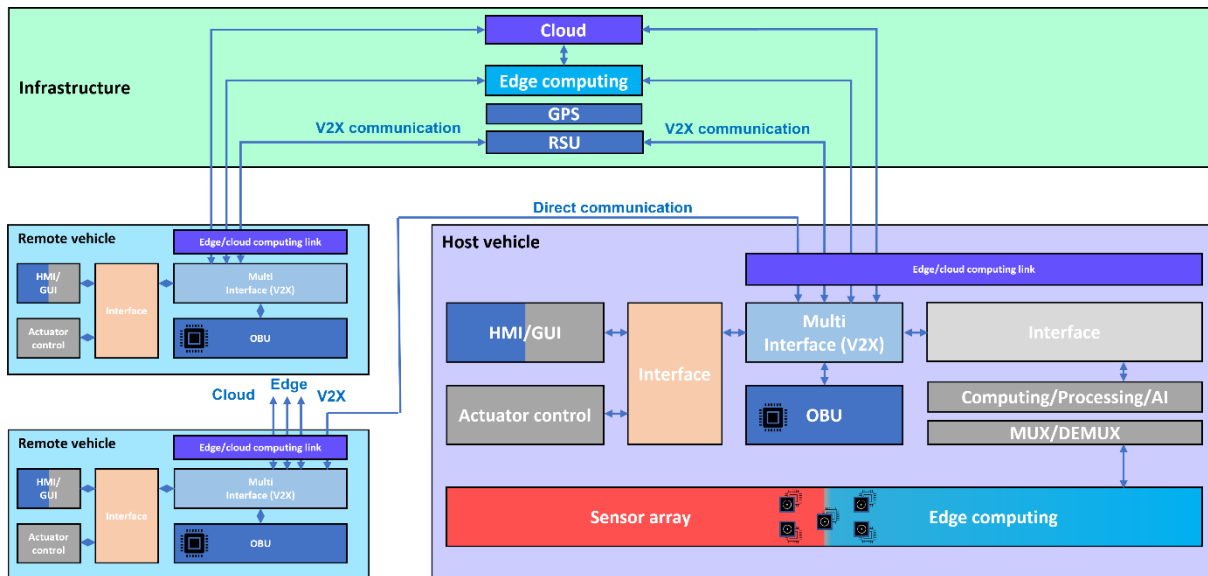


FIGURE 7: SSC 3.1 BLOCK SCHEMATIC OVERVIEW

## 6.4 Treatment on residual risk

Residual risks are the risks that are expected to continue and remains after all the risks have been calculated, accounted, and hedged; and the planned responses of risk has been taken, as well as those that have been deliberately accepted.

$$\text{Residual Risk} = \text{Inherent Risk} - \text{Impact of Risk Controls}$$

Inherent risk is the amount of risk that exists in the absence of controls or other mitigating factors that are not in place. It is also known as the risk before controls or gross risk. The impact of risk controls is the amount of risk eliminated, mitigated, or hedged by taking internal or external risk controls.

Residual risk is a combination of standard ISO26262's [13] probability, severity, and controllability.

Statistics of road traffic accidents related to road conditions and connectivity. Probability of faults detected by road conditions. Historical data to be identified, (not data on CAV (Connected and Automated Vehicles)). Experimental set-up for collecting data for environmental conditions, (vibrations, images, temperature, humidity, road conditions-friction, etc.).

Based on varying degrees of residual risk in different situations, the performance of driving functions can be dynamically controlled by degrading or elevating functionality accordingly to the road/environment conditions, e.g., through adaptation. In defining the scenarios, the degraded functionality of the autonomous driving system influences the ODD, and the ODD monitoring system should handle the degraded operation by modifying the ODD based on the current system capabilities.

Automotive dynamic risk assessment approaches and risk metrics need to be analysed and an evaluation of measurable kinematic quantities to predict the behaviour of other traffic participants based on the road/environment conditions.

A design-time method should be considered for identifying the risk causality to dynamically assess the residual risk considering its situational influences. The residual risk assessment can provide the input to the decision-making component to control the residual risk, such that it is acceptable.

The design-time method should consider the autonomous vehicle environment influencing the residual risk associated with autonomous vehicle behaviours. The residual risk needs to be provided with an associated uncertainty indication passed to a safety decision-making element that concludes the applicable risk control measures that match the situation-specific acceptable risk level best.

## 6.5 Demonstrator relations to the main objectives and key targets

The basic structure of ArchitectECA2030 project comprises five key targets, which are used in eight work packages, to contribute to five main objectives.

### 6.5.1 Objectives

To achieve the goals of ArchitectECA2030, the project focusses on mission-oriented robust electronic components and system (ECS) design, and subsystem and system integration up to sensor fusion. The following overall objectives (O) are addressed in this demonstrator (SSC 3.1):

**O1 - Continuous robust design optimization for each part in the ECS value chain (Technical):** Road condition detection and V2X connectivity will be demonstrated in real surroundings in the Fredrikstad area. That is a robust and secure road surface conditions monitoring system including vehicle sensor arrays, AI/edge computing capabilities, communication internally in the vehicle, to other vehicles at defined distanced, and the road infrastructure. The sensor arrays, computing capabilities, and communication properties are optimised for the applications to be demonstrated.

**O2 - Framework for safety validation of ECS value chain (Technical):** As part of the framework, both functional and non-functional requirements (FR, NFR) are defined, together with key performance indicators (KPIs) for verification and validation the demonstrator components, subsystem, and system.

**O4 - End-user acceptance by trustworthy ECS value chain (Value):** The road surface conditions monitoring system is trustworthy if the residual risk is minimized and end-users can rely on system and its safety functions (information, warnings, and actions). Through this sub-supply chain, we want to demonstrate the ability to perform specified functions while following a set of stated design principles for optimization and acting in the best interests of the end-users.

**O5 - Zero emissions, crashes, and congestions by ECA2030 vehicle (Value):** A monitoring system that provides real-time information on the road conditions in which the vehicle is located at all times is of great value in terms of avoiding accidents and reduce congestions.

The following supply chain specific objectives are addressed in this demonstrator (SSC 3.1):

**SC3-O1 - Investigate the residual risks of subsystems, and systems. Analysis, assessment and quantification of fault modes and their consequences on communication systems:** Investigate the residual risk for the road condition monitoring.

**SC3-O3 - Verification methodologies specifically adapted to ensure safety requirements:** Develop a method to road conditions to identify possible safety issues timely. Road condition detection and V2X connectivity will be demonstrated in real surroundings in the Fredrikstad area. That is a robust and secure road surface conditions monitoring system including vehicle sensor arrays, AI/edge computing capabilities, communication internally in the vehicle, to other vehicles at defined distanced, and the road infrastructure.

**SC3-04 - Apply the planned system integrity and dependability measures into account (security, safety, reliability, resilience, maintainability, and availability) to create the basis for the homologation and validation of the connectivity functions for automated and connected vehicles as mission- and safety-critical systems:** Focus on safety, reliability, and maintainability.

**SC3-05 - Development of a demonstrator showing applicability of the proposed methods:** A demonstrator in which the method is implemented with TRL 4 will be provided at the end of the project.

## 6.5.2 Key targets

Each key target is a generic element that represents a common characteristic of different processes, collaborations, methods, etc. that is necessary for a successful implementation of demonstrator. The following key targets (KT) are addressed in this demonstrator (SSC 3.1):

**KT1 - Architectures, components, sub-systems enabling virtual development and validation (monitoring device, failure risk):**

This demonstrator is addressing connectivity and sensor fusion architecture in the perception domain, with focus on road condition detection/prediction, which among others are influenced by the weather conditions, oil spillage, pothole, etc. This includes incorporating new scenarios in development and testing, and recommendation what kind of data from the test fields is required to quantify the residual risk.

**KT4 - Definition and understanding of test coverage (residual risk, design feedback, lifetime monitoring, aggregated risk):** This demonstrator is addressing connectivity, perception, and algorithm requirements (also including redundancy requirements) to further increase the availability of systems/subsystems and to reduce the probability of malfunctions behaviours below acceptable limits during the expected lifetime. The demonstrator will be tested under real road conditions and in real traffic situations as possible.

## 6.6 Homologation framework mapping

Homologation of autonomous and connected vehicles refers to the certification process of a ECAS vehicle granting that it complies with all local standards and legal regulations such as safety and environmental regulation. Three main elements considered in the homologation process are:

- Technology
- Regulation for connected autonomous vehicles
- Standardisation for connected autonomous vehicles

The demonstrator presented in SSC 3.1 addresses the technology components and analyses the existing standards that support the homologation while identifying the gaps in the elements missing in the current standards to address the residual risk and provide support for the future homologation framework for autonomous and connected vehicles.

Simulating traffic situations is a critical element of homologating autonomous vehicles due to the number of traffic situations and scenarios that need to be validated and tested. The time and costs to perform conventional on-road tests to evaluate the critical scenarios for autonomous vehicles are not anymore achievable. Virtual procedures need to augment existing validation and testing methods for

autonomous vehicles digital homologation by performing simulation testing at an extended scale using new computing capabilities.

Simulation for virtual validation and approval of autonomous vehicles needs to be complemented by physical testing as only testing is limited and not scalable. The next-generation autonomous vehicles solutions for certification require to validate and establish the simulation as a tool to develop standards and support digital homologation. In this context, all the specifications for digital homologation need to comply with using digital testing equipment and virtual platforms.

## 6.7 Non-functional requirements, KPIs, and measures

Three non-functional requirements (NFRs) are defined that match well the requirements addressing the trustable architectures with acceptable residual risk, regarding the SSC 3.1 and its demonstrator. The definitions of the NFRs are aligned with the definitions in the ISO/IEC 25010 standard [2]. One KPI and one measure are defined for each NFR. In Table 2, Table 3, and Table 4 we present three relevant NFRs, KPIs and Measures for the demonstrator.

**TABLE 2: NFRs, KPIs AND MEASURES FOR SSC 3.1 - RELIABILITY (MATURITY)**

NFR	Reliability (Maturity)
NFR definition	<p><b>Reliability</b> is the degree to which a system, product or component performs specified functions under specified conditions for a specified period (ISO/IEC 25010). The relevant sub-characteristic is <b>maturity</b>. That is the degree to which a system, product or component meets needs for reliability under normal operation.</p> <p><b>Reliability</b> is the capability of the road condition sensor to maintain its level of performance under the road and environmental conditions stated (e.g., dry, water, snow, ice, chemicals, and organic materials). For the stated period for operating the vehicle during driving mission. <b>Maturity</b> of the road condition sensors is the capability to avoid failures, as the results of faults in HW and SW algorithms, and to reduce the frequencies of these possible failures. Maturity reflects the degree of reduction in frequencies of failures (compared to the non-mature version in beginning of the project).</p>
KPI name	Tyre/road friction prediction precision increase.
Description	Comparing the tyre/road friction prediction parameters in the beginning and the end of the project.
Measure	Friction parameters.
Type of measure	Quantitative [#]
Method of collection and measurement	Data logging and database historian through demonstrator evaluation (Road condition detection and V2X connectivity).
Demonstrator target	≥ 10% of improvements of the friction parameter measurement accuracy for different road conditions.
KPI for verification and validation	Road friction parameters comparison.

