SECREDAS

Product Security for Cross Domain Reliable Dependable Automated Systems

DELIVERABLE RPORT
D1.7: “Final Demonstrators Description”

Document Type	Deliverable
Document Number	D1.7
Document Title	Final Demonstrators Description
Primary Author(s)	Lino Estêvão, Luis Campos (T1.3 leaders)
Document Date	18/06/2019
Document Version / Status	v1.0
Distribution Level	Public
Reference DoA	May 2019

Project Coordinator	Patrick Pype, NXP Semiconductors, patrick.pype@nxp.com
Project Website	www.secredas.eu (in progress)
JU Grant Agreement Number	783119

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, The Netherlands, Poland, Romania, Sweden and Tunis

CONTRIBUTORS

Name	Organization	Name	Organization
Lino Estêvão	PDM&FC	Joaquim Bastos	ITAV
Luis Campos	PDM&FC	Leos Mikulka	AVL-SF
Rodrigo Santos	PDM&FC	Filipe Carvalho	AVL-SF
Rodolfo Ferreira	PDM&FC	Florian Stahl	AVL-SF
Petr Fiedler	BUT	Boris Goranov	Ubiqu
Karel Kalivoda	IMA	Iuliana Dragomir	TNO
Alper Kocademir	Roche	Hayk Hamazaryan	ZF
Arturo Medela	TST	Stelios Karagiannis	Beyond Vision

FORMAL REVIEWERS

Name	Organization	Date
Roy Pennings	NXP	7/6/2019
Project Steering Board	N/A	18/6/2019

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
V0.1	18/03/2019	Lino Estêvão	Document Draft
V0.2	25/03/2019	Lino Estêvão	Table of contents
V0.3	26/03/2019	Luis Campos	Document Review
V0.4	30/05/2019	Boris Goranov	Update UC4
V1.0	12/06/2019	Rodrigo Santos	Final revision

Executive summary

Work Package 1 (WP1) is developing several user scenarios which are relevant for the SECREDAS project objective to cover the crossroads of security, safety and privacy protection. The scenarios will be used to derive future reference architectures and requirements (input to WP2), develop common technology elements (input to WP3) and for the development of next generation highly secured automotive, health, and rail technology, both hardware and software (input to WP3-8).

Deliverable 1.7 (D1.7) is part of Task 1.3 which aims to translate the user scenarios into demonstrators using the various components identified in task 1.2. The outcome of this task serves as input to WP9 – Demonstrators.

This document Is organized in tree main chapters. In chapter one, the necessary background on evolving use cases / user scenarios as well as common technology elements are summarised and mapped to security threads. Chapter two provides an overview of the demonstrators defined in the SECREDAS DoA. Chapter three establishes the correlation of the last chapters in order to provide a holistic script for each demonstrator.

Table of Contents

Executive summary 3

Table of Contents 4

Acronyms 5

1. Background to deliverable 1.7 6

1.1 Use cases / user scenarios 6

1.2 Common Technology elements / Use Cases 7

1.3 Security and privacy threats map to CTE 12

1.3.1 Top 10 automotive security and privacy threats 12

1.3.2 Mapped threats to CTEs 14

2. Demonstrators 16

3. Demonstrators holistic description: mapping scenarios, threats, and CTEs to demonstrators 17

3.1 DEMO I - Autonomous driving and infrastructure servers: 17

3.2 DEMO II - Driver Monitoring Systems 26

3.3 DEMO III - Cybersecurity and connectivity 33

4. Conclusions on deliverable 1.7 37

List of Figures 38

List of Tables 38

Terminology 39

References 39

ANNEX 1 – Use case scenario's description 40

Scenario description 1.1 40

Scenario description 1.2 43

Scenario description 1.3 44

Scenario description 1.4 46

Scenario description 1.5 48

Scenario description 2.1 49

Scenario description 2.2 50

Scenario description 2.3 51

Scenario description 3.1 53

Scenario description 4.1 54

Scenario description 5.1 55

Scenario description 6.1 57

ANNEX 2 – Components of demonstrator II 58

Acronyms

ADAS	Advanced Driver Assistance System
AES	Advanced Encryption Standard
AHG	Ad-Hoc Group (of ISO or IEC Technical Committees)
AI	Artificial intelligence
API	Application Programming Interface
APP	Application
ASIL	Automotive Safety Integrity Level
CAN	Controller Area Network
C-ITS	Cooperative Intelligent Transport Systems
CEN	European Standardization Committee
CENELEC	European Standardization Committee for electrotechnical standards
CPS	CyberPhysical Systems
CSE	Cryptographic Services Engine
DAC	Discretionary Access Control
DRM	Digital Rights Management
E/E/PE	Electric/Electronic/Programmable Electronics
ECU	Embedded Control Unit
EKMS	Electronic Key Management System
EN	European Norms
ENISA	European Union Agency for Network and Information Security
ERA	EU Agency for Railways
eSE	embedded Secure Element
eNVM	embedded Non-volatile Memory
ETSI	European Telecommunications Standards Institute
EV	Electrical Vehicle
FMEA	Failure Mode Effective Analysis
FOTA	Firmware Over The Air
FPGA	Field Programmable Gate Array
Gateway	A VCU that connects multiple networks within a car
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
HMI	Human Machine Interface
HSM	Hardware Security Module
HW	Hardware
IC	Integrated Circuit
IoT	Internet-of-Things
IP	Intellectual Property
IPv6	Internet Protocol Version 6
ISE	Integrated SE
ISO	International Standardization Organization
IT	Information Technology
ITS	Intelligent Transport Systems
IVS	In-Vehicle System
JTC1	ISO/IEC Joint Technical Committee 1, Information Technology
LAN	Local Area Network
LIN	Local Interconnect Network
LTE	Long Term Evolution (4th generation Mobile Internet)
MAC	Media Access Control
MCU	Micro Controller Unit
M2M	Machine-to-Machine
NWI(P)	New Work Item (Proposal) in standardization
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
OS	Operating System
OTA	Over-The-Air
PDU	Protocol Data Unit
PHY	PHYsical Layer
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RSA	Asymmetric Encryption Algorithm developed by **R**ivest, Adi **S**hamir & Len **A**dleman
RSU	Roadside Unit
RTOS	Real Time Operating System
SC	Sub-Committee
SDO	Standardization Organization
SE	Secure Element
SIL	Safety Integrity Level
SSL	Secure Sockets Layer
SW	Software
TC	Technical Committee
TCB	Trusted Computing Base
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TR	Technical Report
TRL	Technology Readiness Level
TS	Technical Specification
UC	Use Case
UNECE	United Nations Economic Commission for Europe, UN Regulatory Body for road traffic
UNECE WP.29	World Forum for Harmonization of Vehicle Regulations
UWB	Ultra-Wide Band
VCU	Vehicle Control Unit
VDS	Vehicle and Driver Status
VPN	Virtual Private Network
V2X	Vehicle-to-X, where X stands for either Vehicle or Infrastructure
WAVE	Wireless Access in Vehicular Environments
WG	Working Group
WP	Work Package

1. Background to deliverable 1.7

Deliverable 1.7 (D1.7) is part of Task 1.3 and provides the final description of the demonstrators from the previously identified set of user-scenarios, by the Work Package (WP) contributors from partner organizations. The resources gathered in this task will be used as input in WP9 – Common Demonstrators.

This task aspires to translate the set of user-scenarios into demonstrators, making use of the various components identified in Task 1.2. The former showed to be of extreme importance because it presented meticulous detail on the description of concrete user-scenarios and Use Cases (UCs) prone to occur in real-life circumstances. It also paved the way for software and hardware development in order to guarantee the security, safety and privacy protection of a vehicle.

1.1 Use cases / user scenarios

In the early stages of the project a head-line list of possible user scenarios covering the crossroads of security, safety, and privacy protection was formed. This list was then completed with requirements on the CTEs, using reports provided by consortium partners from two tele-conferences and one workshop. Besides the tele-conferences and workshop, there were several skype meetings including partners on WP1. Of the initial list of six scenarios, two were extended with complementary sub-scenarios and in another scenario the scope was expanded. Another scenario was modified to include relevant threats. Also one new scenario was included. The final reference set of scenarios is presented below in Table 1 – Use Cases / User scenarios. Scenarios 1, 3, 4 and 6 are automotive related, scenario 2 is related to health, and scenario 5 is related to rail. For more information on the scenarios, please refer to SECREDAS Deliverable D1.2.

Table 1 – Use Cases / User scenarios.

Nr	Scenario	Sub-scenario nr	Sub- scenario's	Scenario owner	Partners contributing
1	Road intersection	**1.1**	An intersection with traffic lights is approached by a hijacked automated vehicle that has no intention to stop.	UNIMORE	CRF, Prove & Run, NXP-NL, AVL SF, HELM, TNO
		1.2	An automated vehicle approaches intersection which is equipped by a road-side system providing information about vulnerable road users.	UNIMORE	CRF, Prove & Run, NXP-NL, AVL SF, HELM, TNO
		1.3	A car approaches the intersection with current Operational C- ITS functions for green light for priority vehicles and GLOSA (Green Light Optimal Speed Advisor).	UNIMORE	TNO, AVL SF, HELM

		1.4	Emergency vehicle approaches a crowded intersection	UPB / UNIMORE	TNO
		1.5	Resilience of the vehicle's perception systems against false information about the traffic situation	MRTX	MRTX, UNIMORE
2	Vehicle with driver getting health problems	2.1	Health status assessment of a person and how health status can influence the ability to safely drive an (automated) car	PHILIPS	PHILIPS, Roche
		2.2	Driver Monitoring: how human-in-the-loop automated and connected vehicles can be securely preserved from external threats?	FICO- ADAS	FICO-ADAS, CSIC, INDRA, PHILIPS, TST, Roche
		2.3	Vehicle and driver status monitoring (incl. driver's health and wellbeing)	OULU	NOKIA-FI, SOLI, HALT
3	Keep car secure for the whole vehicle product life time	3.1	Vehicle updates are changes made to the hardware or software of a security, safety, or privacy relevant item that is deployed in the field	AVL-SF / ZF	Prove & Run, AIT, AVL SF, ZF, IMEC-NL, IOTR, TNO, Secinto, GUT
4	Advanced access to vehicle	4.1	Demonstrator is reflecting the trend for property (vehicle) sharing. The traveller orders a car in the target destination via cloud-based service.	IMA	GTO, Ubiqu, BUT, TST, IMEC-NL, CISC, Secinto
5	Rail	5.1	Show the technical feasibility of a virtualization approach using hypervisor technology. This approach will separate different safety critical applications and manage redundancy.	Thales	Thales, AIT, TUKL
6	Incident investigation	6.1	A critical situation is recognized, and it needs to be virtually reproduced and analysed.	ZF	ZF

Annex 1 provides detailed descriptions for each scenario.