**TABLE 3: NFRs, KPIs AND MEASURES FOR SSC 3.1 - COMPATIBILITY (INTEROPERABILITY)**

NFR	Usability (Operability)
NFR definition	<p><b>Usability</b> is the degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use (ISO/IEC 25010). The relevant sub-characteristic is</p>

	<p><b>operability.</b> That is the degree to which a product or system has attributes that make it easy to operate and control.</p> <p><b>Usability</b> is the capability of the road condition monitoring system to be used to achieve the specified performance and goals, under specified road and environment conditions. <b>Operability</b> is the capability of road conditions system to be easily operated and controlled with respect to the attributes for road condition detection under different road and environment conditions.</p>																											
KPI name	Information rate versus vehicle speed.																											
Description	Frequency of updated information relatively to vehicle speed																											
Measure	Measuring the speed between friction information updates and calculate the travelled distance.																											
Type of measure	Quantitative [m].																											
Method of collection and measurement	Data logging of information rate, friction information, and vehicle speed.																											
Demonstrator target	<p>The sensor provides 1 Hz starting from 5 km/h and increases the sampling rate until the maximum of 8 Hz to speeds starting from 70 km/h as presented in the table below.</p> <table border="1" data-bbox="694 862 1204 1299"> <thead> <tr> <th>Speed [km/h]</th> <th>Sample rate [Hz]</th> <th>Distance (between two readings) [m]</th> </tr> </thead> <tbody> <tr> <td>0 - 5</td> <td>1</td> <td>1.4</td> </tr> <tr> <td>6 - 10</td> <td>2</td> <td>1.4</td> </tr> <tr> <td>11 - 15</td> <td>3</td> <td>1.4</td> </tr> <tr> <td>16 - 20</td> <td>4</td> <td>1.4</td> </tr> <tr> <td>21 - 25</td> <td>5</td> <td>1.4</td> </tr> <tr> <td>26 - 30</td> <td>6</td> <td>1.4</td> </tr> <tr> <td>31 - 35</td> <td>7</td> <td>1.4</td> </tr> <tr> <td>36 - 70</td> <td>8</td> <td>2.0</td> </tr> </tbody> </table>	Speed [km/h]	Sample rate [Hz]	Distance (between two readings) [m]	0 - 5	1	1.4	6 - 10	2	1.4	11 - 15	3	1.4	16 - 20	4	1.4	21 - 25	5	1.4	26 - 30	6	1.4	31 - 35	7	1.4	36 - 70	8	2.0
Speed [km/h]	Sample rate [Hz]	Distance (between two readings) [m]																										
0 - 5	1	1.4																										
6 - 10	2	1.4																										
11 - 15	3	1.4																										
16 - 20	4	1.4																										
21 - 25	5	1.4																										
26 - 30	6	1.4																										
31 - 35	7	1.4																										
36 - 70	8	2.0																										
KPI for verification and validation	Frequency of information related to road condition, friction, and vehicle speed.																											

**TABLE 4: NFRs, KPIS AND MEASURES FOR SSC 3.1 - MAINTAINABILITY (TESTABILITY)**

NFR	Maintainability (Testability)
NFR definition	<p><b>Maintainability</b> is the degree of effectiveness and efficiency with which a product or system can be modified to improve it, correct it, or adapt it to changes in environment, and in requirements (ISO/IEC 25010). The relevant sub-characteristic is <b>testability</b>. That is the degree of effectiveness and efficiency with which test criteria can be established for a system, product or component and tests can be performed to determine whether those criteria have been met.</p> <p><b>Maintainability</b> is the capability of road condition system to be modified including corrections, improvements, adaptations to changes in the environment and the requirements and functional spec. <b>Testability</b> is the capability of the road condition system to be validated and how effective the test criteria is, and what test can be performed to demo that the test criteria are met.</p>
KPI name	Testability dataset.
Description	There is a dataset of signals prepared to emulate the information received by the sensor and processed by the algorithm to evaluate the road condition.
Measure	Dataset available for each road condition.

Type of measure	Quantitative [#].
Method of collection and measurement	Data recording along tests executed in real roads.
Demonstrator target	One dataset for each road condition.
KPI for verification and validation	<b>Dataset to 3 road conditions.</b> <b>Defect ratio in each testing phase.</b> Unit test - 80% Test of each sensor and system individually.

## 6.8 Functional requirements, KPIs, and measures

Three functional requirements (FRs) are defined that match well the requirements addressing implementation of the SSC 3.1 demonstrator. The definitions are based on the demonstrator system design implemented and aligned with the elements described for trustable architectures with acceptable residual risk. One KPI and one measure are defined for each FR, that will be used for supervising the development and the demonstrator results. In Table 5, Table 6, and Table 7 we present three relevant FRs, KPIs and Measures for the demonstrator.

**TABLE 5: FRs, KPIs AND MEASURES FOR SSC 3.1 - MONITORING DETECTION**

FR	Monitoring detection
FR definition	The ability to detect and recognize different road surface conditions in "real-time".
KPI name	Road surface pattern recognition.
Description	Road surface monitoring and distinguish between different types of road surfaces (e.g., dry, water, snow, ice, chemicals, and organic materials).
Measure	Number of road surfaces recognized within a defined accuracy.
Type of measure	Quantitative [# and %].
Method of collection and measurement	Demonstrator evaluation: Road condition detection and V2X connectivity. Tests with vehicle, sensor/ camera, V2X communication and different defined road surfaces. The vehicle is moving towards and over the road surfaces.
Demonstrator target	Distinguish between three types of road surfaces, (accuracy $\geq 70\%$ for each type of road surface).
KPI for Verification and validation	Verification of 3 different types of road surfaces carried out 10 times each.

**TABLE 6: FRs, KPIs AND MEASURES FOR SSC 3.1 - PREDICTION ALGORITHMS**

FR	Prediction algorithms
FR definition	The ability to predict road friction (tyre/road) for different road surface conditions in "real-time".
KPI name	Road friction prediction.
Description	The algorithms shall predict the road friction for a specific road surface.
Measure	Friction coefficient.
Type of measure	Quantitative [%].
Method of collection and measurement	The vehicle will drive over an area having the road condition sensor making the

	measurement simultaneously with friction mapped by a reference friction sensor system used currently in the market. The reference sensor will be installed in the same car to read the same road condition simultaneously with the TracSense Friction Sensor. The comparison between the two measurements will be done to guarantee the accuracy.
Demonstrator target	Deviation between real braking distance and predicted/ calculated braking distance should be less than 30%.
KPI for Verification and validation	AI model accuracy $\geq 70\%$ .

**TABLE 7: FRs, KPIs AND MEASURES FOR SSC 3.1 - WIRELESS CONNECTIVITY**

FR	Wireless connectivity
FR definition	The ability to securely transmit data between the relevant "components/ actors" (in-vehicle, V2V, V2I) with low latency on the required communication protocols.
KPI name	Communication redundancy.
Description	Different wireless communication channels supported by the system for the intended type of information/functionality.
Measure	Number of communication channels.
Type of measure	Quantitative [#].
Method of collection and measurement	The data collection and measurements will be carried out as part of the demonstrator evaluation: Road condition detection and V2X connectivity. Tests with sensors/vehicles/infrastructure communications.
Demonstrator target	Two different communication channels for redundancy of information (e.g., V2X and Cellular), and that the functionality is maintained even if one of the channels fails.
KPI for Verification and validation	Validation of two different independent wireless channels,

## 6.9 Mapping to existing standards

Several standards have been identified to be relevant for this demonstrator. The standards address topics covering the road vehicles safety of the intended functionality safety, functional safety, wireless communication for information exchange between systems local and metropolitan area networks, safety/cybersecurity for automated driving systems and evaluation of autonomous products. The mapping these standards to the structure of ArchitectECA2030 covered by SSC 3.1 is illustrated in the form of a V-model in Figure 8.

The SSC 3.1 activities plan to evaluate a model-based approach to safety to enhance the existing functional safety and ASIL (ISO 26262) requirements in the automotive that can cope with multi-agent environments. Using the Responsibility-Sensitive Safety (RSS) [5] applied to autonomous vehicles as a rigorous mathematical model and formalizing an interpretation of the law can give a different perspective to safety measures. The "Safety First for Automated Driving (SaFAD) paper [20] has been adopted by ISO as a technical report and is considered the first step towards standardization to include the RSS in the Drive Planning Element.

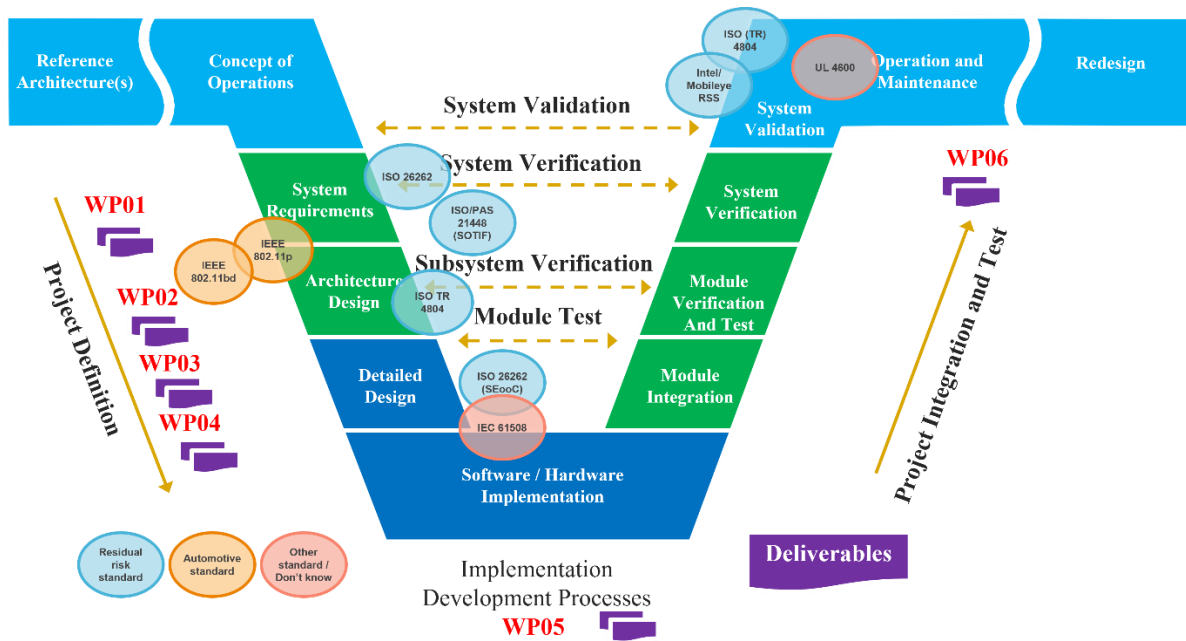


FIGURE 8: STANDARDS MAPPING V-MODEL ARCHITECTECA2030 RELEVANT FOR SC3

The short description of the standards and their relevance is summarized in Table 8.

TABLE 8: MAPPING OF EXISTING STANDARDS FOR SSC 3.1

Standard code	Standard title	Why relevant	How to use
ISO/PAS 21448 (2019)	Road vehicles - Safety of the intended functionality (SOTIF) [12].	Facilitates the residual risk framework integration for connectivity systems connected with perception devices. This document provides guidance on the applicable design, verification and validation measures needed to achieve the safety of the intended functionality. 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).	Determine residual risk related to different demonstrator functionalities associated with the integration of connectivity systems and perception devices. ISO 21448 does not include unsafe interactions between system components.
ISO 26262 (2018)	Road vehicles - Functional safety [13].	Address safety-related systems that include one or more E/E systems and that are installed in series production passenger cars (with a maximum gross vehicle mass up to 3 500 kg). The Automotive Safety Integrity Level (ASIL) is a key component for ISO 26262 compliance. Each safety requirement is assigned an ASIL of A, B, C, or D, (where D is the most safety critical processes/	Map demonstrator safety related requirements (functionalities, performances, features) according to the ASIL requirements.

		<p>strictest testing regulations). The ASIL is focusing on the harm to the driver and other road users and is not addressing the technologies used in the system.</p> <p>Note that 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.</p>	
IEC 61508 (2010)	Functional safety of electrical/electronic/programmable electronic safety-related systems [14].	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).	To be used in conjunction with IEC 26262 and ISO/PAS 21448
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).	Amendment 6 specifies the extensions to IEEE 802.11 standard for wireless local area networks (WLANs) providing wireless communications while in a vehicular environment.	V2X communication related to the connectivity domain.
IEEE 802.11bd (2018)	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 [15].	This amendment provides enhancements for the next generation V2X.	V2X communication related to the connectivity domain.
ISO/TR 4804: 2020	Road vehicles - Safety and cybersecurity for automated driving systems - Design, verification, and validation	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. Provides an overview and guidance of the generic steps for developing and validating a safe and secure automated driving system with the goal of achieving a positive risk balance and the	Use the framework for a harmonised safety design by applying the safety principles systematically and break them into safety by design capabilities, elements, and architectures.

		avoidance of unreasonable risk. This standard describes a framework for a harmonized safety design by systematically breaking down safety principles into safety by design capabilities, elements, and architectures. Gives guidance to system developers with a dedicated safety lifecycle for Deep Neural Networks (DNNs) used for automated driving systems. It considers safety by design, verification and validation methods for automated driving focused on SAE level 3 and level 4 automation features of automated vehicles. In addition, it outlines cybersecurity considerations in conjunction with safety aspects.	
ANSI/UL 4600 (2020)	Standard for Evaluation of Autonomous Products	Address 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).	Evaluate the framework of UL 4600 to build structured arguments that autonomous vehicles are sufficiently safe. Investigate how to use UL 4600 to validate the safety of artificial intelligence (AI) components.

## 6.10 Verification and validation

Verification and validation of the SSC3.2 demonstrator includes experimental validation of the sensor and module for road conditions monitoring.

In addition, the FRs and NFRs defined for the demonstrator will be validated based on specific KPIs described for each requirement.

The verification and validation should check if a hazard and risk analysis for the automated system is conducted.

The integration in the overall vehicle design and the mobility ecosystem must be considered together with good design and redundancy to address the identified risk and hazards.

The design must be checked that leads to an acceptable residual risk for the ODD concerns.

The demonstrator will make use of procedures for merging the real-time simulation of driving environments with real tests on complete vehicle or on one or several subsystems in parallel to reduce testing time and costs and analyse complex interactions in complete sets of tests.

## 6.11 Demonstrator milestones

Table 9 shows the main milestones to fulfil the demonstrator in SSC 3.1, and can be seen in connection with the SC3 timeline in **Error! Reference source not found.**

TABLE 9: SSC 3.1 DEMONSTRATOR MILESTONES

Due date	Description
M12	Requirements available.
M24	Method to assess road conditions related failure mechanisms proposed.
M30	Final experimental hardware for the demonstrator build.
M36	Concept is validated for the use case using dedicated experiments aligned with TRL 4.

## 7 SSC 3.2 Digital twin package monitoring (DigiPack)

Electronic packages are exposed to varying environmental conditions such as elevated temperature, moisture diffusion, mechanical vibrations, etc. during their operation-lifetime.

This results in mechanical, thermal, chemical, and electrical degradation of its constituent materials, which can lead to package-level and board-level failures. The demonstrator is aimed at developing a methodology for quantification of remaining useful life based on the status of degradation.

### 7.1 Target goals and achievements

The aim of this research is to develop data-driven, and physics-of-degradation based models combined with the Digital Twin technology for lifetime monitoring and design for reliability.

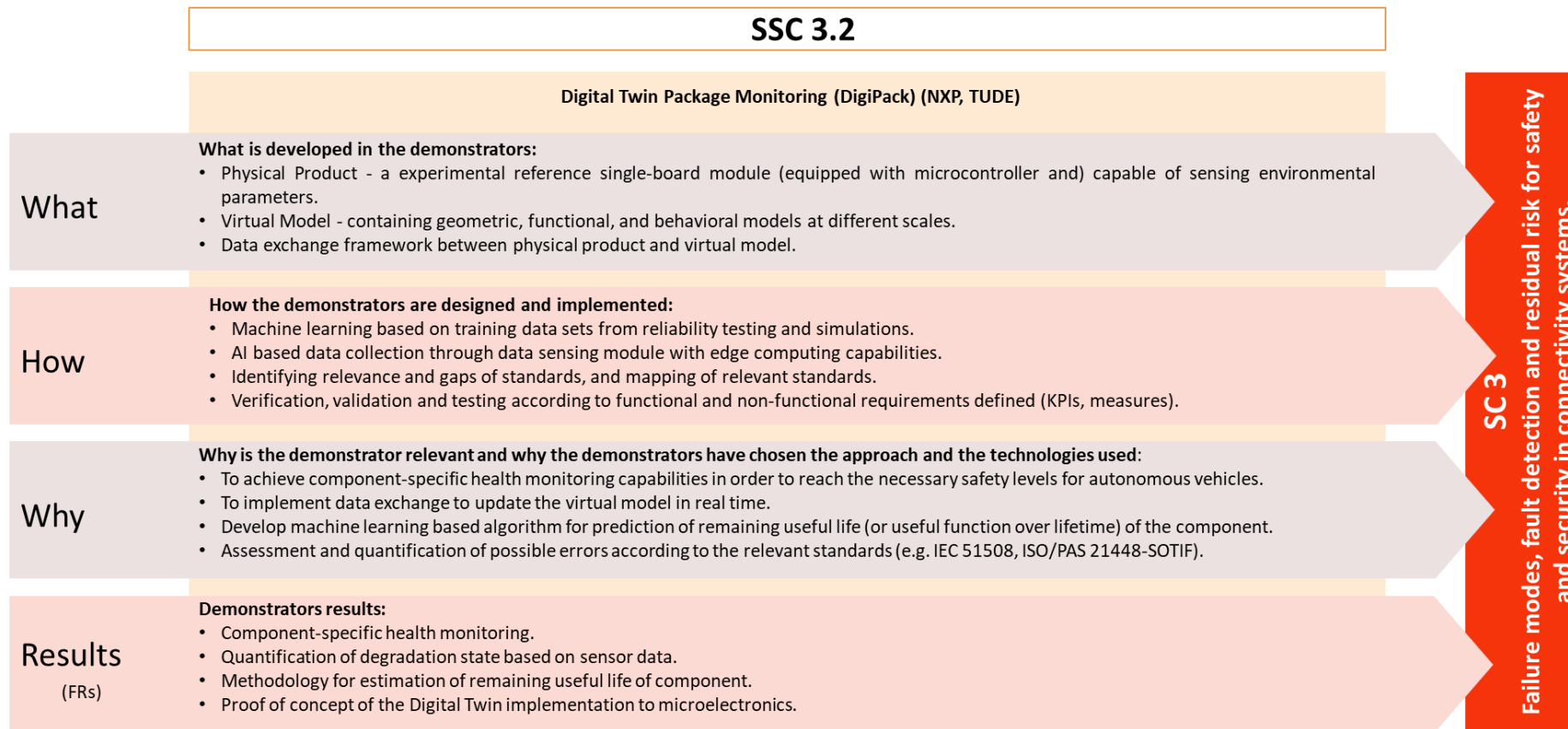
Based on this, following goals and achievements have been planned for the demonstrator:

- Develop a working test-component (a programmable microcontroller with sensors for monitoring exposure to ambient conditions, i.e., causes of degradation).
- Prepare models for relevant degradation (ageing) mechanisms.
- Develop a digital twin of the test component – which includes connections (data exchange framework) between physical product and virtual product to update it with current status of degradation.
- Develop virtual sensors using digital twin-based simulations to extract more data (data mining).
- Prepare machine learning based models for translating (real and virtual) sensor data into predicting the remaining useful life of the test-component.

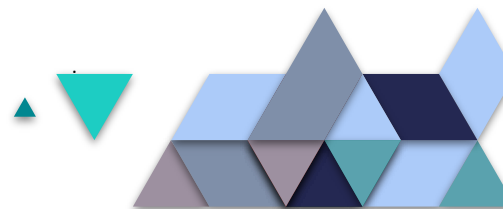
## 7.2 Demonstrator structure

This demonstrator focuses on creating a working proof of concept of the Digital Twin, which has a structure with 3 key parts – physical product (hardware), virtual model (software), and data (exchange and analytics).

Various aspects of the demonstrator and the expected outcomes have been summarized in Figure 9.



**FIGURE 9: DEMONSTRATOR SSC 3.2 STRUCTURE**



### 7.3 Demonstrator description

The Digital Twin demonstrator will be developed by collaboration of NXP and TUDE. A five-dimensional structure of Digital Twin is indicated in Figure 10.

The first step involves designing and fabricating the physical product, i.e., the data-sensing module, with various sensors to gather data of the environmental variables such as temperature, humidity, and mechanical vibrations.

Standard accelerated stress-tests for reliability will be carried out on the data-sensing module to monitor various degradation mechanisms and failure modes related to packaging (e.g., delamination, bond wire cracks, and solder joint failure).

Virtual model of the module will be developed followed by its experimental validation. Within the concept of the digital twin a data exchange framework between the virtual model (e.g., finite element model, response surface model, or analytical model) and the physical product is to be established.

Data-driven (machine learning) and physics-of-degradation based algorithms for lifetime prediction will be developed.

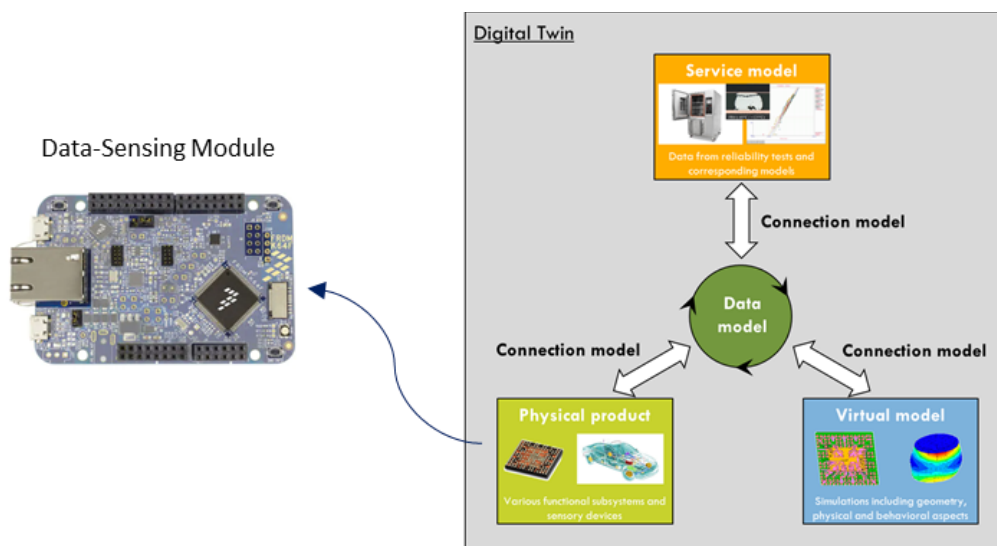
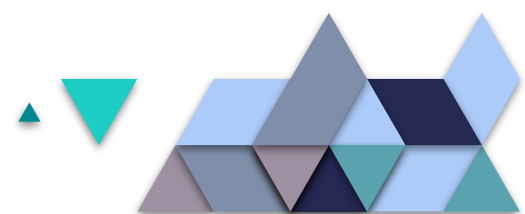


FIGURE 10 DEMONSTRATOR SSC 3.2 OVERVIEW

### 7.4 Treatment on residual risk

A technology or a demonstrator has several inherent risks associated with it. Some of them are controllable. Residual risks can be explained as the risks remaining out of all inherent risks after consideration of various measures to overcome the controllable risks. Following bullet-points summarize their relationship and definitions.

- **Residual Risk = Inherent Risk – Impact of Risk Controls**
- **Inherent risk** is the amount of risk that exists in the absence of controls or other mitigating factors that are not in place. It is also known as the risk before controls or gross risk.



- **The impact of risk controls** is the amount of risk eliminated, mitigated, or hedged by taking internal or external risk controls.

The demonstrator SSC3.2 DigiPack aims to implement Digital Twin, which has 3 key components – physical product (hardware), virtual model (software), and data. Thus, the identified residual risks related to the demonstrator functions are also categorized into these 3 types, e.g., sensor failure, errors in virtual model, and loss of connectivity to the cloud, respectively.

In addition, this demonstrator is aimed at Digital Twin based monitoring of component degradation and prediction of remaining useful life (RUL). Thus, this aspect addresses residual risks in the following way:

- DigiPack will provide a risk control for mitigating the risks imposed by the degradation of microelectronics packages.
- Condition monitoring can be understood as risk control or risk avoidance strategy.
- RUL prediction can reduce residual risk by initiating a maintenance before the actual risk happens.

## 7.5 Demonstrator relations to the main objectives and key targets

The demonstrator SSC 3.2 DigiPack will mainly contribute to the following objectives and key targets of ArchitectECA2030.