1.2 Common Technology elements / UCs

In deliverable D1.3, Common Technology Elements (CTEs) were identified based on the UC scenarios to provide safety, security and privacy in a reusable manner. The defined CTEs must comprise the following characteristics:

- existing industrial proven technologies (TRL7 or higher);
- domain-independent elements applicable for "cross-domains";
- develop & validate several CTEs for the reference architecture;
- CTEs will be identified and further developed, supporting their domain specific implementation;

- expected Outcome: A list of CTEs and descriptions of the made adaptations, necessary to fulfil the requirements coming from different domains reducing development cost by 20%.

Task 1.2 has proven to be of great importance, because it provided descriptions of CTEs for the reference architecture and the exchange between different domains (See Figure 1 below), while identifying the interest of the partners on the various CTEs.

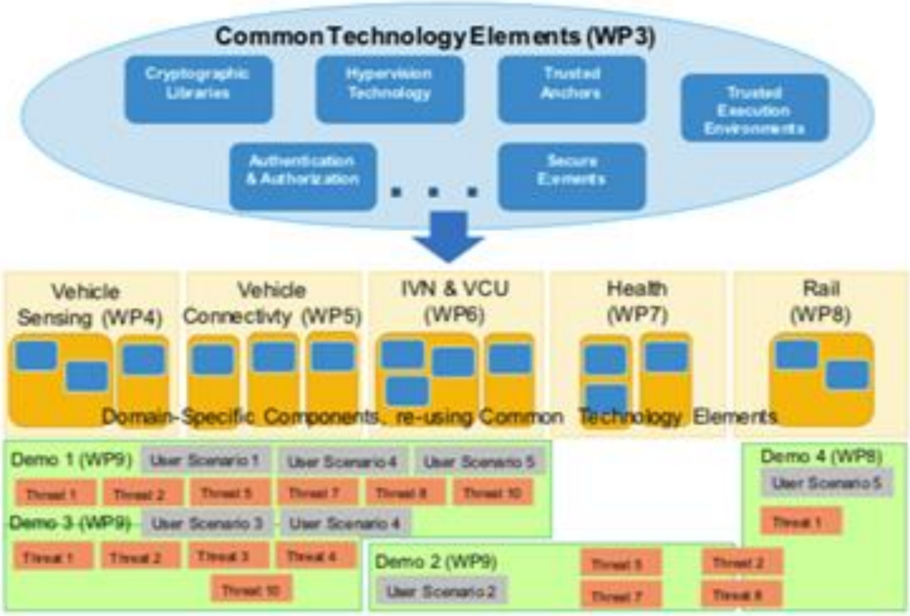


Figure 1 – Combination of generic and domain-specific components towards common demonstrators.

Deliverable D1.3 generated a number of inputs, as shown below in Table 2. The elements will be defined during the project by the responsible partner, in close cooperation with the involved partners in the CTEs.

Table 2 – Initial definition of CTEs and owners.

Nr.	Common technology Element	Owner	Use Cases	
			Mandatory	Optional
2.1	Key-Distribution Protocols	AIT	UC1, UC3, UC4	
2.2	Cryptography Libraries	AIT	UC3, UC5, UC6	UC1
2.3	Hypervision Technology	P&R	UC5	
2.4	Hardware Isolation Technologies	ZF	UC3	
2.5	Secure Elements	ZF	UC1. UC2, UC3, UC4, UC6	
2.6	Secure OS/Trusted execution Environment	P&R	UC3	
2.7	V2X Communication		UC1, UC2, UC3, UC4	

2.8	Authentication and Authorization	CEVT	UC1, UC2, UC3, UC4	
2.9	C-ITS services	CEVT	UC1	
2.10	Identity management	CISC-AT	UC2, UC4	UC1, UC3
2.11	Trusted Anchor		UC3	UC1
2.12	Firewalls	CEVT		UC3
2.13	Certificate Management			UC1, UC3
2.14	Security Testing Framework	FhG (IESE)	UC3	UC4
2.15	Differential Privacy	BME		
2.16	Transport-Layer Security	ZF	UC3, UC6	
2.17	OTA-Updates		UC3, UC4	
2.18	Long-Term Support	ZF	UC3, UC6	
2.19	Distributed Ledger Technologies	AIT		

As mentioned, Table 2 presents the initial inputs from deliverable D1.3 taken from the results of the scenarios to CTE mapping. However, the list was not final, and it did not provide a full description of current CTEs leaving some grey areas, which can generate problems when defining the next steps. Nevertheless, it is useful for identifying the application of components and the scenarios in which they will be used.

Then, with the help of D1.4 a more detailed table was created (Table 3). Where the overall CTEs requirements per UC are listed provide a clear overview of their impacts on safety, security and privacy aspects. Requirements on safety, security and privacy were also defined from the functional and technical points of view.

Table 3 – CTE´s requirements descriptions / use case.

Scenario / Use case Nr	CTE Nr	Partner	Requirement	Functional	Technical	Privacy	Security	Safety
UC1	2.1 Key-Distribution Protocols	UPB	Inter-vehicles trustworthy and privacy guaranteed communication resilient in crowded crossroads		x	x	x	

		UPB	Guarantee scalable PK-based AA procedures		x		x	
		UPB	Minimize PK certificate related operations costs (i.e. transfer, storage, signing/verification).		x	x	x	
	2.7 V2X Communication	TNO-IVS	C-ITS security deployed according to version (v1.3.1)	x		x	x	
			The vehicle gateway (OBU) should provide wireless and secure communication (e.g. ITS-G5, LTE) to various independent infrastructure services (cross-domain), users and the cloud		x	x	x	
			The user (VRU) should be identified by something he possesses, e.g. using smart devices like smartphone or wearables. On-board unit (OBU) in case of a vehicle.	x		x	x	
			The OBU (e.g. gateway device) should provide secure elements to store keys and sensitive user data.		x	X	x	
			User authentication and authorization will be provided by secure C-ITS services and/or by secure cloud services		x	x	x	
			The libraries should support the minimal set of cryptographic algorithms/functions from C-ITS security v1.3.1		x	x	x	
UC 2	2.5 Secure Elements	Philips	Secure data transmission from the sensor to ECU		x		x	
	2.7 V2X Communication		The vehicle gateway should provide wireless and secure communication to cloud services		x		x	
	2.8 Authentication and Authorization		User authentication and authorization will be provided by secure cloud services	x			x	
	2.10 Identity management		Only the user should be able to change privacy settings depending on the service he uses	x		x		

UC3	2.17 OTA-updates		The firmware or software of the vehicle's components should be able to be updated either remotely or locally in a secure and safe way.	x			x	x
	2.18 Long-term support		The vehicle system, hardware and software components should be able to handle new vulnerabilities and security incidents during product lifetime.	x			x	x
	2.1 Key-Distribution Protocols	Ubiqu	Dynamic security relationship between cloud, vehicles and users		x	x	x	
UC 4	2.5 Secure Elements	CISC	The developed hardware (e.g. gateway device) should provide secure elements to store keys and sensitive user data		x		x	
		Ubiqu	The developed hardware (e.g. vehicle opening device) should provide secure elements to store keys and sensitive user data and cloud gateway should provide a secure element to protect master keys		x		x	
	2.7 V2X Communication	CISC	The vehicle gateway should provide wireless and secure communication (e.g. NFC, BLE) to various independent infrastructure services (cross-domain), users and the cloud		x		x	
		Ubiqu	Phone and vehicle should provide wireless and secure communication (BLE)		x		x	
	2.8 Authentication and Authorization	CISC	The in-vehicle gateway should securely store permission tickets to authorize access to restricted areas like parking spaces.		x		x	
			User authentication and authorization will be provided by secure cloud services	x			x	
		IMEC-NL	User authentication and authorization based on distance bounding		x		x	
		Ubiqu	Offline access		x		x	
			API for authentication and authorization for 3rd party User authentication and authorization		x		x	

	2.10 Identity management	CISC	The user should be identified by something he possesses, e.g. using smart devices like smartphone or wearables.	x			x	
			The user should be able to change privacy settings depending on the service he uses	x		x		
			The user should be alerted when privacy settings are changing	x		x		
UC 5	2.2 Cryptography Libraries	THALES	The libraries should support state of the art cryptographic algorithms and the used key lengths should be considered secure for the long lifetime of railway applications (20+ years), cf. NIST SP 800-131A		x		x	
			Free/Libre and Open Source Software (FOSS) should be used in order to minimize development and life cycle costs and disclose potential vulnerabilities					
	2.3 Hypervision Technology	THALES	The Hypervisor should support scheduling modes that enable diversity of VM instances, e.g., scheduling VMs on different Hardware and/or at different times if required.		x			x
			The Hypervisor must not transparently withdraw resources from a running VM instance, i.e., swap it out of memory or live migrate it to another physical machine. If it needs to, the VM needs to be alerted.		x			x
			The Hypervisor should support strict partitioning of resources, e.g., it must not transparently deduplicate storage or memory and share the same physical resources between VMs		x			x
	2.11 Trusted Anchor	THALES	(CTE=VPN) Save connection certificates in a trusted platform module (TPM)		x		x	
			(CTE=VPN) Re-keying should be employed on a regular, frequent basis		x		x	

1.3 Security and privacy threats map to CTE

1.3.1 Top 10 automotive security and privacy threats

Table 4 below shows the initial compilation of top automotive security and privacy threats to be considered in the SECREDAS project. It is based on recent results of security research in the automotive domain. The table was taken from the original SECREDAS DoA.

Table 4 – Top automotive security and privacy threats to be considered in the SECREDAS project.