### 7.5.1 Objectives

#### **O3 - Identification and management of residual risks over the entire ECS value chain (Technical):**

This objective relates to secure connected and automated vehicles by ensuring their reliability and functional safety. The outcome of the objective is an accepted monitoring device methodology. DigiPack will contribute to this objective by developing a Digital Twin to monitor failure mechanism that are related to microelectronic packages. The Digital Twin is based on edge computing and will be able to connect to the higher-level architecture of the vehicle.

#### **O5 - Zero emissions, crashes, and congestions by ECA2030 vehicle (Value):**

The main outcome of this objective is to increase the sustainability of automated vehicles by reducing emission, crashes, and congestions. DigiPack will contribute to this objective by actively monitoring the state of the system and predicting possible malfunction in a timely manner. This will not only significantly reduce the risk of crashes due to a malfunction, but also reduces congestions because of defective cars on the road.

#### **SC3-O3 - Verification methodologies specifically adapted to ensure safety requirements:**

DigiPack will develop a method to detect degradation of the microelectronic packages to identify possible failure timely.

#### **SC3-O5 - Development of a demonstrator showing applicability of the proposed methods:**

A demonstrator in which the method is implemented with TRL 4-5 will be provided at the end of the project.

## 7.5.2 Key targets

### **KT1 - Architectures, components, sub-systems enabling virtual development and validation (monitoring device, failure risk):**

With DigiPack we will develop a method to actively monitor safety and mission-critical components for (autonomous) vehicles to reduce the probability of malfunctioning of such vehicles below an accepted limit (KT1.2).

### **KT2 - Methods and tools to validate the models used in virtual validation (lifetime monitoring, residual risk, methods, and tools):**

With DigiPack we can record the data of built-in sensor within electronic systems, such as ECUs, process this data (edge computing), and send it to the cloud for further processing (KT2.9, KT2.12). This will assist the development of a database of test data related to automated and autonomous driving (KT2.1).

## 7.6 Homologation framework mapping

Quality is a key aspect in customer-supplier relations. Therefore, an increased test coverage at various levels of the supply chain (e.g., new test options for mechanical properties and enhanced test models for longer lifetime of systems) will strengthen the competitive advantage of the European ECS industry. Reliable electronic components and systems are essential for a fast ramp up of new products. High volumes are produced in very short time periods and the lifecycles of products are getting even shorter. Consequently, any issues emerged from non-reliable electronics create serious business problems for OEMs in different domains and must be avoided.

Reliability prediction today is mostly based on specific tests that are documented within specification manuals. These tests are performed intensively during product qualification and on sample basis during the life cycle of the product.

New IoT options, combined with edge and/or cloud computing possibilities can run real time analysis when reliability specific parameters are measured and recorded at system level.

Such system-level prognostics helps avoid failures by detecting them beforehand, and thus reducing the residual risk, which is a key consideration of the homologation framework.

This demonstrator aims to address component-specific health monitoring using Digital Twin technology. It involves continuous evaluation of the component degradation state and prediction of remaining useful life based on data-driven algorithms, which directly contributes to reduction of residual risk of component failure.

We plan to utilize existing international standards indicated in Table 18 and identify gaps in the context of Digital Twin – structure, implementation, and associated residual risks. For example, we have identified that the international standard for Digital Twin (IPC 2551) [18] describes the structure well but lacks information about its implementation as well as about safety and residual risks.

## 7.7 Non-functional requirements, KPIs, and measures

Non-functional requirements are the specifications that describes a system's operation capabilities and constraints that enhance its functionality.

In Table 10, Table 11, Table 12, and Table 13 we present the four most relevant NFRs, KPIs and Measures for SSC 3.2. Selected NFRs – main characteristics and sub-characteristics – are as per their definition in ISO/IEC 25010.

**TABLE 10: NFRs, KPIs AND MEASURES FOR SSC 3.2 - COMPATIBILITY (INTEROPERABILITY)**

<b>NFR</b>	<b>Compatibility (Interoperability)</b>
NFR definition	<p><u>Definition as per ISO/IEC 25010:</u> Degree to which a product, system or component can exchange information with other products, systems, or components, and/or perform its required functions, while sharing the same hardware or software environment</p> <p><u>Demonstrator-specific definition:</u> Degree to which the Digital Twin implementation can be extended for different hardware, here, families of electronic packages.</p>
KPI name	Extent of methodology transfer
Description	How compatible is the methodology (of D.T.) for other package families?
Measure	Number of supported package families
Type of measure	Quantitative [number]
Method of collection and measurement	Determine the number of families the Digital Twin is implemented for.
Demonstrator target	2 families
KPI for Verification and validation	Number of package families monitored by the demonstrator

**TABLE 11: NFRs, KPIs AND MEASURES FOR SSC 3.2 - FUNCTIONAL STABILITY (FUNCTIONAL CORRECTNESS)**

<b>NFR</b>	<b>Functional Stability (Functional Correctness)</b>
NFR definition	<p><u>Definition as per ISO/IEC 25010:</u> Degree to which a product or system provides functions that meet stated and implied needs when used under specified conditions.</p> <p><u>Demonstrator-specific definition:</u> Degree to which the Digital Twin retains its functionality and accuracy over the course of component degradation.</p>
KPI name	Functional correctness
Description	How stable and sustained does the functionality of the package and D.T. remains
Measure	Sustainability of function (computation performance)
Type of measure	Quantitative [percentage]
Method of collection and measurement	Accuracy comparison of aged (accelerated tests) components
Demonstrator target	<10% loss of accuracy in 10 years
KPI for Verification and validation	Ratio of predicted life and actual lifetime (accelerated stress test)

**TABLE 12: NFRs, KPIs AND MEASURES FOR SSC 3.2 - PERFORMANCE EFFICIENCY (RESOURCE UTILIZATION)**

<b>NFR</b>	<b>Performance Efficiency (Resource Utilization)</b>
NFR definition	<u>Definition as per ISO/IEC 25010:</u> Performance relative to the amount of resources used under stated conditions

	<b>Demonstrator-specific definition:</b> The share of resources consumed by the Digital Twin functionality, i.e., data acquisition, data analysis, and prediction algorithms.
KPI name	Utilization of processor and memory
Description	How computationally compact can D.T. be.
Measure	Ratio of power
Type of measure	Quantitative [percentage]
Method of collection and measurement	Measure the power consumption of processor
Demonstrator target	<1% of processor resources
KPI for Verification and validation	Ratio of power consumption of processor w&w/o Digital Twin

**TABLE 13 NFRS, KPIS AND MEASURES FOR SSC 3.2 - RELIABILITY (MATURITY)**

<b>NFR</b>	<b>Reliability (Maturity) [of Digital Twin model]</b>
NFR definition	<u>Definition as per ISO/IEC 25010:</u> Degree to which inherent problems and faults of a technology have been removed or reduced. <u>Demonstrator-specific definition:</u> Degree to which the Digital Twin implementation is technologically mature and reliable for lifetime prediction
KPI name	Technology readiness level
Description	An indicator to measure the maturity of technologies during the acquisition phase of a program
Measure	TRL indicator (range: 1–9)
Type of measure	Qualitative
Method of collection and measurement	Comparison of lab results with industrially relevant environmental results
Demonstrator target	4 or 5
KPI for Verification and validation	TRL defined as per ISO 16290 standard

## 7.8 Functional requirements, KPIs, and measures

Functional requirements are the key features of the demonstrator. In Table 14, Table 15, Table 16, and Table 17 we present the four most relevant FRs, KPIs and Measures for SSC 3.2.

**TABLE 14: FRs, KPIS AND MEASURES FOR SSC 3.2 - MONITORING ENVIRONMENTAL PARAMETERS**

<b>FR</b>	<b>Monitoring environmental parameters</b>
FR definition	Data collection of the exposure to ambient conditions through sensors
KPI name	Extent of data acquisition
Description	Which parameters (variables) are being measured
Measure	Number of measured parameters
Type of measure	Quantitative [number]
Method of collection and measurement	Types of sensors used
Demonstrator target	4 (temp., humidity, vibrations, stresses)

KPI for Verification and validation	Minimum number of types of sensors for sufficiently accurate health monitoring
-------------------------------------	--

**TABLE 15: FRs, KPIs AND MEASURES FOR SSC 3.2 - ALGORITHM FOR LIFETIME PREDICTION**

FR	Algorithm for lifetime prediction
FR definition	Quantification (prediction) of remaining useful life of the component
KPI name	Accuracy of RUL prediction
Description	How accurate can the RUL be predicted
Measure	Tolerance in time units (number of days/months)
Type of measure	Quantitative [time]
Method of collection and measurement	Performing accelerated lifetime tests
Demonstrator target	±30 days
KPI for Verification and validation	Difference between actual and predicted lifetime at accelerated stress test conditions

**TABLE 16: FRs, KPIs AND MEASURES FOR SSC 3.2 - EVALUATION OF DEGRADATION STATE**

FR	Evaluation of degradation state
FR definition	Evaluation of current state of degradation based on degradation models and history of sensed data
KPI name	Spectrum of degradation (ageing) mechanisms
Description	What degradation mechanism are being considered/analysed
Measure	Number of ageing mechanisms
Type of measure	Quantitative [number]
Method of collection and measurement	Independent accelerated stress tests for each aging mechanism
Demonstrator target	3
KPI for Verification and validation	Number of ageing conditions at which device monitors health accurately

**TABLE 17 : FRs, KPIs AND MEASURES FOR SSC 3.2 - FAILURE (TYPE) PREDICTION**

FR	Failure (type) prediction
FR definition	Machine learning based prediction of failure mode
KPI name	Scope of prediction of failure modes
Description	Which failure modes are being considered
Measure	Number of failure modes
Type of measure	Quantitative [number]
Method of collection and measurement	Perform failure analysis after accelerated stress testing to confirm failure modes
Demonstrator target	2
KPI for Verification and validation	Number of failure modes observed after accelerated stress testing

## 7.9 Mapping to existing standards

Five standards have been selected for this demonstrator, and their relevance is summarized in Table 18. First 2 standards are for the structure of Digital Twin and for the data exchange framework among various aspects of Digital Twin, respectively. Following 2 standards are related to safety, security and quantification of residual risks. Last one is for determining various accelerated stress test conditions for the failure mechanisms associated with this demonstrator. The mapping these standards to the structure of ArchitectECA2030 is indicated in the form of a V-model in Figure 11.

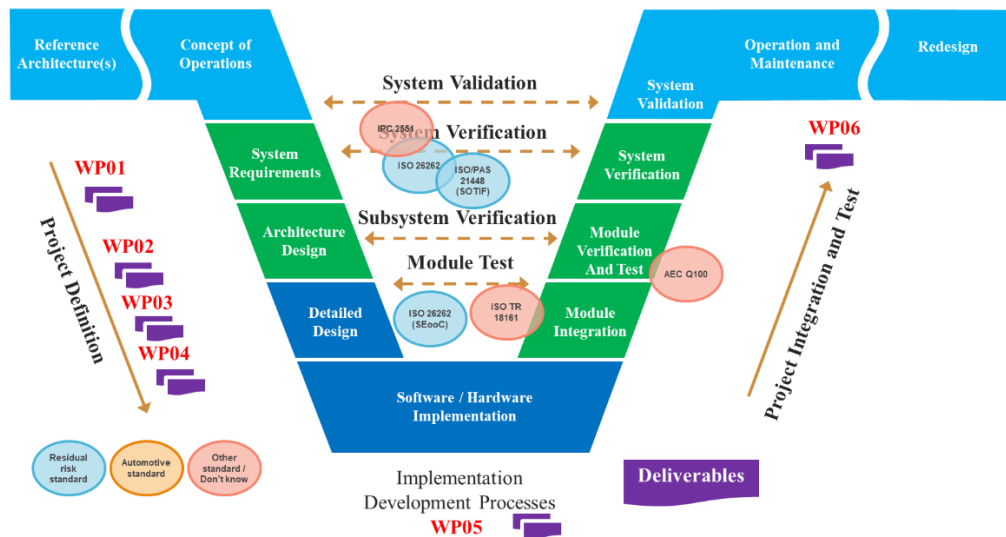


FIGURE 11: STANDARDS MAPPING V-MODEL ARCHITECTECA2030

TABLE 18: MAPPING OF EXISTING STANDARDS FOR SSC 3.2

Standard code	Standard title	Why relevant	How to use
IPC-2551	International Standard for Digital Twins [18].	The purpose of the standard is to enable interoperability of all forms of processing of digital data related to a product, that precisely match and represents the physical capabilities. In this way, any manufacturer can create and utilize the IPC Digital Twin to represent every process and possible actions taken on a product within the manufacturing and lifecycle environment, for engineering, modelling, planning, quality and reliability analysis, simulations, etc.	To use the hierarchical structure of IPC Digital Twin and its various aspects as reference for the demonstrator.
ISO/TR 18161	Automation systems and integration – Applications integration approach using information exchange requirements modelling and software capability profiling [11].	This standard describes an approach to specify requirements of information exchange between applications. A method for data exchange among physical product equipped with sensors, control and acquisition software, and diagnostics software has been described with an example of an integrated smart pump application, along with its interoperability requirements. Data acquisition and data exchange are	To implement data exchange framework among various aspects of Digital Twin, i.e., physical product equipped with sensors, control and acquisition software, virtual model, and data