	Description
I	Attacks on backend server. An attacker can compromise a backend server and uses it to attack the connected cars. An attacker may launch a DoS attack on backend servers to disrupt their services. An attacker may target sensitive data at the server or information in other part of the cloud. For example, mobile apps are used to allow a user to query the status and control the car from his or her smartphone. Insecure APIs at the backend allow an attacker to interact with the car using falsified API requests[1].
II	Attacking a car using V2X communication channels. An attacker may spoof V2X messages, tamper with transmitted data or code, attack data integrity, exploit the trust relation, gain unauthorized access to data, jam the communication channel on the protocol or RF level, inject malware or malicious V2X messages. For example, non-secure protocols such as HTTP are sometimes used for V2X communications. Even when TLS/SSL is used, if the client software does not properly check the server certificate, an attacker can launch a Man-in-the-Middle attack to steal the user's credentials to further control the car[2].
III	Attacking a car by exploiting software update. An attacker may compromise the Over-the-Air (OTA) Updates or local and physical software update process, manipulate the software before the update process, or even compromise cryptographic keys to compromise code signing. For example, the 2014 Jeep Cherokee was remotely hacked by updating the Renesas V850 firmware to allow the compromised telematics unit to send messages directly to the ECUs on the CAN bus.
IV	Social engineering or exploits vulnerabilities and weaknesses introduced by human errors. An attacker may trick an owner, operator, or maintenance engineer to unintentionally install malware or change the setting to enable an attack. An attacker may also exploit errors in system configuration or usage.
V	Attacking a car's interfaces and functions for external connectivity. An attacker may access and manipulate functions designed to remotely operate systems or provide telematics data, short range wireless systems and sensors, and applications with poor software security. An attacker may also utilize physical interfaces such as USB or diagnostic port, or even media connected to the car as a point of attack. For example, connected cars rely on network devices with TCP/UDP ports to interact with outside world. Even the IP address of a connected car is protected by network separation provided by network operator, open ports and services with weak or no authentication pose security risks. An attacker can remotely scan and access the open ports and exploit the services as an entry point to the on-board system[3]. In addition, CAN can be accessed physically through OBD port, charging station, or a mechanic's computer[4].
VI	Attacks on in-vehicle network or software of on-board systems. An attacker may extract data and code, manipulate vehicle data, erase data and code, inject malware, inject or overwrite existing software, disrupt system operation, and manipulate vehicle parameters.
VII	Attacks that exploit security flaws in system design. An attacker may break the encryption due to insecure cryptographic design such as lack of encryption, weak key strength, or the use of deprecated cryptographic algorithms. Bugs in software and hardware may provide the attacker exploitable vulnerabilities and means of access or privilege escalation. Poor network design such as weakness in internet-facing ports and internal network separation also pose security risks. Crypto systems in the car should last for a long period of time. Lack of crypto agility, i.e. not being able to upgrade broken or obsolete cryptographic systems over time, may affect the whole security posture.
VIII	Attacks on privacy or data lost and leakage. V2X communication packets may contain identifiable information. Some of the information may be anonymized or pseudonymized. However, an attacker may still be able to intercept the V2X packets, footprint and track a car's movement in certain period and area and re-identify the user. Personal data may be transferred to third-party service providers in V2X communications. Sensitive data from cars may be lost or leaked due to physical damage, failure of IT components, or change of ownership.
IX	Physical manipulation of on-board systems to enable an attack. Manipulation of OEM hardware or adding unauthorized devices may enable a remote attack afterwards.

[1] Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs https://www.troyhunt.com/controlling-vehiclefeatures-of-nissan/

[2] Locate, unlocks, remote starts GM/Onstar cars https://www.youtube.com/watch?v=3olXUbS-prU&feature=youtu.be

[3] Remote Exploitation of an Unaltered Passenger Vehicle http://illmatics.com/Remote%20Car%20Hacking.pdf

[4] Comprehensive Experimental Analyses of Automotive Attack Surfaces http://www.autosec.org/pubs/cars-usenixsec2011.pdf

X	Attacks on sensors. Sensors for road safety and autonomous driving functions are subject to spoofing and jamming. It allows an attacker to disrupt the autonomous driving function

1.3.2 Mapped threats to CTEs

The goal from Task 1.2 has been to find suitable relations between the threats in the UC scenarios and CTEs that cover today's security and privacy threats. WP3 partners have provided t**Error! Reference source not found.** below, which helps UC owners to identify CTEs able to cover specific threats within the top ten of automotive security and privacy threats.

Table 5 – CTEs covered by each threat.

	Description	Sub-categories	CTEs
I	Comprise of back-end server	Server used to attack vehicle	Cryptography libraries, Secure OS/ Trusted Execution Environment (TEE), Authentication and Authorization, Identity Management, Differential Privacy, Transport-layer security, Long-Term Support
		Services from back-end server disrupted	
		Data leakage	
II	Communication channels used to attack a vehicle	Spoofing	Key distribution protocol, Cryptography libraries, Secure Elements, Secure OS/ Trusted Execution Environment (TEE), Authentication and Authorization, C-ITS Services, 3G/4G/5G Communication, Identity Management, Trusted anchor, Certificate Management, Transport-layer security, Differential Privacy, Long-term support
		Communication permits tampering with vehicle held code/data	
		Attack on integrity/ data trust	
		Information disclosure	
		Denial of service	
		Elevation of privileges	
		Virus infection	
		Message injection	
III	Update process used to attack a vehicle	Misuses of updates	Key distribution protocol, Cryptography libraries, Secure Elements, Secure OS/ Trusted Execution Environment (TEE), Trusted anchor, Certificate Management, Transport-layer security, Long-term support, Authentication and Authorization, C-ITS Services, Identity Management
		Denying updates	
IV	Human factor and social engineering	Human factor and social engineering	Cryptography libraries, Secure Elements, Secure OS/ Trusted Execution Environment (TEE), Identity Management, Trusted anchor, Certificate Management, Transport-layer security, Long-term support,
		Unintended actions	

V	Comprise of external connectivity	Vehicle functions using connectivity	Secure Elements, Secure OS/ Trusted Execution Environment (TEE), Authentication and Authorization, C-ITS Services, 3G/4G/5G Communication, Identity Management, Trusted Anchor, Certificate Management, Transport- layer Security, Long-Term support
		Vehicle functions using connectivity	
		External interfaces	
VI	Target on an attack on a vehicle	Extract data/code	Crypto libraries, Hardware isolation, Secure Element, TEE, Authentication/Authorization, 3G/4G/5G Communication, Identity Management, Trusted Anchor, Certificate Management, Transport-layer Security, Long-Term support
		Manipulate vehicle data	
		Erase data/code	
		Introduce malware	
		Introduce new software or overwrite existing SW	
		Disrupt systems or operations	
		Manipulate vehicle parameters	
VII	System design exploits (inadequate design and planning or lack of adaption)	Encryption	Key distribution protocol, Crypto libraries, Hardware isolation, Secure Element, TEE, Authentication/Authorization 3G/4G/5G Communication, Transport-layer Security, Long-Term support
		Early stage attack	
		SW and HW development	
		Network design	
VIII	Data loss from vehicle	Physical loss of data	Hardware isolation, Secure Element, TEE, Identity Management, Trusted Anchor, Certificate Management, Transport-layer Security, Long-Term support
		Unintended transfer of data	
IX	Physical manipulation of systems to enable an attack	Physical manipulation of system to enable an attack	Secure Element, TEE, Identity Management, Trusted Anchor, Certificate Management, Transport-layer Security, Long-Term support, Authentication/Authorization, Differential Privacy
X	Attack on sensors	Sensor spoofing - Spoofing of physical effects which are detectable by sensors e.g. radar signals	Will be provided in version 2 of deliverable D1.3.

2. Demonstrators

Deliverable D1.7 translates the information gathered from previous tasks in WP1 related to the user scenarios to the Common Demonstrators in WP9. WP9 will integrate and thus validate the distinct developments that have been conducted in all the other WPs. The demonstrators will be carried out to cover the key user scenarios from WP1. From original SECREDAS DoA, three different demonstrators will be conducted as outcome of WP9, as shown below. Based on this, the next chapter will provide a holistic description of each demonstrator.

DEMO I illustrates **Autonomous driving and infrastructure servers**.
This demonstrator will be conducted at designated experimentation locations in the Dutch City of Helmond and focusses on intersection crossing, which combines complexity of road users and Cooperative traffic control. The systems to be showcased in this demonstrator will have TRL5 to TRL 6 and include Automated vehicles, city surveillance, cybersecurity and V2X communications. The core demonstrator vehicle, owned and operated by TNO, will be an automated vehicle in motion at an actual (designated) road intersection in Helmond and equipped with sensors such as radar, lidar and video cameras in order to send secured information about the vehicle environment to the infrastructure.

DEMO II will address **Driver Monitoring Systems**.
This demonstrator will focus on the integration of Driver monitoring systems such as Drowsiness/Stress detection from FICO-ADAS and health assessment from PHILIPS. The systems composing inside the demonstrator are related to driver monitoring and cybersecurity with TRL2 to TRL4. Physiological data will be sent to a server secured by TST.
The demo will consist of two parts:

1. monitoring driver and secured transmission of the driver’s physiological data to an infrastructure server;
2. simulation of a cyberattack targeted at transmission of physiological data.

DEMO III will address **Cybersecurity and connectivity**.
The targeted systems for this demonstrator are all related to cybersecurity and connectivity. DEMO III is, in fact, comprised of a set of stand-alone single technology showcases, with no interaction between them. The demonstrations are at partner facilities under laboratory conditions. All individual demonstrations are centred around secure advanced access to a vehicle based on authentication, authorization and identity management. The demonstrator will show technologies that enable a car to be secure whilst user privacy is taken into the account.

Table 6 – Use case scenarios covered, and contributors for each demonstrator.

Demonstrator	Leader	Use case scenarios covered	Contributors

DEMO I – Autonomous Driving	TNO	**UC 1, 3, 6**	**Security:** AVL-AT, OTM, PDMFC, P&R, ITAV, AVL-SF, BeyondVision, STACK;
			Hardware: CISC, NXP, CRF, VIF;
			Software: TNO, CRF, PDMFC;
			OTA Updates: COMSOL, AVL-SF;
			Connectivity: FICO-AAA, MM, TNO, YGK, CMS, STACK;
			Others: TML, FICO-ADAS, HELM, CSIC, MRTX, NOKIA.

DEMO II – Driver Monitoring	FICO-ADAS	**UC 2**	**Security:** P&R, ROCHE, OTM, INDRA, BeyondVision, STACK;
			Authentication: BUT, OTM;
			Hardware: NXP, SEN;
			Connectivity: YGK, STACK;
			Others: PHILIPS, FICO-ADAS, PDMFC, TST, OULU, NOKIA, SOLI, HALT, CSIC.

DEMO III – Security and Privacy	IMA	**UC 3, 4**	**Security:** AIT, OTM, P&R, GTO, FhG, CMS, INDRA, UBIQU, BeyondVision, IMEC-NL;
			Connectivity: GTO, YGK, CMS, GUT, INDRA, IMA, TST, IMEC-NL;
			Software: AVL-AT, P&R, BUT, IMA;
			OTA Updates: AIT;
			Hardware: IMA, NXP.

3. Demonstrators holistic description: mapping scenarios, threats, and CTEs to demonstrators

In this chapter, we describe a holistic process which links each demonstrator covered in chapter 2 to user scenarios covered in chapter 1 of this document.

3.1 DEMO I - Autonomous driving and infrastructure servers:

For the first demonstrator, three images are shown because the demonstrator aims to cover three different scenarios at an intersection.

Scenario I

A cooperative road intersection is equipped with a Roadside Surveillance/Monitoring System to monitor traffic. The intersection has traffic lights supervised by a Traffic Management System. The intersection is approached by an automated vehicle which has been hijacked (and/or the C-ITS system has been attacked) in such a manner that it will not stop for a red signal at the intersection. Thanks to the supplementary information transmitted by the Roadside

Surveillance/Monitoring System, the traffic management system's operator will be able to react to this emergency by switching all traffic lights (all directions) to red, in parallel, surrounding automated vehicles will also be notified that a vehicle has been hijacked.