		relevant for the Digital Twin demonstrator.	analysis and diagnostics software.
ISO 26262: 2018 1-12	Road vehicles - Functional safety [13].	Address safety-related systems that include one or more electrical/electronic (E/E) systems and that are installed in series production passenger cars (with a maximum gross vehicle mass up to 3 500 kg). The Automotive Safety Integrity Level (ASIL) is a key component for ISO 26262 compliance. Each safety requirement is assigned an ASIL of A, B, C, or D, (where D is the most safety critical processes/ strictest testing regulations). The ASIL is focusing on the harm to the driver and other road users and is not addressing the technologies used in the system.	Mapping the demonstrator requirements, features, and performance indicators to Automotive Safety Integrity Level (ASIL).
ISO/PAS 21448:2019 (SOTIF)	Road vehicles - Safety of the intended functionality (SOTIF) [12].	This document provides guidance on the applicable design, verification and validation measures needed to achieve the safety of the intended functionality. 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).	Determining residual risks related to hardware, software, and data associated with the demonstrator.
AEC Q100	Failure mechanism-based stress test qualification for integrated circuits [19].	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), and AEC Q200 (Passive components).	To determine relevant accelerated stress tests for failure mechanisms associated with the demonstrator.

## 7.10 Verification and validation

Verification and validation (V&V) of this demonstrator includes experimental validation of the virtual model (simulation-based results), for which accelerated stress tests will be carried out on the physical product and corresponding behaviour of the virtual model will be compared for validation. In addition, targets set for the FRs and NFRs of this demonstrator will be verified based on the V&V-specific KPIs defined for every requirement.

These V&V-specific KPIs represent a quantifiable measure for verification of the demonstrator targets. For example, this demonstrator aims to collect relevant data of the environmental parameters such as temperature, humidity, etc. Thus, the KPI ‘minimum number of types of sensors’ has been set for V&V. Similarly, the demonstrator aims to evaluate current state of component degradation, for which the ‘number of ageing mechanisms’ is a validation KPI. More details on V&V-specific KPIs corresponding to each NFR, and FR can be found in Table 10 to Table 17.

## 7.11 Demonstrator milestones

Milestones (MS) of the demonstrator SSC3.2 DigiPack are indicated in Table 19 along with their end-dates and contribution in respective work packages (WP) of ArchitectECA2030.

**TABLE 19: MILESTONES OF THE DEMONSTRATOR SSC 3.2**

MS	WP	Milestone Title	Due Date
MS1	WP1	Requirements and targets available	Jun. 2021 (m12)
MS2	WP4	Digital Twin-based method to assess package related failure mechanisms proposed	Jun. 2022 (m24)
MS3	WP5	Final Experimental hardware for the demonstrator build	Jan. 2023 (m30)
MS4	WP6	Digital Twin driven prognostics of lifetime is validated for the use case using dedicated reliability experiments aligned TRL 4-5	Jun. 2023 (m36)

## 8 SSC 3.3 Built-in Connectivity Component Ageing Monitoring (BIAM)

### 8.1 Target goals and achievements

The objective of this demonstrator is to identify possible faults (sources of error), as well as the analysis and quantification of the residual risk regarding the interaction between the perception domain and the V2X connectivity domain of automated vehicles.

The demonstrator is structured as a combination of an integrated circuit and corresponding software implementing a dedicated software stack.

Modelling the hardware/software interfaces at appropriate abstraction level(s) enables formal analysis and conformance testing of the connectivity component.

### 8.2 Demonstrator structure

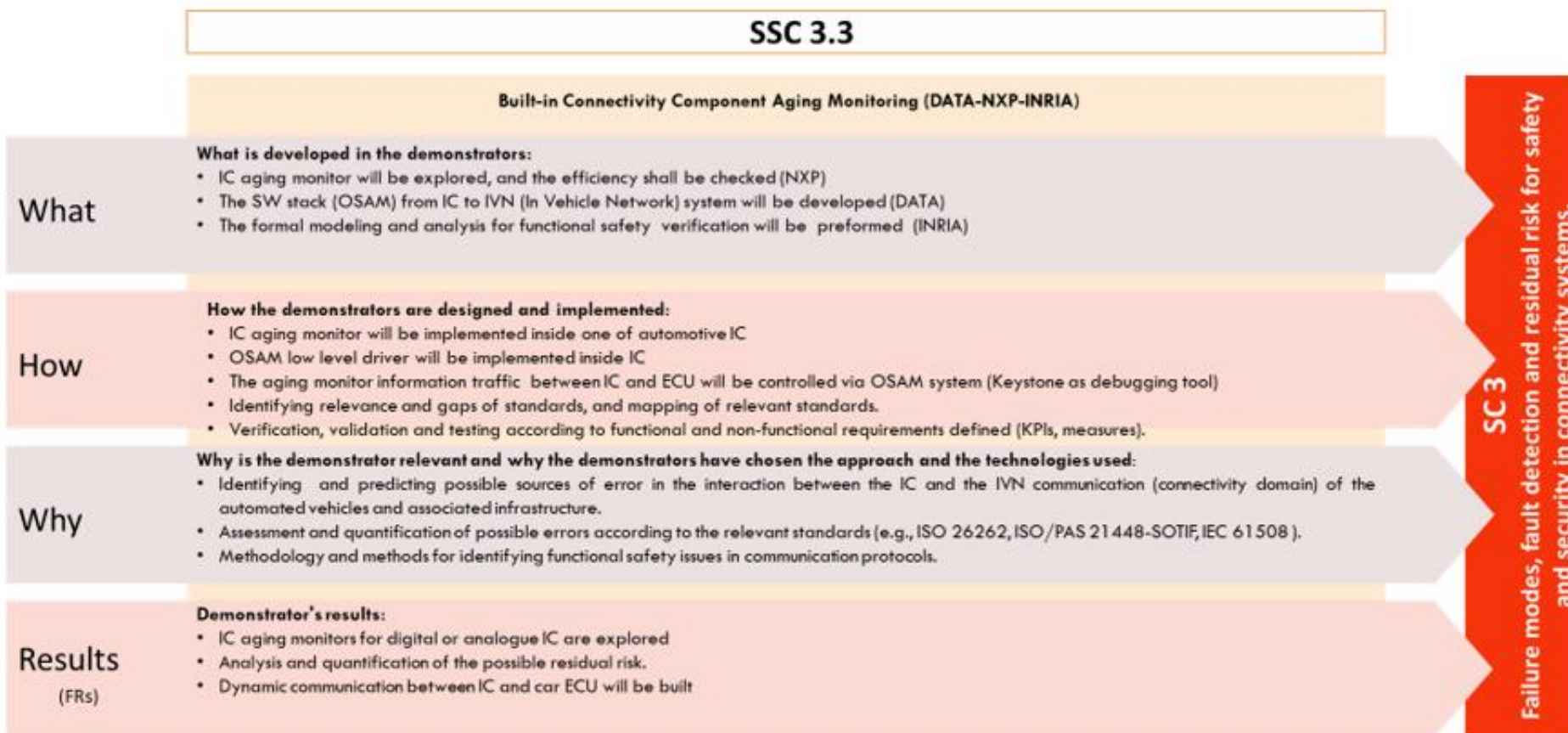
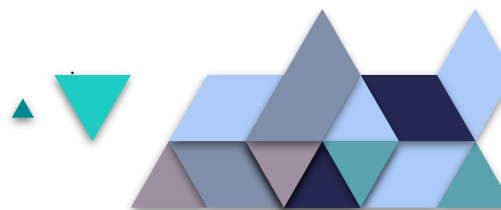


FIGURE 12: DEMONSTRATOR SSC 3.3 STRUCTURE



### 8.3 Demonstrator description

Health condition refers to the system and device performance. The deterioration of the health condition leads to non-recoverable multiple-point failures in the future that make the system unavailable.

Different types of ageing monitors will be evaluated by **NXP**, including monitoring of digital ICs and analogue components for different front-end processes.

The information from IC ageing monitor to the inside car system or Specific Car clouds will be interfaced via the OSAM SW environment developed by **DATA**.

The feasibility and verification of connection of health monitor combined with OSAM system will be done by **INRIA**, using formal models at appropriate abstraction levels.

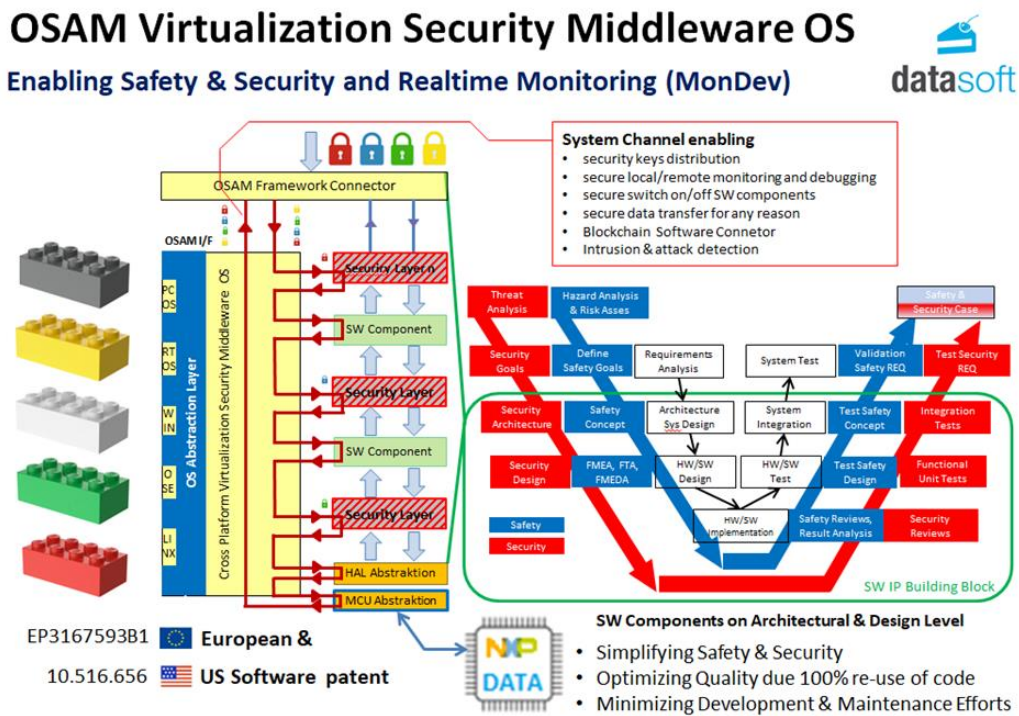
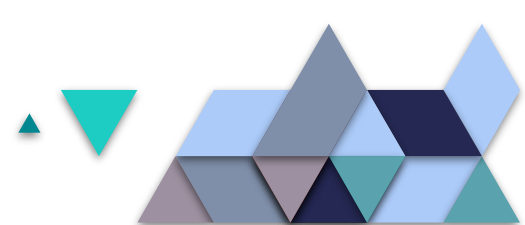


FIGURE 13: MONDEV ENABLING ON NXP MCU LEVEL WITH INTEGRATED OSAM DEVICE DRIVER ABSTRACTION

### 8.4 Treatment on residual risk

Residual Risks are risks which are not addressed by the ISO26262 [13] today. As the today's ISO26262 defines risk related to the ASIL level D ( $\Rightarrow 10^{-8}$  to  $10^{-7}$ ), residual will get covered by extending this risk levels to ASIL E ( $\geq 10^{-9}$  to  $< 10^{-8}$ ) related to autonomous driving.

The residual risk correlates with the safety and security of the software i.e., the probability of a malfunction. However, since residual risk occur on different disciplines in the development process, technical concerns as well as organizational and process related topics needs to get taken into consideration (and provided to SC5 for standardization).



## 8.5 Demonstrator relations to the main objectives and key targets

### 8.5.1 Objectives

The demonstrator SSC 3.3 aims at the following overall objectives:

**O1 - Continuous robust design optimization for each part in the ECS value chain (Technical):** IC ageing monitor is to detect the healthy condition of circuit and improve the circuit performance with the information we collect to extend the lifetime of IC.

**O2 - Framework for safety validation of ECS value chain (Technical):** OSAM system is to build out the connection between IC especially MCU with ECS.

**O3 - Identification and management of residual risks of the entire ECS value chain (Technical):** Formal models will provide quantitative estimates of residual risks of the ageing monitor IC.

The following supply chain specific objectives are addressed in this demonstrator (SSC 3.3):

**SC3-O1 - Investigate the residual risks of subsystems, and systems. Analysis, assessment and quantification of fault modes and their consequences on communication systems:** The different type of ageing models will be evaluated for different part of IC: digital or analogue circuit.

**SC3-O2 - Providing methods and tools for fault detection, localization, and repair:** In this demonstrator the different IC health information will be assembled which can assist to system decision on fault detection and repair. OSAM will provide the infrastructure for communication structure.

**SC3-O3 - Verification methodologies specifically adapted to ensure safety requirements:** In this demonstrator we will verify if the health monitor can provide the right information to the system and how it can be communicated with other part of ECS.

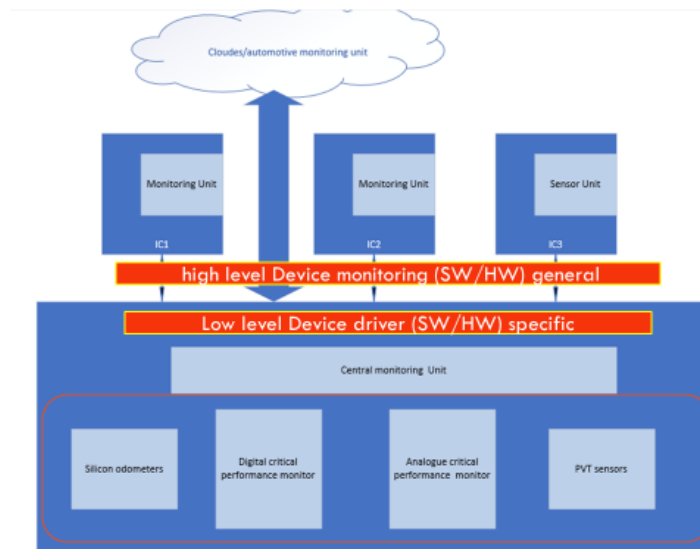
### 8.5.2 Key targets

**KT1 - Architectures, components, sub-systems enabling virtual development and validation (monitoring device, failure risk):** The demonstrator will contribute to novel architectures of ECS communication to handle safety component message. The different driver structure towards of ECS and MCU will be explored.

**KT4 - Definition and understanding of test coverage (residual risk, design feedback, lifetime monitoring, aggregated risk):** The basic task of IC ageing monitoring is to provide information of the remaining lifetime for the monitored subsystem and its availability for a mission. It helps planning scenarios of vehicle utilization and its maintenance as well. The demonstrator will contribute to adding these functionalities to digital IC and analogue IC.

## 8.6 Homologation framework mapping

The ageing monitor enables a more precise estimation of the degradation state of the IC and thus a better approximation of the residual risk over time. This helps to provide more accurate information in the homologation process. A good estimate of the reliability of the connection devices is crucial to ensure proper functioning and safety. In this demonstrator, we aim to communicate IC health conditions inside car even to Clouds to assist future car system decision matrix.



**FIGURE 14 IC AGEING MONITOR CONTRIBUTIONS**

## 8.7 Non-functional requirements, KPIs, and measures

In Table 20, Table 21, and Table 22 we present the three most relevant NFRs, KPIs and Measures for SSC 3.3.

**TABLE 20: NFRs, KPIs AND MEASURES FOR SSC 3.3 - COMPATIBILITY (INTEROPERABILITY)**

NFR	Compatibility (Interoperability)
NFR definition	Degree to which a product, system or component can exchange information with other products, systems or components, and/or perform its required functions, while sharing the same hardware or software environment.
KPI name	Extent of methodology transfer.
Description	How compatible is the methodology (of D.T.) for other technology and IC product
Measure	Number of supported IC fabrication processes and different type of MCU products.
Type of measure	Quantitative [number].
Method of collection and measurement	Determine the number of processes.
Demonstrator target	2 processes.
KPI for Verification and validation	Number of processes used for IC ageing monitor.

**TABLE 21: NFRs, KPIs AND MEASURES FOR SSC 3.3 - RELIABILITY**

NFR	Reliability
NFR definition	IC ageing monitor shall fulfil automotive reliability requirement.
KPI name	Life time.
Description	Ageing monitor can work in the extreme mission profile.
Measure	Ageing simulation.
Type of measure	Quantities (hours).

Method of collection and measurement	Ageing simulation with all ageing mechanisms (BTI, HCI and TDDB).
Demonstrator target	>10K hours.
KPI for Verification and validation	At least 2 different type of ageing monitors passed desired target hours.

**TABLE 22: NFRs, KPIs AND MEASURES FOR SSC 3.3 - MAINTAINABILITY**

<b>NFR</b>	<b>Maintainability</b>
NFR definition	Degree of effectiveness and efficiency with which a product or system can be modified to improve it, correct it or adapt it to changes in environment, and in requirements (ISO 25010). Relevant sub-characteristic is testability.
KPI name	Software update and hardware self-testability.
Description	Monitoring and updating of the ageing monitor can get performed via the OSAM during run time.
Measure	Means to update software and BIST of ageing monitor.
Type of measure	Quantitative [number] and qualitative (checking).
Method of collection and measurement	How many ways the software can be updated.
Demonstrator target	2 ways for update software and BIST for ageing monitor.
KPI for Verification and validation	Different ways to update software and if BIST works.

## 8.8 Functional requirements, KPIs, and measures

In Table 23, Table 24, Table 25 and Table 26 we present the most relevant FRs, KPIs and Measures for SSC 3.3.

**TABLE 23: FRs, KPIs AND MEASURES FOR SSC 3.3 - EVALUATION OF IC DEGRADATION STATE**

<b>FR</b>	<b>Evaluation of IC degradation state</b>
FR definition	Evaluation of current state of degradation based on degradation models and history of research.
KPI name	Overview of degradation (ageing) mechanisms.
Description	What degradation mechanism are being considered/analysed.
Measure	Number of ageing mechanisms.
Type of measure	Quantitative[number].
Method of collection and measurement	Literature study and ageing simulation for one IC against each of ageing mechanism
Demonstrator target	3
KPI for Verification and validation	Select the most relevant aging mechanism for IC.

**TABLE 24: FRs, KPIs AND MEASURES FOR SSC 3.3 - MONITORING IC PROCESS PARAMETERS**

<b>FR</b>	<b>Monitoring IC process parameters</b>
FR definition	Data collection of the possible monitors for the different ageing mechanism.
KPI name	Type of IC aging monitor.

Description	Which circuit is suitable for monitoring the different ageing mechanism?
Measure	Number of ageing monitors.
Type of measure	Quantitative[number].
Method of collection and measurement	Types of sensors used state of the art.
Demonstrator target	4 (TDDDB, BTI, HCI and 1 for analogue IC).
KPI for Verification and validation	Minimum number of types of sensors for sufficiently accurate health monitoring.

**TABLE 25: FRs, KPIs AND MEASURES FOR SSC 3.3 - OSAM INTERFACES**

FR	OSAM interfaces
FR definition	OSAM provides a generic interface between the MCU hardware on chip component level and the application software enable monitoring between the IC and ECU (input to MonDev to SC5 for standardization purposes).
KPI name	Type of interface.
Description	A chip independent generic driver abstraction is getting introduced enabling monitoring on Car ECU level as well as on MCU level by implementing the OSAM interface (input to MonDev to SC5 for standardization purposes)
Measure	Nr of driver.
Type of measure	Quantitively [number].
Method of collection and measurement	Type of interface required to enable communication.
Demonstrator target	2
KPI for Verification and validation	Identifying different requirement for 2 different interfaces and pass the communication verification.

**TABLE 26: FRs, KPIs AND MEASURES FOR SSC 3.3 - CONFORMANCE TEST INTERFACES**

FR	Conformance test interfaces
FR definition	The whole system shall be tested for performance and conformance.
KPI name	Verification requirement.
Description	Conformance of system-level behaviour.
Measure	Test suite execution verdict.
Type of measure	PASS/FAIL.
Method of collection and measurement	Perform failure analysis after accelerated testing to confirm failure modes.
Demonstrator target	Ageing monitor flag can be properly delivered to ECU.
KPI for Verification and validation	Automated generation of a conformance test suite from the formal model.

## 8.9 Mapping to existing standards

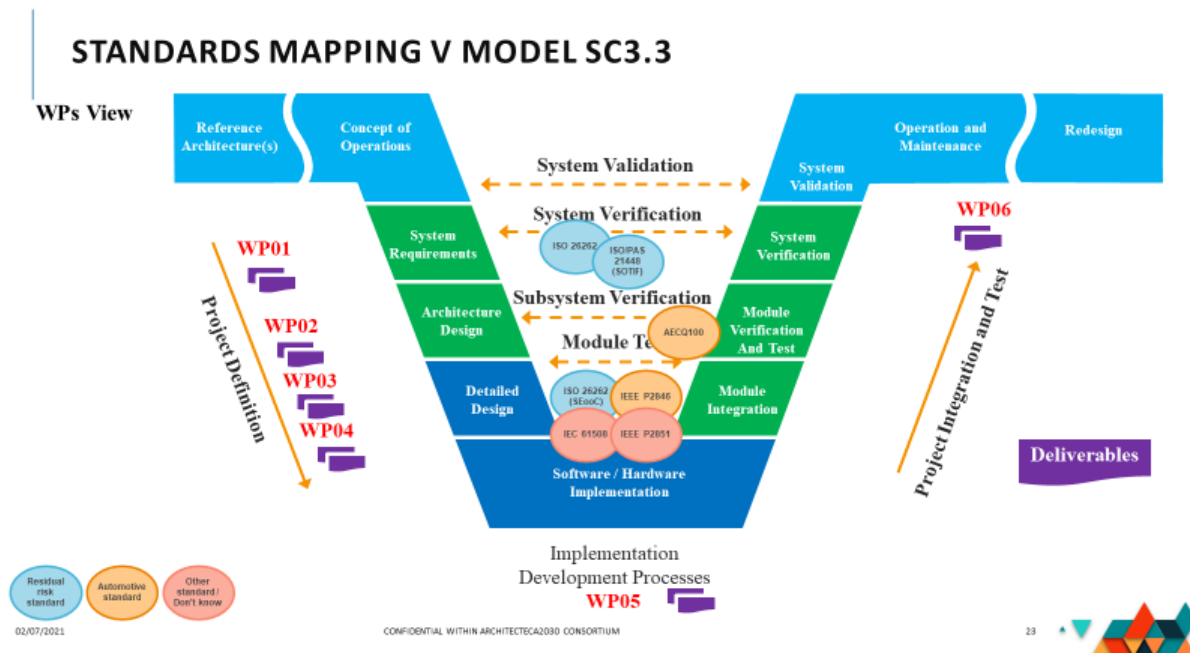


FIGURE 15: STANDARDS MAPPING V-MODEL SSC 3.3

TABLE 27: MAPPING OF EXISTING STANDARDS FOR SSC 3.3

Standard code	Standard title	Why relevant	How to use
ISO 26262	Road Vehicles – Functional Safety [13].	Ageing monitor is needed for ASILD+ IC	Determine residual risk related to different demonstrator functionalities associated with the integration of connectivity systems and perception devices.
ISO/PAS 21448	Road Vehicles – Safety of the intended functionality [12].	Ageing monitor is needed for ASILD+ IC	Map demonstrator safety related requirements (functionalities, performances, features) according to the ASIL requirements.
IEC 61508	IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems., (for industrial related applications) [14].	Ageing monitor is needed for ASILD+ IC	Will be used in conjunction with IEC 26262 and ISO/PAS 21448.
IEEE P2846	Assumptions for Models in Safety-Related Automated Vehicle Behaviour [16].	During the verification, the model limitation shall be aware	Will be used during the verification phase to set the boundaries and expectations of verification results.
IEEE P2851	Exchange/ Interoperability Format for Safety Analysis and Safety Verification of IP, SoC and Mixed Signal ICs [17].	The state of art of safety analysis shall be known	Will be used to analyse safety related test case.