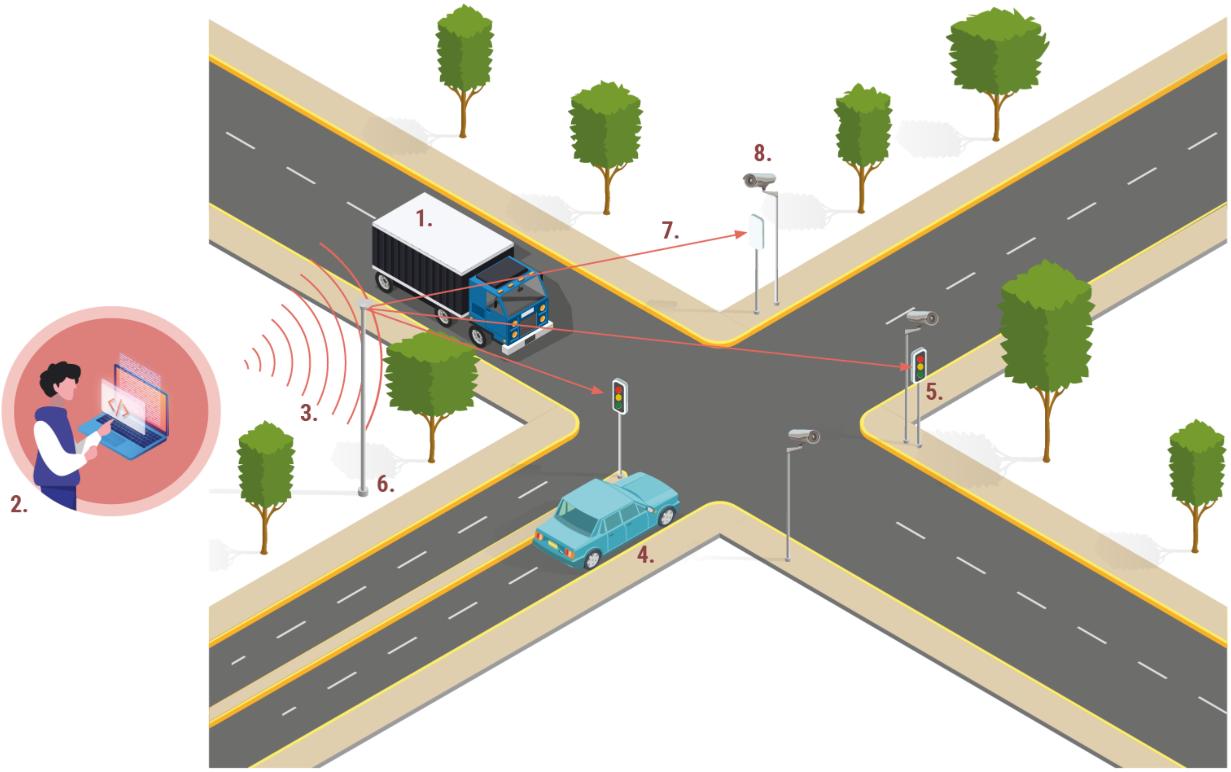


Figure 2 – Illustration of the first scenario of the demonstrator I.

Table 7 – Table with the legend of the first scenario of the demonstrator I to show each partner contribution.

Agent #	Components	Supplier	Description
1 – Hijacked Vehicle	V2X communication	MM	Participation in the translation of the innovative concepts at the basis of Vehicle Control Unit into a physical demonstrator
	LIDAR	AVL-SF	AVL-SF: SW - ADAS functionalities (sensor fusion) for future mobility concepts
	RADAR	IMEC, AVL-SF, ZF	IMEC: Continuous-wave radar at 79GHz design in cost- and power-efficient downscaled CMOS technology. AVL-SF: SW - ADAS functionalities (sensor fusion) for future mobility concepts ZF: ZF combines environmental sensors, such as camera and radar with central electronic control units in the vehicle.
	Other Sensors	AVL-SF	AVL-SF: SW - Develops ADAS functionalities (sensor fusion) for future mobility concepts

2 – Hacker	Computer / Software	Beyond Vision	Beyond Vision aims to provide test vectors generated using combinatorial testing methods to simulate cyber-attacks.
3 – V2X Communication	V2X communication	FICO-AAA	FICO-AAA will do the integration in a vehicle of the communication devices V2X/TCU-SCM/GW. FICOAAA can provide additionally Antennas set-up for GPS, Radio, and more if necessary.
	Encryption	NXP, ITAV, PDMFC	NXP: Investigate on Enhanced Encryption methods as wells as performant hardware for authentication to fulfil the requested performance and data throughput ITAV: Public-key and symmetric-key encryption schemes to provide such confidentiality through efficient encryption algorithms PFM: Secure radio communications including encryption
4 – Car	Car	TNO	TNO will provide a car with several sensors.
	LIDAR	AVL-SF	AVL-SF: SW - ADAS functionalities (sensor fusion) for future mobility concepts
	RADAR	AVL-SF	AVL-SF: SW - ADAS functionalities (sensor fusion) for future mobility concepts
	ADAS	AVL-SF	AVL-SF: SW – Sensor fusion for different sensors intended primarily for AD functionalities. Additionally, AVL-SF can contribute with a development of other parts of AD SW (e.g. environment interpretation, decision making, motion control, etc.)
	V2X communication	FICO-AAA, Indra	FICO-AAA: Please refer to point 3 of the present table. Indra: Intelligent Traffic Lights
	Front camera	MRTX, AVL-SF	MRTX: Hardware to collect frame by frame video footage of the situation in front of the vehicle AVL-SF: SW - ADAS functionalities (sensor fusion) for future mobility concepts
	Perception software	MRTX, AVL-SF	MRTX: Machine learning based software module to detect objects and agents in a given traffic situation AVL-SF: SW – mentioned in sections for various sensors and ADAS in general
6 – Road Control Unit	V2X communication	FICO-AAA, Indra	FICO-AAA: Please refer to point 3 of the present table. Indra: Refer to point 4 of this table.

7 – Road Control Unit Communication	Roadside Cameras	CRF	Network cameras and associated analytics for traffic analysis
	Authentication	ITAV	Pseudonym-based systems for privacy preserving authentication and message delivery with conditional privacy
8 – Roadside Video Surveillance	Interconnection	CRF	Design of the architecture of the interconnection between an infrastructure video surveillance system and the C-ITS entities
	Cameras	CRF	Network video surveillance cameras

Scenario II

An automated vehicle approaches an intersection without traffic lights but equipped with a Roadside Surveillance/Monitoring System with an enhanced Local Dynamic Map that can provides information about vulnerable road users. The vulnerable road users communicate their position and speed to Roadside Units via wearables to the road-side system (may include video surveillance system) close to the intersection, and to near cars. This information will be used by the automated car to cross the intersection without any safety risk for the vulnerable road users or need to adapt speed, hence preventing sudden stops.

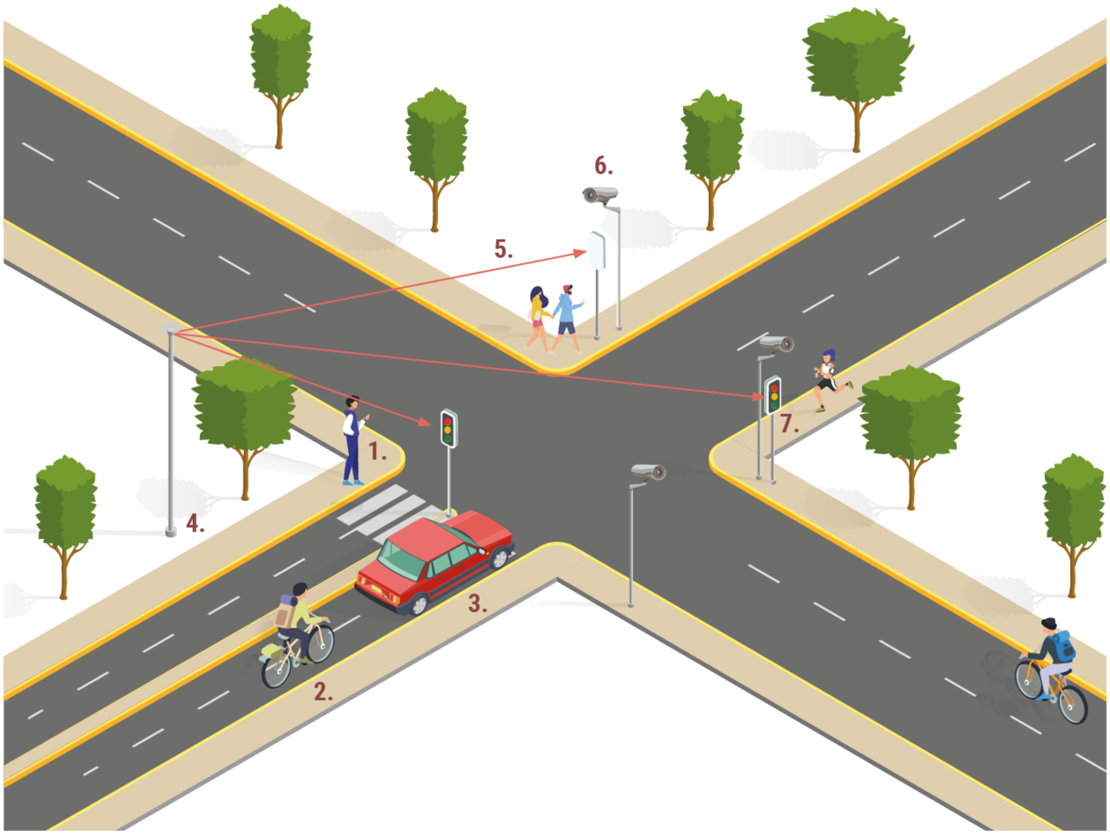


Figure 3 – Illustration of the second scenario of the demonstrator I.

Table 8 – Table with the legend of the second scenario of the demonstrator I to show each partner contribution.

Agent #	Components	Supplier	Description
3 – Car	Car	TNO	Refer to Table 7
	LIDAR	AVL-SF	AVL-SF: SW – Same as Scenario I. Refer to Table 7
	RADAR	AVL-SF	AVL-SF: SW – Same as Scenario I. Refer to Table 7
	ADAS	AVL-SF	AVL-SF: SW – Same as Scenario I. Refer to Table 7
	V2X communication	Indra	Intelligent Traffic Lights
4 – Road Control Unit	V2X communication	FICO-AAA	Refer to table 7.
5 – Road Control Unit Communication	Authentication	ITAV	Pseudonym-based systems for privacy preserving authentication and message delivery with conditional privacy
6 – Roadside Video Surveillance	Roadside Cameras	CRF	Network cameras and associated analytics for traffic analysis
7 – Traffic Lights	V2X communication	Indra	Intelligent Traffic Lights

Scenario III

A priority vehicle approaches an intersection with current Operation C-ITS functions for green light to priority vehicles and GLOSA (Green Light Optimal Speed Advisor). All other lanes receive a red signal to avoid collision.

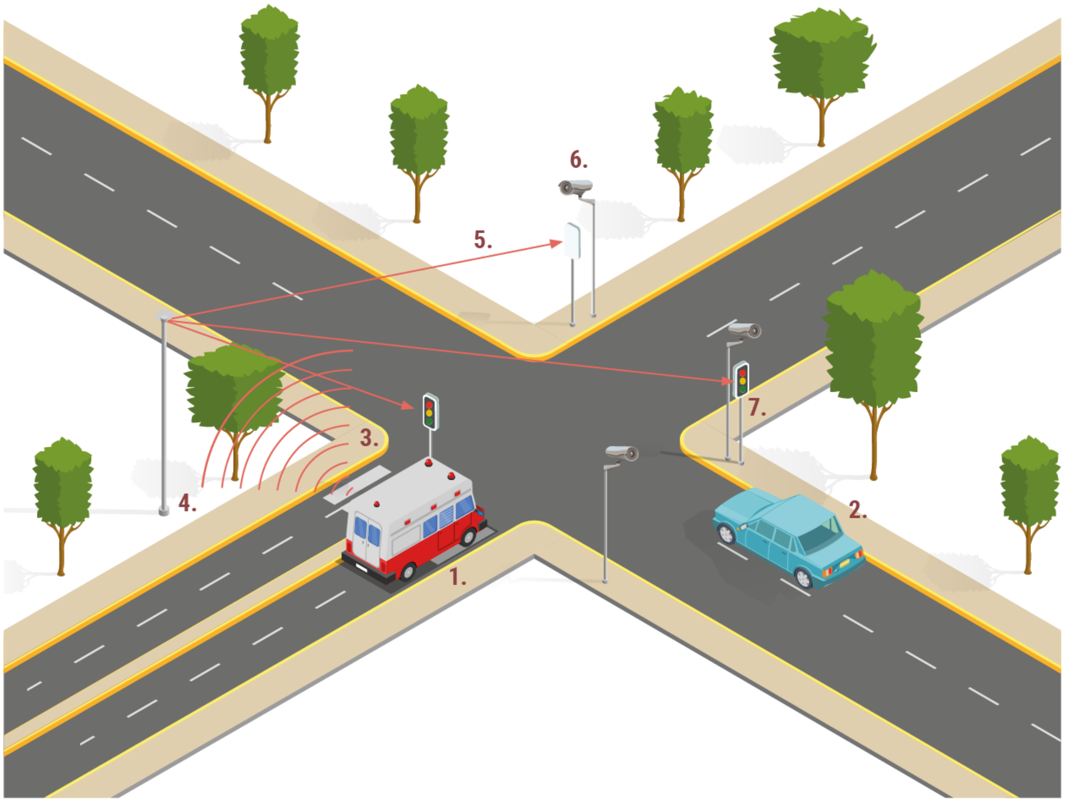


Figure 4 – Representation of the third scenario of the demonstrator I.

Table 9 – Table with the legend of the third scenario of the demonstrator I to show each partner contribution.

Agent #	Components	Supplier	Description
2 – Car	Car	TNO	Refer to Table 7
	LIDAR	AVL-SF	AVL-SF: SW – Same as Scenario I. Refer to Table 7
	RADAR	AVL-SF	AVL-SF: SW – Same as Scenario I. Refer to Table 7
	ADAS	AVL-SF	AVL-SF: SW – Same as Scenario I. Refer to Table 7
	V2X communication	FICO-AAA, Indra	FICO-AAA: Please refer to point 3 of the present table. Indra: Intelligent Traffic Lights
3 – V2X Communication	V2X communication	FICO-AAA	Refer to table 7.
4 – Road Control Unit	V2X communication	FICO-AAA	Refer to table 7.
5 – Road Control Unit Communication	Authentication	ITAV	Pseudonym-based systems for privacy preserving authentication and message delivery with conditional privacy

6 – Roadside Video Surveillance	Roadside Cameras	CRF	Network cameras and associated analytics for traffic analysis
7 – Traffic Lights	V2X communication	Indra	Intelligent Traffic Lights

PDMFC will cooperate with several partners to define the architecture and integration of all the vehicle subsystems through an architecture phase. Hardware and software connectivity will be identified, bus loads and control (perception-decision-actuation) loops delays evaluated and software integration layer developed to support decision making in the relevant computing unit. This integration software layer can contribute to data fusion and will abstract the hardware in order to develop portable decision-making software portable which can be used in various platforms.

Table 10 – Description of demonstrator 1

Demonstrator		
Demonstrator reference / owner / contact person	DEMO 1 - Autonomous Driving – TNO	
Context	Autonomous driving and infrastructure servers	
User scenarios reference	UC1	
Involved Common Technology elements	UC1	2.1 Key-Distribution Protocols
		2.7 V2X Communication
		others

Detailed Threats	Single or multiple attacks taking place in above scenario • One of the road users (that has been target of a cyber-attack aiming at hijacking an automated vehicle for criminal purposes) is ignoring the traffic light signals (and speed advice). This is detected thanks to the shared world model and mitigation measures are taken to control/stop the automated vehicle and/or traffic light and to alert other road users and authorities creating a safer situation and a more resilient system; • One of the road users (hacker) is spoofing the C-ITS system by injecting corrupted/tampered data (e.g. wrong location or speed) to the shared world model, but as SECREDAS system allows fast detection of such attack, all road participants at the intersection crossing are notified/warned of the cyberattack, the traffic lights controller is adjusted to mitigate the impact of the malicious data; • A hacker performs a DoS attack on the automated intersection crossing by means of overloading the V2X communication channel. This attack is detected by the SECREDAS system that will adjust the traffic lights controller to switch to conventional control mode (e.g. fixed durations of red-green periods). In case the road-side unit is hacked, it sends wrong/tampered information (e.g. GLOSA) to affect speed of vehicles present at intersection. The SECREDAS system also needs to detect this roadside unit attack and mitigate the impact on the intersection crossing; • Privacy attack: a hacker intercepts V2X messages in to track a given vehicle & re-identify the user; • One of the road users (hacker) is sending out false identification, i.e. pretending being an emergency vehicle and therefore creating disturbance to normal traffic flows at possibly critical instant (example: actual police car sent to an emergency scene attempting to cross the intersection and blocked by the disturbance); • Secure VM software to prevent vulnerabilities such as trojan, compatibility to legacy systems, information leakage and risk of virtualization sprawl.
Assumptions	The Traffic Management System is able to monitor the traffic in the intersection and all the communication with the infrastructure, as well as detect hijacked vehicles and monitor them; The Roadside Surveillance/Monitoring System is able to send traffic video analysis information to the Traffic Management System for the traffic management system operator to take measures to clear/close the intersection and to force hacked vehicle to stop; The Roadside Surveillance/Monitoring System is able to share traffic video analysis information with connected vehicles through Traffic Management System and Roadside Units located near the intersection; Each VRU has a wearable for data communication; All the actors are connected via at least one V2X technology; Untrusted network on cluster boundary;

Compliance needs	C-ITS standards;
	TCP/IP protocols between Roadside Surveillance/Monitoring System and Traffic Management System;
	IEC 62443 industrial network and system security.

Table 11 – Demonstrator 1 related to use cases and threats

Holistic description in Step-by-step execution.						
User Scenario	Threat	Threat subcategory	CTE	Holistic description of action	Validation process /Impact of non-validation	
UC1.1	2,6	Inject malicious V2X messages, spoofing, Manipulate vehicle data	Crypto libraries, Hardware isolation, TEE, Secure Element, Authentication/ Authorization, C-	A hacker can gain access and inject malicious code, steal important information, or even take control of the car.	The controlling units detect one car is anomalous and inform the others, while	If the attack is successful and goes unnoticed it can lead to a severe accident. Private data can be stolen from users.

			ITS services, V2X Communication, Identity Management, Trusted Anchor, Certificate Management, Transport-layer Security, Long-Term support.		taking security measures. Driver is informed about the attack and takes full control of the vehicle. Pedestrians are also informed that one car is being attacked.	
UC1.2	2	Spoofing	Key distribution protocol, Cryptography libraries, Authentication and Authorization, Identity Management.			
UC1.3	2	Communication permits tampering with vehicle held code/ data	Key distribution protocol, Cryptography libraries, Authentication and Authorization, Identity Management.			
UC1.4	2	Message injection	Key distribution protocol, Cryptography libraries, Authentication and Authorization, Identity Management.			
UC1.5	10	Sensor spoofing - Spoofing of physical effects which are detectable by sensors	Authentication and Authorization, Identity Management.	The intersection is populated with other vehicles and vulnerable users and is being approached by an automated vehicle. The perception system of the automated vehicle has been attacked in such a manner that it would obtain false information about the traffic situation at the road intersection (e.g. disregard red traffic light, disregard oncoming traffic, disregard vulnerable road users) and hence perform driving actions which endanger other road	The driver is informed about the attempted attack even if it is prevented, so that he can take over control if necessary	If the adversarial attack on the perception system is not detected, the driver is informed pre-emptively to intervene manually

				users at the intersection. Despite the attempted attacks on the perception stack, the software of the automated vehicle is able to pre-emptively detect the attacks and can be shown to be robust against the attempted attack. The automated vehicle continues to behave in a safe manner at the intersection		

3.2 DEMO II - Driver Monitoring Systems

In DEMO II, two systems will be extensively tested: one is from FICO-ADAS to detect drowsiness, and the other from PHILIPS to assess a driver’s health status. Data from the driver will be sent to/from wearables, to the car and to the road surveillance system. The encrypted data flow masquerades the user’s identity. This demonstrator will explore how personal health data can be safely and securely exploited in an in-car environment, and how ‘human-in-the-loop’ automated and connected vehicles can be securely protected against external threats.