AEC Q100	Failure mechanism-based stress test qualification for integrated circuits [19].	Ageing monitor verification shall apply automotive standard to check the lifetime behaviour	AEC Q100 will be used as baseline for IC component reliability and quality requirement.
----------	---	---	---

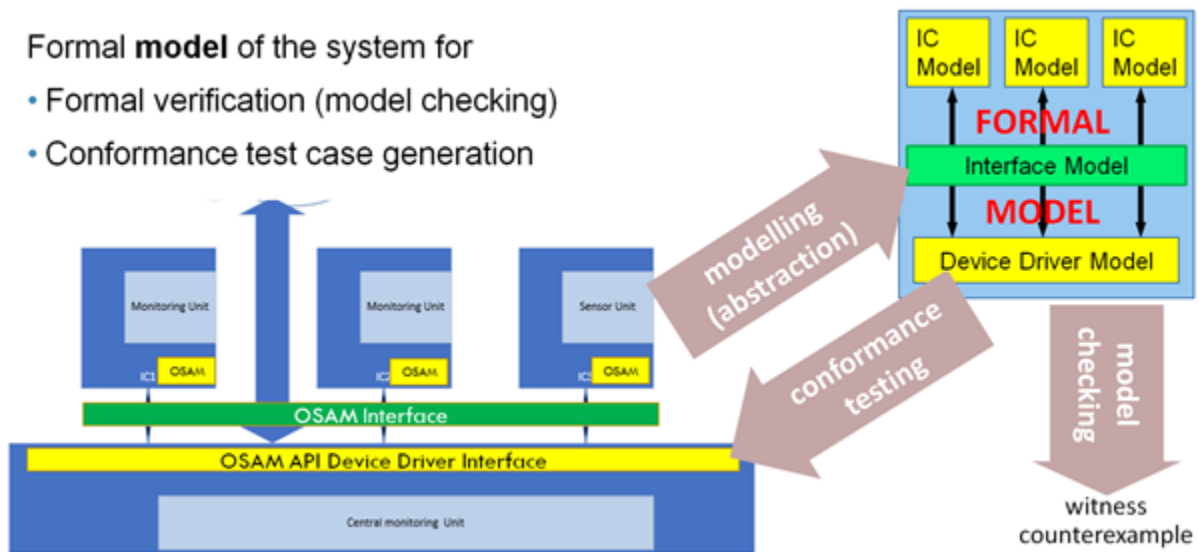
### 8.10 Verification and validation

To assess and quantify possible failures and systemic uncertainties, formal analysis tools of the state-of-the-art CADP toolbox [3][7] will be applied in three steps.

First, the hardware/software interfaces are formally modelled at appropriate abstraction levels to achieve good compromise between the size and precision of the model.

Then, functional, and quantitative properties will be formally expressed and checked on the model. In the case the properties are not satisfied, counterexamples provided by the verification tools will help to understand and correct the system [7].

Last, an automatically generated conformance test suite will be used to ensure that the system indeed conforms to the validated formal models [4][6].



**FIGURE 16: VERIFICATION AND VALIDATION OVERVIEW**

As CADP is based on process calculi, the toolbox is particularly suitable for the formal analysis of communication protocol stacks, because the modelling languages of CADP are based on the LOTOS language at the heart being a standard proposed for exactly this task in the context of the ISO/OSI protocol stack [8].

CADP has also been used for the verification of cryptographic protocols [9].

### 8.11 Demonstrator milestones

Table 28 shows the project's overall milestones (MS) in relation with the work packages (WP) and the plan to fulfil the demonstrator in SSC 3.3.

**TABLE 28: SSC 3.3 DEMONSTRATOR MILESTONES (SSC 3.3)**

MS	WP	MS Title	Due date
MS1	WP1	Requirements and targets available. Initial concept for demonstrator is defined	June 2021
MS2.1	WP4	Selection of ageing monitors are analysed and the residual risks for IC process monitoring devices are identified	June 2022
MS2.2	WP4	OSAM SW/HW has been worked out	June 2022
MS2.3	WP4	INRIA virtual environment has been implemented	June 2022
MS3	WP4 WP5	IC ageing monitor, OSAM and INRIA verification environment are integrated.	December 2022
MS4	WP6	Overall system monitoring device verified.	June 2023

## 9 SC3 demonstrators summarized

The three SC3 demonstrators use a methodology for risk estimations of connectivity systems considering the planned system integrity, and dependability and the FRs and NFRs are defined to understand the residual risk associated with connectivity systems.

The RCD-V2X demonstrator addresses road condition detection and V2X connectivity development. The demonstrator is applying residual risk analysis and classification for supporting a framework and methodology for integrating autonomous vehicle domains by implementing a road condition detection sensor combined with the onboard unit (OBU) for V2X connectivity.

The DigiPack demonstrator focuses on developing a digital twin concept and implementing lifetime prognostics of electronic components packages. Virtual simulation and validation of the models are designed for the demonstrator. Identification of residual risk for different operating conditions for autonomous vehicles is planned. The work includes developing data-driven and physics-of-degradation models combined with the digital twin technology for lifetime monitoring and design for reliability.

The BIAM demonstrator implements a built-in connectivity monitoring device and addresses the reliability analysis and risk identification for connectivity component ageing monitoring used in autonomous vehicle operating conditions.

Table 29 summarises the main standards that are used by the three demonstrators in their developments.

**TABLE 29: MAPPING OF EXISTING STANDARDS SUMMARISED**

Standards vs Demonstrators	SSC 3.1	SSC 3.2	SSC 3.3
ISO/TR 18161 [11]		X	
ISO/PAS 21448 (SOTIF) (2019) [12]	X	X	X
ISO 26262 (2018) [13]	X	X	X
IEC 61508 (2010) [14]	X		X

IEEE 802.11p	x		
IEEE 802.11bd (2018) [15]	X		
IEEE P2846 [16]			X
IEEE P2851 [17]			X
IPC-2551 [18]		X	
AEC Q100 [19]		X	X
ANSI/UL 4600	x		
ISO/TR 4804	x		

## 10 Conclusion

### 10.1 Contribution to overall picture

The deliverable D1.3 presents the FRs and NFRs of the three demonstrators in SC3. The FRs and NFRs of the demonstrators are defined to support clarifying the risks to electronic and component systems integrated into autonomous vehicles that can occur due to connectivity domain systems. The deliverable discusses ways in which the residual risk can be identified and mitigated. The demonstrators developed in SC3 have been chosen to improve the ability to understand residual risks associated with connectivity systems and what elements are needed to support the digital homologation of autonomous vehicles.

### 10.2 Relation to the state-of-the-art and progress beyond it

The work in SC3 builds on the state-of-the-art and advance it. The details of this progress are described for each partner involved in Table 30 and refined as the work is going.

**TABLE 30: STATE OF THE ART AND BEYOND**

Partner (Topic)	Description
SINTEF (RCD-V2X)	As road surface conditions monitoring systems today are not part of automotive sensor suits, the demonstrator will provide the technology and methods to assess and mitigate the effects of varying surface conditions. Integration and interaction of the V2X connectivity and the perception for road conditions. Perform tests for the evaluation of residual risk that are aligned with the standard framework and use it as input to the methodology for risk estimations of connectivity systems to support virtual validation of automated and connected vehicles. SINTEF address the residual risk framework for safety and security in connectivity systems for electric, connected, and automated vehicles.
NXT (RCD-V2X)	As road surface conditions monitoring systems today are not part of automotive sensor suits, the demonstrator will provide the technology and methods to assess and mitigate the effects of varying surface conditions. Integration and interaction of the V2X connectivity and the perception for road conditions. Perform tests for the evaluation of residual risk that are aligned with the standard framework and use it as input to the methodology for risk estimations of connectivity systems to support virtual validation of automated and connected vehicles. NXT address the integration, interaction and tests between the perception domain and the connectivity domain.

TSENSE (RCD-V2X)	As road surface conditions monitoring systems today are not part of automotive sensor suits, the demonstrator will provide the technology and methods to assess and mitigate the effects of varying surface conditions. Integration and interaction of the V2X connectivity and the perception for road conditions. Perform tests for the evaluation of residual risk that are aligned with the standard framework and use it as input to the methodology for risk estimations of connectivity systems to support virtual validation of automated and connected vehicles. TSENSE address the sensor development, integration, and validation.
NXP (DigiPack)	Digital Twins based health monitoring using edge computing are currently in concept phase, and monitoring of microelectronics package degradation is only performed in academia. We aim for developing data-driven and physics-of-degradation models combined with the Digital Twin technology for lifetime prediction and design for reliability.
TUDE (DigiPack)	Digital Twins based health monitoring using edge computing are currently in concept phase, and monitoring of microelectronics package degradation is only performed in academia. We aim for developing data-driven and physics-of-degradation models combined with the Digital Twin technology for lifetime prediction and design for reliability.
NXP (BIAM)	Early life failures (ELF) are effectively screened out by stress test for automotive IC. With long mission profile expected with Autonomous driving, the in-field IC health monitoring is needed to flag the degrading performance to the car central system. To realize the Fail operational and Fail predication. Different types of ageing monitors will be evaluated by NXP, including monitoring of digital ICs and analogue components for different front-end processes.
INRIA (BIAM)	The application of CADP to the OSAM framework challenges the formal analysis by the combination of cryptographic aspects in a protocol stack.
DATA (BIAM)	<p><b>State of the art for secure monitoring and debugging:</b></p> <ul style="list-style-type: none"> <li>• Proprietary solutions.</li> <li>• Limited to ASIL-D.</li> <li>• Standardized interfaces.</li> </ul> <p><b>Progress beyond the state of the art:</b></p> <ul style="list-style-type: none"> <li>• Radical reduction on development efforts and costs due Safety &amp; Security by design.</li> <li>• 100% re-use of code.</li> </ul> <p>Tunnel effect use on chip level for monitoring purposes.</p>

### 10.3 Impacts to other WPs, Tasks and SCs

The work carried out in task T1.3 (WP1) regarding the SC3 demonstrators will mainly contribute to WP4 through task T4.1 "Identification and management of risks in automotive ECS in the connectivity and perception interacting domains"; to WP5 through task T5.1 "Integration of the residual risk framework in connectivity and perception systems" and to WP6 through task T6.1 "Validation of mission oriented ECS in the connectivity and perception interacting domains".

**TABLE 31: OUTCOME AND IMPACTS**

Partner (Topic)	Description
SINTEF (RCD-V2X)	Demonstrator SSC 3.1 will contribute to WP4 - framework and identification of residual risks for the road condition detection and V2X connectivity system, WP5 - integration of the residual risk framework in road condition detection and V2X

	connectivity system, and WP6 - validation of the road condition detection and V2X connectivity system.
NXT (RCD-V2X)	Demonstrator SSC 3.1 will contribute to WP4 - framework and identification of residual risks for the road condition detection and V2X connectivity system, WP5 - integration of the residual risk framework in road condition detection and V2X connectivity system, and WP6 - validation of the road condition detection and V2X connectivity system.
TSENSE (RCD-V2X)	Demonstrator SSC 3.1 will contribute to WP4 - framework and identification of residual risks for the road condition detection and V2X connectivity system, WP5 - integration of the residual risk framework in road condition detection and V2X connectivity system, and WP6 - validation of the road condition detection and V2X connectivity system.
NXP (DigiPack)	Demonstrator SSC 3.2 will contribute to WP4 – developing methods for Digital Twin, WP5 – building a prototype, and WP6 – validating Digital Twin.
TUDE (DigiPack)	Demonstrator SSC 3.2 will contribute to WP4 – developing methods for Digital Twin, WP5 – building a prototype, and WP6 – validating Digital Twin.
NXP (BIAM)	Demonstrator SSC 3.3 will be used to carry on the whole developing work. The main deliverables are in WP1, WP4 and WP7.
INRIA (BIAM)	Demonstrator SSC 3.3 will be used in subsequent work packages.
DATA (BIAM)	The OSAM virtualization security middleware OS can be applied to software related issues where safety and security is relevant.

## 10.4 Contribution to demonstration

**TABLE 32: CONTRIBUTION TO DEMONSTRATORS**

Partner (Topic)	Description
SINTEF (RCD-V2X)	Methodology, system integration and validation for demonstrator SSC 3.1.
NXT (RCD-V2X)	Sensor system integration, interfaces and V2X tests for demonstrator SSC 3.1.
TSENSE (RCD-V2X)	Integration, sensor development and validation for demonstrator SSC 3.1.
NXP (DigiPack)	Providing experimental data on products performance, (expertise on the) virtual model, and hardware for demonstrator SSC3.2.
TUDE (DigiPack)	Developing methods for data model and connections model (AI, machine learning) for Digital Twin and providing software for the demonstrator SSC 3.2.
NXP (BIAM)	Analysis of fault modes and their consequences on actuators and propulsion systems. The different type of ageing models will be evaluated for different part of IC: digital or analogue circuit. Providing methods and tools for fault detection, localization, and repair.
INRIA (BIAM)	Formal analysis and test case generation for the demonstrator SSC 3.3.
DATA (BIAM)	The requirements describe the intended use of the device driver abstraction.

## 10.5 Other conclusions and lessons learned

**TABLE 33: OTHER CONCLUSIONS AND LEARNINGS**

Partner (Topic)	Description
SINTEF (RCD-V2X)	The definition of FRs and NFRs are critical for increasing the safety design of the HW/SW components of autonomous and connected vehicles and integrate them into

	the proper architecture. Continually evaluating and improving the residual risk present in the system is required for autonomous vehicles. Identifying latent and emergent risks is essential to enable identifying, implementing, and verifying additional mitigation measures. Modifying the ODD based on the current system capabilities and aligned with the residual risk control actions need further investigation for autonomous vehicles.
NXT (RCD-V2X)	Self-assessment and iteration over the system development and deployment lifecycle are essential to developing the safety case and the scenarios for SSC3.1.
TSENSE (RCD-V2X)	The importance of defining properly the FRs and NFRs for the demonstrator SSC3.1 and the alignment with the different standards available.
NXP (DigiPack)	Goals and requirements of the demonstrator SSC3.2 as well as the partner-specific contribution have been clearly defined. Relation to industrial standards has been studied.
TUDE (DigiPack)	Goals and requirements of the demonstrator SSC3.2 as well as the partner-specific contribution have been clearly defined. Relation to industrial standards has been studied.
NXP (BIAM)	The cooperation with other partners for one demonstrator is good experience to extend the view along the developing phase.
INRIA (BIAM)	Goals and requirements of the demonstrator SSC 3.3 have been defined and provide an interesting case study on applying formal methods at the hardware/software interface.
DATA (BIAM)	Goals and requirements of the demonstrator SSC3.2 and the partner-specific contributions have been defined.

## 11 References

- [1] Vogel, M., Knapik, P., Cohrs, M., Szyperrek, B., Pueschel, W., Etzel, H., Fiebig, D., Rausch, A., and Kuhrmann, M. Metrics in automotive software development: A systematic literature review. *Journal of Software: Evolution and Process* published by John Wiley & Sons Ltd., May 2020. Online at: <https://onlinelibrary.wiley.com/doi/full/10.1002/smr.2296>
- [2] ISO/IEC 25010:2011. Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models. Online at: <https://www.iso.org/standard/35733.html>
- [3] Garavel, H., Lang, F., Mateescu, R., and Serwe, W. "CADP 2011: A Toolbox for the Construction and Analysis of Distributed Processes". *International Journal on Software Tools for Technology Transfer*, doi: [10.1007/s10009-012-0244-z](https://doi.org/10.1007/s10009-012-0244-z)
- [4] Marsso, L., Mateescu, R., and Serwe, W. "TESTOR: A Modular Tool for On-the-Fly Conformance Test Case Generation". *Proceedings of the 24<sup>th</sup> International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2018)*, doi: [10.1007/978-3-319-89963-3\\_13](https://doi.org/10.1007/978-3-319-89963-3_13)
- [5] MobilEye. Implementing the RSS Model on NHTSA Pre-Crash Scenarios, 2019. Available online at: [https://static.mobileye.com/website/corporate/rss/rss\\_on\\_nhtsa.pdf](https://static.mobileye.com/website/corporate/rss/rss_on_nhtsa.pdf)
- [6] Kriouile A., Serwe W. "Using a Formal Model to Improve Verification of a Cache-Coherent System-on-Chip". *Proceedings of the 21<sup>st</sup> International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2015)*, doi: [10.1007/978-3-662-46681-0\\_62](https://doi.org/10.1007/978-3-662-46681-0_62)
- [7] Lantreibecq, E. and Serwe, W. "Formal Analysis of a Hardware Dynamic Task Dispatcher with CADP". *Science of Computer Programming*, doi: [10.1016/j.scico.2013.01.003](https://doi.org/10.1016/j.scico.2013.01.003)
- [8] Mazzanti, F., Ferrari, A., and Spagnolo, G. "Towards formal methods diversity in railways: an experience report with seven frameworks". *International Journal Software Tools for Technology Transfer* 20(3): 263-288 (2018), doi: [10.1007/s10009-018-0488-3](https://doi.org/10.1007/s10009-018-0488-3)
- [9] "LOTOS - A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour". ISO/IEC standard 8807, 1989.
- [10] Serwe, W. "Formal Specification and Verification of Fully Asynchronous Implementations of the Data Encryption Standard". In *Proceedings of the 1st International Workshop on Models for Formal Analysis of Real Systems (MARS'2015)*, doi: [10.4204/EPTCS.196.6](https://doi.org/10.4204/EPTCS.196.6).
- [11] ISO/TR 18161 (2013): Automation systems and integration – Applications integration approach using information exchange requirements modelling and software capability profiling. Online at: <https://www.iso.org/standard/60899.html>
- [12] ISO/PAS 21448 (2019): Road vehicles - Safety of the intended functionality (SOTIF). Online at: <https://www.iso.org/standard/70939.html>
- [13] ISO 26262 (2018): Road vehicles - Functional safety. Online at: <https://www.iso.org/standard/68383.html>
- [14] IEC 61508 (2010): Functional safety of electrical/electronic/programmable electronic safety-related systems. Online at: <https://webstore.iec.ch/publication/5515>
- [15] IEEE 802.11bd (2018): 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. Online at: [https://standards.ieee.org/project/802\\_11bd.html](https://standards.ieee.org/project/802_11bd.html)

- [16] IEEE P2846 (2020): Assumptions for Models in Safety-Related Automated Vehicle Behaviour. Online at: xxx <https://standards.ieee.org/project/2846.html>
- [17] IEEE P2851 (2019): Exchange/ Interoperability Format for Safety Analysis and Safety Verification of IP, SoC and Mixed Signal ICs. Online at: <https://standards.ieee.org/project/2851.html>
- [18] IPC-2551 (2020): International Standard for Digital Twins. Online at: <https://shop.ipc.org/IPC-2551-English-D>
- [19] AEC Q100 (2014): Failure mechanism based stress test qualification for integrated circuits. Online at: [http://www.aecouncil.com/Documents/AEC\\_Q100\\_Rev\\_H\\_Base\\_Document.pdf](http://www.aecouncil.com/Documents/AEC_Q100_Rev_H_Base_Document.pdf)
- [20] Wood, M. et al., 2019. *Safety First for Automated Driving*. Available online at: <https://www.daimler.com/documents/innovation/other/safety-first-for-automated-driving.pdf>

## 12 List of figures

Figure 1: SC 3 demonstrators .....	9
Figure 2: SC 3 demonstrators structure and content.....	10
Figure 3: SC 3 demonstrators timeline.....	11
Figure 4: Demonstrator SSC 3.1 structure.....	12
Figure 5: SSC 3.1 cooperation and roles.....	13
Figure 6: Demonstrator SSC 3.1 overview.....	14
Figure 7: SSC 3.1 block schematic overview.....	15
Figure 8: Standards mapping V-model ArchitectECA2030 relevant for SC3 .....	22
Figure 9: Demonstrator SSC 3.2 structure.....	27
Figure 10 Demonstrator SSC 3.2 overview.....	28
Figure 11: Standards mapping V-model ArchitectECA2030.....	34
Figure 12: Demonstrator SSC 3.3 structure.....	37
Figure 13: MonDev enabling on NXP MCU level with integrated OSAM Device Driver Abstraction ....	38
Figure 14 IC ageing monitor contributions.....	40
Figure 15: Standards mapping V-model SSC 3.3 .....	43
Figure 16: Verification and validation overview.....	44

## 13 List of tables

Table 1: Contributions of partners .....	6
Table 2: NFRs, KPIs and Measures for SSC 3.1 - Reliability (Maturity) .....	18
Table 3: NFRs, KPIs and Measures for SSC 3.1 - Compatibility (Interoperability) .....	18
Table 4: NFRs, KPIs and Measures for SSC 3.1 - Maintainability (Testability) .....	19
Table 5: FRs, KPIs and Measures for SSC 3.1 - Monitoring detection .....	20
Table 6: FRs, KPIs and Measures for SSC 3.1 - Prediction algorithms .....	20
Table 7: FRs, KPIs and Measures for SSC 3.1 - Wireless connectivity .....	21
Table 8: Mapping of existing standards for SSC 3.1 .....	22
Table 9: SSC 3.1 demonstrator milestones .....	25
Table 10: NFRs, KPIs and Measures for SSC 3.2 - Compatibility (Interoperability) .....	31
Table 11: NFRs, KPIs and Measures for SSC 3.2 - Functional Stability (Functional Correctness) .....	31
Table 12: NFRs, KPIs and Measures for SSC 3.2 - Performance Efficiency (Resource Utilization) .....	31
Table 13 NFRS, KPIS AND MEASURES FOR SSC 3.2 - Reliability (Maturity) .....	32
Table 14: FRs, KPIs and Measures for SSC 3.2 - Monitoring environmental parameters .....	32
Table 15: FRs, KPIs and Measures for SSC 3.2 - Algorithm for lifetime prediction .....	33
Table 16: FRs, KPIs and Measures for SSC 3.2 - Evaluation of degradation state .....	33
Table 17 : FRs, KPIs and Measures for SSC 3.2 - Failure (type) prediction .....	33
Table 18: Mapping of existing standards for SSC 3.2 .....	34
Table 19: Milestones of the demonstrator SSC 3.2 .....	36
Table 20: NFRs, KPIs and Measures for SSC 3.3 - Compatibility (Interoperability) .....	40
Table 21: NFRs, KPIs and Measures for SSC 3.3 - Reliability .....	40
Table 22: NFRs, KPIs and Measures for SSC 3.3 - Maintainability .....	41
Table 23: FRs, KPIs and Measures for SSC 3.3 - Evaluation of IC degradation state .....	41
Table 24: FRs, KPIs and Measures for SSC 3.3 - Monitoring IC process parameters .....	41
Table 25: FRs, KPIs and Measures for SSC 3.3 - OSAM interfaces .....	42
Table 26: FRs, KPIs and Measures for SSC 3.3 - Conformance test interfaces .....	42
Table 27: Mapping of existing standards for SSC 3.3 .....	43
Table 28: SSC 3.3 demonstrator milestones (SSC 3.3) .....	45
Table 29: Mapping of existing standards summarised .....	45
Table 30: State of the art and beyond .....	46
Table 31: Outcome and impacts .....	47
Table 32: Contribution to demonstrators .....	48
Table 33: Other conclusions and learnings .....	48

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