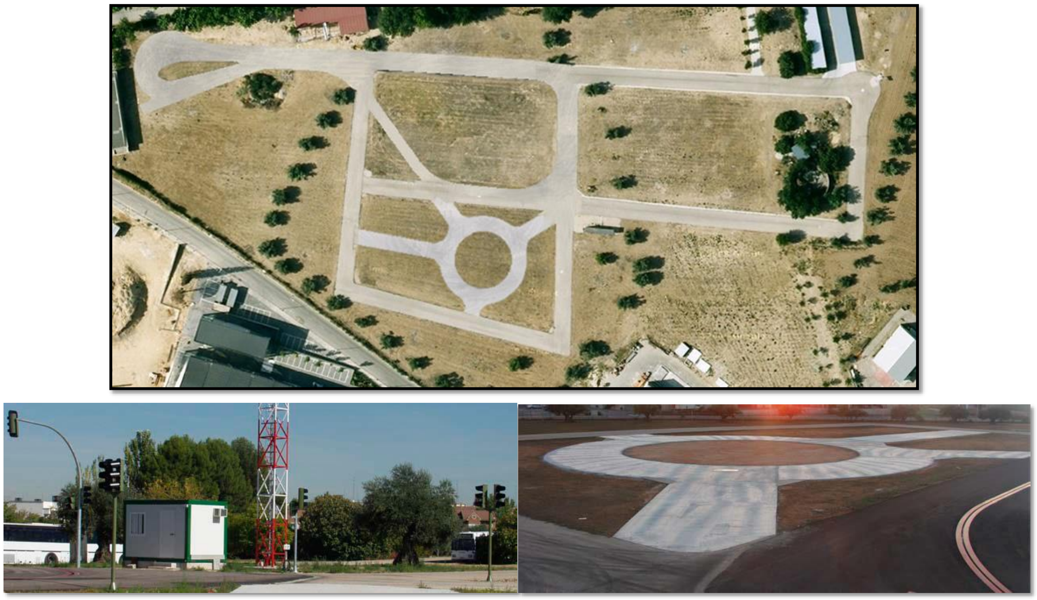


Figure 5 – CSIC Test track

The demonstrator will take place at CSIC premises (see Figure 5), where urban driving scenarios can be realistically reproduced. The demonstration will cover two different scenarios:

In the first one (**Health status Assessment**), an "enhanced cruise control" will use the personal health data to determine if a driver becomes sleepy or drowsy and intervene with the cruise control e.g. to keep longer distances with a preceding car and to take measures to increase the alertness of the driver. Furthermore, it will be explored what kind of security measures are needed when driver health problems are detected in the context of automated driving. It will be demonstrated that sensors and software unobtrusively measure vital signs of the driver and derive its health status from the driver.
Different technologies to measure vital signs will be evaluated: unobtrusive monitoring of heart rate, blood pressure, glucose levels and respiration rate, some can be detected by camera and by wearables, and their relation to the ability of the driver to drive healthy and safely. Health status assessment form the bases of driver performance management, which is a complex case because it requires assess to the driver's capability to take back control in the context of autonomous and semi-autonomous driving. Driver performance management is part of the wider domain of driver's health status assessment. On top of their relevance for driver performance assessment, these measures also serve as health markers timely indicating health issues.

In the second one (**Driver Monitoring**), two different Use Cases will be considered using a SAE L3 automated vehicle that will drive automatically following a route selected by the driver, simulating the circulation in a real urban environment. The vehicle (Citroën DS3, see Figure 10 and details just below the figure) will receive relevant information from a control centre which has a global view of the traffic and the environment conditions. This information will be sent via I2V communications, using the ETSI ITS-G5 / IEEE 802.11p communication standard to enable de deployment of Day 1 C-ITS services. These services will be deployed physically in the testing facilities, both installing intelligent RSUs or IoT/M2M devices in sensitive places and developing the corresponding back-end infrastructure. A cloud-based control centre would generate the traffic incidents and integrate the information collected from the road sensors and/or in the simulated events. In addition to that, the automated vehicle will be equipped with systems to obtain physiologic signals that will detect drowsiness and stress of the vehicle passenger. The relevant UCs are:

1. **UC2.2a L3 operation with road works**

The L3 system of the vehicle will be notified of road works ahead and will prevent the driver from taking control when approaching it. If the driver still prefers to supervise only (following the drowsiness level provided by the driver monitoring system), an L2 driving mode will be adopted. In that case, if the driving context does not allow to maintain the initial route, a global planner will be automatically used to find an alternative route. The system will then notify the driver, and the later will have to confirm the mission change. A hazardous location notification service (Road works warning) will be sent to the vehicle, then the vehicle will notify the driver. The notification will imply the need to take control over the car, in order to perform the route change.

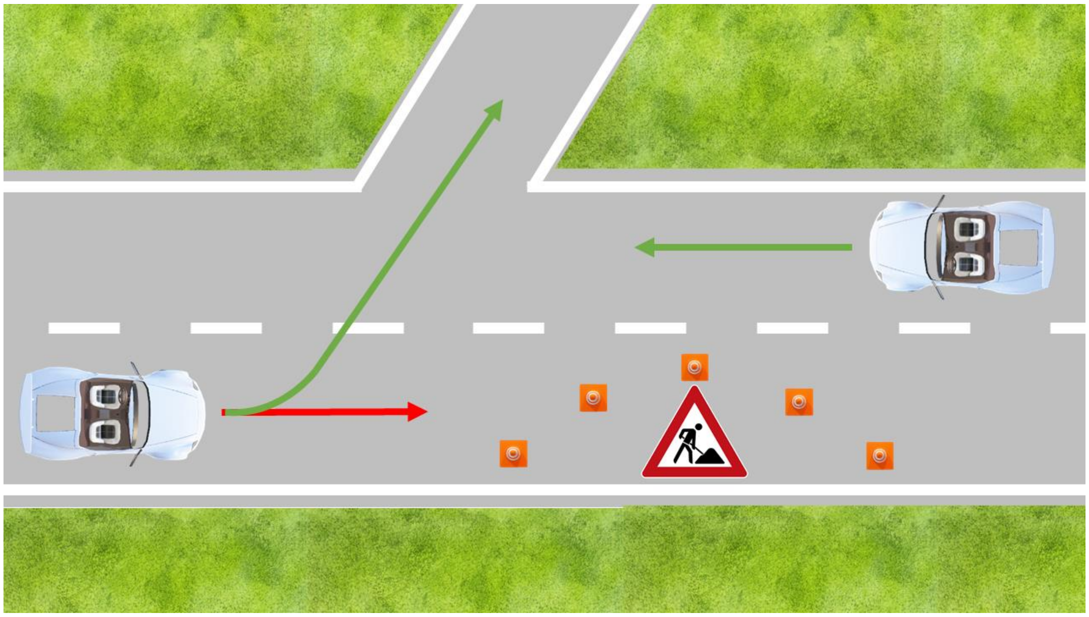


Figure 6 – Representation of UC 2.2a.

2. UC2.2b L3 operation with speed limits variation

The automated vehicle system is notified that a vehicle in front has stopped in the middle of the road. It location is transmitted and the automated vehicle system adapts its target speed following two C-ITS services (in-vehicle speed limits and slow/stationary vehicle). Before reaching the speed limit change zone, the driver is advised that a speed reduction must be applied and a closer supervision (L2) will be required. Depending on driver status, different intensity alarms will be produced.

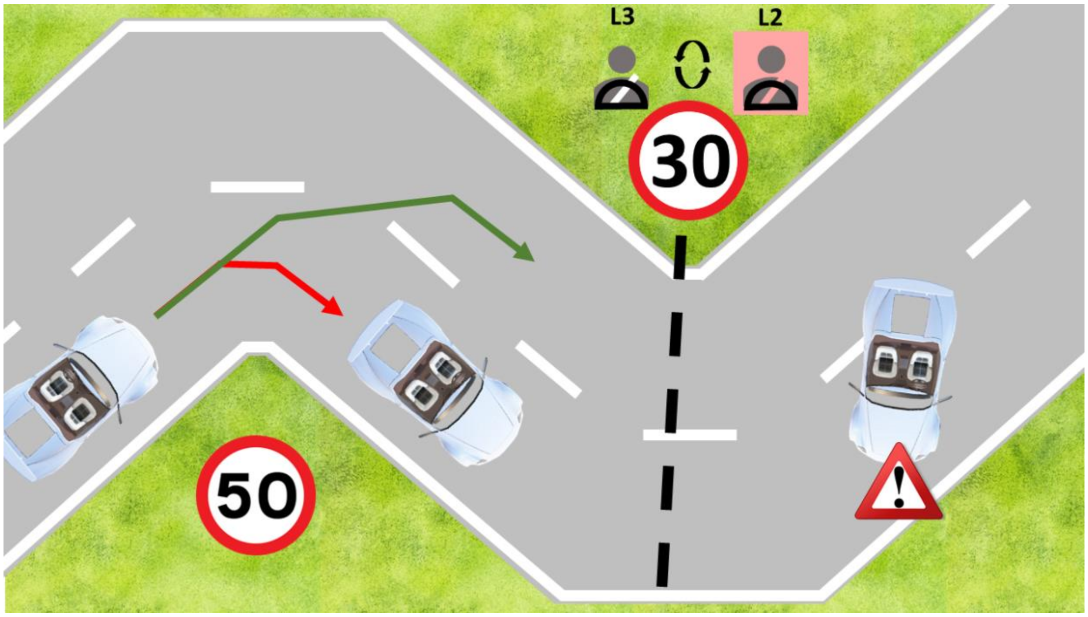


Figure 7 – Representation of UC 2.2b.

Figure 8 below shows some of the constituents needed for this demo.

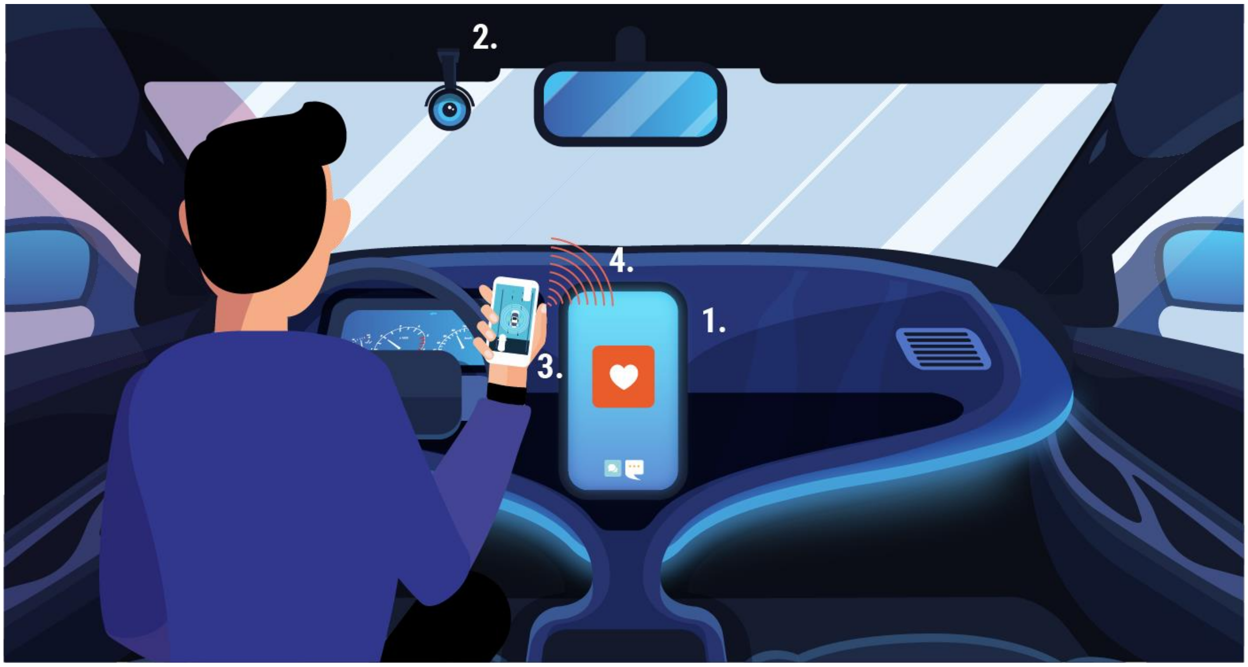


Figure 8 – Illustration of the demonstrator II and its constituents.

Table 12 - Table with the legend of the demonstrator II and each partner contribution.

Agent #	Components	Supplier	Description
1 – Car / Car Computer	Communication	Intel	NUC Intel (purchased)
	Car	CSIC	Please refer to Annex 2 (page **Error! Bookmark not defined.**)
	Testing tools	PDMFC	Automated virtual testing tools will be developed to test vehicle intelligence
2 – Detection Systems	Camera	FICOSA	Infrared camera
	Wristband	Philips	Wearable sensing technologies such as patches and watches for continuous and unobtrusive monitoring of people's physiology, health and behaviour. Improvement of comfort levels to allow for long-term monitoring during daily life
	Software	PDMFC	A procedure to evaluate drivers' condition
3 – Wearables/ Phone	Communication	Beyond Vision	Secure connection providing anonymized data to assess and evaluate the condition of the driver
	Interface	Philips	Refer to point 2, wristband section.
4 – Communication with Road Control Unit	V2X communication	INDRA	Infrastructure equipment such as RSUs, RADARs, intelligent traffic lights, VMSs, and HCC software and services
	Authentication	ITAV	Pseudonym-based systems for Privacy-preserving authentication

Table 13 – Description of demonstrator 2.

Demonstrator		
Demonstrator reference / owner / contact person	DEMO 2 - Autonomous Driving – FICO-ADAS	
Context	Driver Monitoring Systems	
User scenarios reference	UC2	
Involved Common Technology elements	UC2	2.5 Secure Elements
		2.7 V2X Communication
		2.8 Authentication and Authorization
		2.10 Identity management
Detailed Threats	Attacking the car using V2X communication channels, where attackers may spoof V2X messages, tamper with transmitted data or code, attack data integrity, exploit the trust relation, gain unauthorised access to data, jam the communication channel on the protocol or RF level, inject malware or malicious V2X messages; Attacks that exploit security flaws in the overall system design, breaking the encryption while transmitting personal and therefore sensitive information from/to the vehicle; Attacks on privacy or data lost and leakage in V2X communication, leading to data loose or leak. Indeed, Authentication measures should be perfect, so the driver does not get mixed up with someone else in the car; Collecting physiological parameters from the driver (e.g. blood pressure, pulse rate profile) requires privacy protection.	
Detailed requirements	There shall be a secure and unique set of keys to connect to every Vehicle Gateway and to the Driver Monitoring Gateway. The credentials stored on the Vehicle Gateway and in the Driver Monitoring Gateway shall be difficult to extract or transfer to another one. A series of mechanisms to prevent tampering of the firmware shall be implemented on the Vehicle Gateway (secure boot, FW encryption, FW signature), along with some others to prevent remote code execution. In addition, in the Control Centre and in the Drive Monitoring Gateway some mechanisms to prevent spoofing shall be implemented. Furthermore, TLS shall be used for the communication channel between the Vehicle Gateway and the Control Centre.	
Assumptions	Prospective assessment of aptness of the person to drive a car based on health assessment outcome is sufficiently accurate to be actionable by the vehicle; The cyber threat may give false information to the autonomous and semiautonomous systems in order to cause an accident; Sleep quality affects readiness on the following work period. Heart rate is related to attention. Environment quality (temperature, oxygen/carbon dioxide, etc.) affect both driver's readiness and passengers' comfort. Resource use affects the need of maintenance and more generally logistics. A longer route could be faster (e.g. in winter conditions a recently ploughed route could be faster and safer even if longer) (road case).	

Table 14 – Demonstrator 2 related to use cases and threats

Holistic description in Step-by-step execution.						
User Scenario	Threat	Threat subcategory	CTE	Holistic description of action	Validation process /Impact of non-validation	
UC2.1	2	Spoofing, communication permits tampering with vehicle held code/data, attack on integrity/ data trust, elevation of privileges	Key distribution protocol, Cryptography libraries, Secure Elements, Secure OS/ Trusted Execution Environment (TEE), Authentication and Authorization, C-ITS Services, 3G/4G/5G Communication, Identity Management, Trusted anchor, Certificate Management, Transport-layer security, Differential Privacy, Long-term support	1. Any communications between two parties (e.g. wearable, vehicle, cloud) happen over a secure channel (encrypted payload and authenticated identity). 2. PINs, passwords, passphrases vulnerable to dictionary/brute force attacks are rejected. 3. Authentication and other sensitive logic is run inside Trusted Execution Environments (TEE)	1. Only HTTPS and Bluetooth connections equal to and higher than 4.2 are supported. 2. New PINs, passwords, passphrases are validated based on NIST, OWASP guidelines. 3. Only signed code runs on the chain from secure bootloader to execution of authentication and other sensitive logic.	1. For Bluetooth devices version 4.0 and 4.1 an HTTPS implementation over Bluetooth is supported. 2. A secure Bluetooth connection is accepted only when its needed and actively ended if not needed anymore. Biometric measures are supported as alternative where available. 3. If a TEE implementation is not available, respective logic is run inside virtualized guest OS initiated by a securely booted VMM.
UC2.2	7	Encryption, SW and HW development, network design	Key distribution protocol, Crypto libraries, Hardware isolation, Secure Element, TEE, Authentication/ Authorization, 3G/4G/5G Communication, Transport-layer Security, Long-Term support	1. Develop rules for consistency / feasibility checks to check for atypical communication / operations. 2. Automated consistency / feasibility checks are applied by network watchdogs to network traffic and by log intelligence systems to log entries to detect atypical communication / operations. 3. After alerting human operators to atypical communication /	1. While developing rules for these checks make use of redundant information in message payloads, feasible number of messages, average values plus some standard deviation and possible value ranges for data as well as metadata attributes. 2. Train an AI model employing	1. In case some values are not available to use in checks use other values which are available. 2. Where an AI model is not feasible, use statistical methods. 3. Where a cut-off from communication is not feasible other respective actors are instructed to ignore communication from suspected malicious actor.

				operations and receiving confirmation from them, respective network traffic is interrupted, and other mitigation actions are taken.	aforementioned rules for typical attack scenarios and deploy this model on the network watchdogs and log intelligence systems. 3. Suspected malicious actors are cut off from communication.	
UC2.3	1, 2	Data leakage, attack on integrity/ data trust	Cryptography libraries, Secure OS/ Trusted Execution Environment (TEE), Authentication and Authorization, 3G/4G/5G Communication, Identity Management, Transport-layer security, Differential Privacy, Long-term support	1. Automatically anonymize / pseudonymize PII / PHI (Personally Identifying Information / Protected Health Information) content during communication 2. Automatically encrypt PII/PHI content during data storage 3. Design-in robust defences against re-linking using differential privacy, privacy budget and other techniques.	1. All PII/PHI are identified during development and respective automated anonymization / pseudonymization features are implemented. 2. All PII/PHI are identified during development and respective encrypted storage features are implemented. 3. All attributes which could be used for re-linking are identified and designed with protective measures to guard against this.	1. Employ periodic privacy penetration testing to identify further PII/PHI not initially identified. 2. If encrypted storage is not feasible fallback to reversible pseudonymization. 3. Employ periodic privacy penetration testing focused on re-linking attacks to identify if all needed attributes are identified and if the protective measures work as intended.

3.3 DEMO III - Cybersecurity and connectivity

The secure car access system (CAS) demonstrator will demonstrate the V2X communication and will employ SECREDAS-developed components. Secure identification of drivers and vehicles into an already existing large infrastructure will be demonstrated. This scenario aims to meet the needs of Tier 1 automotive suppliers in search of advanced access to the vehicle & on-request V2X identification, which follows the trend for vehicle sharing.

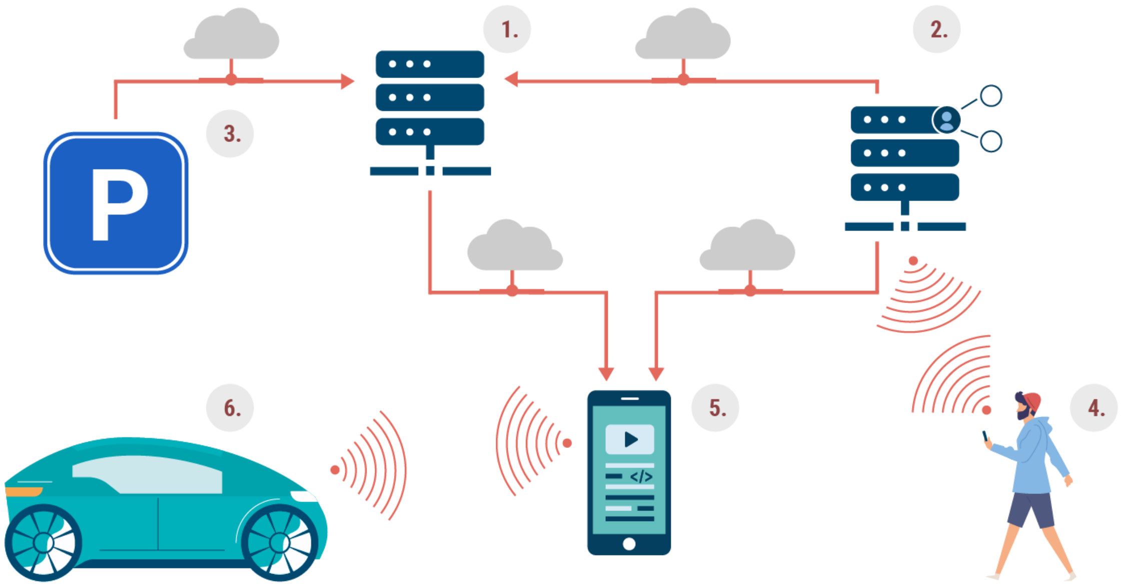


Figure 9 – Illustration of the demonstrator III and its constituents.

Table 15 – Table with the legend of the demonstrator III image and a description of the required components.

Agent #	Components	Description
1 – Car Sharing Web Server	Authentication	AAA server (authentication, authorization, and accounting)
	Communication	Communication interfaces (HTTPS, REST API): Web Browser (User credentials), Mobile App (Car Location), Identity Management (Authorization)
	Database	Vehicle database
2 – Identity Management Server	Communication	Communication interfaces (HTTPS, REST API): Web Server, Mobile App, Parking &Payment
	Database	User Credential Database

3 – Parking/Payment Management Server	Communication	Payment Status information exchange (HTTPS), Parking Barrier Control
	Parking/Payment Control system	Payment handling, Control of barrier
4 – Client Browser/App	Communication	Communication interface (HTTPS, REST API) – Authentication process, Client data transfer
	Interface	Car Sharing Web user interface
5 – Car Sharing Mobile App	Communication	Communication interface (HTTPS, REST API, NFC, BLE): Car location info, Authorization Credentials transfer, Access Rights Update Package transfer
	Secure storage	Secure storage of credentials
6 – Car	Communication	Communication interfaces (NFC, BLE) – Access Rights Update Package reception, Authorization Credential reception, Parking Barrier Unlock Data
	Access Reader	Access Reader with BLE/NFC functionality
	ACU	Access Control Unit

Table 16 – Description of demonstrator 3.

Demonstrator		
Demonstrator reference / owner / contact person	DEMO 3 - Security and Privacy – IMA	
Context	Cybersecurity and connectivity	
User scenarios reference	UC3, UC4	
Involved Common Technology elements	UC3	2.1 Key Distribution Protocol
		2.2 Cryptography Libraries
		2.5 Secure Elements
		2.6 Secure OS/ Trusted Execution Environment (TEE)
		2.8 Authentication and Authorization
		2.11 Trusted Anchor
		2.12 Firewalls
		2.16 Transport-Layer Security
		2.17 OTA-Updates

	UC4	2.5 Secure Elements
		2.7 V2X Communication
		2.8 Authentication and Authorization
		2.10 Identity management
Detailed Threats	Attack surface is the open ports/services and APIs of the on-board system and the backend system (attacks to bypass access control and authentication mechanisms), as well as the communication link that connects the backend system to the on-board telematics unit (MITM attacks). The attacker attacks weakest link in the OTA update process and injects malicious software into the update; Non-secure communication protocol or improper server certificate check; No or weak encryption. Sensitive data related to users and manufactures must be properly protected; No or weak protection of in-vehicle network; User identification through V2X communication; Spoofing identity of the user; Tampering with data in transfer; Attacks on privacy or data lost and leakage. Privacy of the car user must be guaranteed during the authentication process in order to prevent leakage of personal data; Denial of services. The vehicle is in a remote offline location. Note: Detailed Threat Analysis is part of deliverable D1.2.	
Detailed requirements	The service must not be denied even if the car is parked in remote location with no connectivity therefore encrypted authorization update package has to be delivered to the car by the authorized user as part of the User-Car Access reader interaction. Non-repudiation at all steps must be guaranteed as well as user privacy (e.g. identity and location).	
Assumptions	OEM backend server is a trusted environment; The link between OEM and Gateway, and the link between key-bearing device and reader are untrusted; Gateway is secured against remote and local attacks; In-vehicle communication is a trusted environment.	
Compliance needs	UNECE, "Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD".	

Table 17 – Demonstrator 3 related to use cases and threats.

Holistic description in Step-by-step execution.						
User Scenario	Threat	Threat subcategory	CTE	Holistic description of action	Validation process /Impact of non-validation	
UC3.1	1, 3	Server used to attack vehicle, misuses of updates, Denying updates	Key distribution protocol, Cryptography libraries, Secure OS/ Trusted Execution Environment (TEE),	1. Develop a methodical process to test the communications between servers and vehicle, as well as servers and human.	1. While developing the process it is also important to understand what kind of data it is possible to	1. In case of some data gets available to attackers, encryption should be used to preserve security and privacy

			Authentication and Authorization, Identity Management, Differential Privacy, Transport-layer security, Long-Term Support, Identity Management	2. Alerts for every time an update is denied, or any kind of intrusion is detected. 3. Develop procedures to ensure that updates are regularly done, and sometimes brute force them.	intercept. Then evaluate if the data does not expose information 2. Generate a log data for the updates. This can show how some fails or errors happened. If the problem is related to a hole in the software.	
UC4.1	7	Encryption, network design	Key distribution protocol, Crypto libraries, Hardware isolation, Secure Element, TEE, Authentication/ Authorization, 3G/4G/5G Communication, Transport-layer Security, Long-Term support	1. Develop rules for consistency / feasibility checks (sanitation layer) to check for atypical operations. 2. Automated consistency / feasibility checks are applied to all data incoming from non-trusted environment, log entries to record non-standard operations. 3. Alerting human (or AI] operators to atypical behaviour and assure that mitigation actions are taken. 4.Develop procedures for cyclic evaluation of strength of cryptographic primitives used to assure use of to prevent reliance on outdated security.	1. While developing rules for these checks make use of inherent redundant information in message payloads and contextual information. 2. Generate log data for typical use scenarios, attack scenarios and make this log data available for user training and AI training. 3. Develop list of primitives used during development and validate that the used ones are recommended for future use.	1. In case some values are not available to use in checks use other resiliency principles where possible. 2. Where an AI model is not feasible, use statistical methods. 3. Primitives that cannot be updated are likely to become threats in the future due their possible obsolescence.

4. Conclusions on deliverable 1.7

This document presents the final approaches of each individual partner on each demonstrator, while blending the demonstrators with the impact of each CTE. There will be three main demonstrators, whereby the first demonstrator is divided in three sub-scenarios to enrich the spectrum of SECREDAS' tests.

The result of D1.7 is a combination of CTE mapping with UCs applied to demonstrators. The document will help several WP leaders, especially the WP3 leader, to define their work with regard to meeting WP9 requirements.

Several issues were identified during the development of this deliverable, which explains the delay in its delivery:

- defining each partner's contribution in relation to each demonstration proved to be a difficult and time-consuming task, because some partners' works cover a wide range of areas;
- several deliverables prior to D1.7 were delayed; that made it difficult to gather the necessary information to write this deliverable.

List of Figures

Figure 1 – Combination of generic and domain-specific components towards common demonstrators. 8
Figure 2 – Illustration of the first scenario of the demonstrator I. 18
Figure 3 – Illustration of the second scenario of the demonstrator I. 20
Figure 4 – Representation of the third scenario of the demonstrator I. 22
Figure 5 – CSIC Test track 26
Figure 6 – Representation of UC 2.2a. 28
Figure 7 – Representation of UC 2.2b. 28
Figure 8 – Illustration of the demonstrator II and its constituents. 29
Figure 9 – Illustration of the demonstrator III and its constituents. 33
Figure 10 - CSIC’s automated vehicle: Sensors and equipment. 58
Figure 11 – Photographs of the possible interactions between the car, traffic lights, GPS and V2X communication. 59
Figure 12 - Hardware and software components around LCM. 60

List of Tables

Table 1 – Use Cases / User scenarios. 6
Table 2 – Initial definition of CTEs and owners. 8
Table 3 – CTE´s requirements descriptions / use case. 9
Table 4 – Top automotive security and privacy threats to be considered in the SECREDAS project. 13
Table 5 – CTEs covered by each threat. 14
Table 6 – Use case scenarios covered, and contributors for each demonstrator. 17
Table 7 – Table with the legend of the first scenario of the demonstrator I to show each partner contribution. 18
Table 8 – Table with the legend of the second scenario of the demonstrator I to show each partner contribution.. 21
Table 9 – Table with the legend of the third scenario of the demonstrator I to show each partner contribution. 22
Table 10 – Description of demonstrator 1 23
Table 11 – Demonstrator 1 related to use cases and threats 24
Table 12 - Table with the legend of the demonstrator II and each partner contribution. 29
Table 13 – Description of demonstrator 2. 30
Table 14 – Demonstrator 2 related to use cases and threats 31
Table 15 – Table with the legend of the demonstrator III and each partner contribution. 33
Table 16 – Description of demonstrator 3. 34
Table 17 – Demonstrator 3 related to use cases and threats. 35
Table 18 TRL - Technology readiness level 39

Terminology

Table 18 – TRL – Technology readiness level

TRL nr.	Description
1	Basic principles observed
2	Technology concept formulated
3	Experimental proof of concept
4	Technology validated in lab
5	Technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
6	Technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
7	System prototype demonstration in operational environment
8	System complete and qualified
9	Actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

References

Project webpage, http://www.secredas.eu
D1.2: Deliverable Title, SECREDAS Project deliverable, 2018

ANNEX 1 – Use case scenario's description

Scenario 1 detailed description

Scenario description 1.1

Scenario	
Context	Road intersection
Owner / Contact person	TNO, UNIMORE
Description of defining behaviour	A cooperative road intersection is equipped with a Roadside Surveillance/Monitoring System to monitor its traffic. The intersection which has traffic lights supervised by Traffic Management System, is being approached by an automated vehicle, this vehicle has been hijacked (and/or the C-ITS system has been attacked) in such a manner that it will not stop for red sign traffic light at the intersection. Thanks to the supplementary information transmitted by the Roadside Surveillance/Monitoring System, the traffic management system's operator will be able to react to this emergency situation by switching all traffic lights (all directions) to red, while the hijacked vehicle might be remotely forced to stop by action from traffic management system operator. In parallel surrounding automated vehicles will also receive this supplementary information.
Actors / stakeholders	1. Automated vehicle (hacking target) and its driver; 2. Hacker; 3. Other vehicles and their drivers; 4. Traffic Management System and its service operator; 5. Roadside Surveillance/Monitoring System and its service operator.
Infrastructure – system components and connections	1. Vehicles have capabilities to communicate with the roadside infrastructure (V2X); 2. Traffic Lights Controller has communication interfaces with Traffic Management System; 3. Traffic Management System has IP network interface with Roadside Surveillance/Monitoring System and controls multiple Traffic Light Controller close to the intersection; 4. Roadside Surveillance/Monitoring System has IP network interface with Traffic Management System; 5. Roadside Unit have capabilities to communicate with vehicles (V2X).

Step-by-step execution	Step I: The hijacked automated vehicle approaches the intersection and the traffic lights just switched to red. At the same time other vehicles, from other direction starts crossing the intersection. Each vehicle communicates its position, heading and speed via V2X messages to other vehicles and to the Roadside Units. The Roadside Surveillance/Monitoring System continuously monitors traffic of vehicles at the intersection. Step II: The hijacked automated vehicle sends misleading information in V2X messages to other vehicles and Roadside Unit at the intersection (telling that it is slowing down) but continues driving at high speed approaching the intersection maximizing probability of collision. Step III: The Roadside Surveillance/Monitoring System transmits video analysis results information to the Traffic Management System such as (hijacked) vehicle actual speed, which differs from wrong speed information broadcast in V2X messages from the hijacked vehicle. Traffic Management System thanks to information received from Roadside Surveillance/Monitoring System, is able to detect a mismatch with hacked vehicle's V2X messages. Traffic management system operator will identify an emergency situation and in turn, instructs other vehicles intersection to stop crossing the intersection and will initiate a request toward the traffic light controller to switch all lights to red. Step IV: Traffic lights are switched to red for all roads to block all traffic at the intersection. All vehicles get a V2X notification to clear the intersection if engaged or wait by the red traffic light. Step V(optional): The hijacked automated vehicle is also remotely instructed to stop by the Traffic Management System.
Data flow	During all steps(I-V), all vehicles transmit their position, heading, and speed information through V2X messages to the Roadside Units toward the Traffic Management System. Traffic Management System at intersection communicate GLOSA information to the vehicles through the Roadside Units. Step III: The Roadside Surveillance/Monitoring System transmits traffic video analysis information to Traffic Management System for the operator to initiate requests to all vehicles to force them to clear the intersection. It also sends object detection location and speed information to all vehicles. Step IV: Traffic Light Controller at intersection communicates with the Traffic Management System to confirm that all lights are switched to red. Step V: The Traffic Management System transmits request to stop to the hijacked vehicle.
Assumptions	The Traffic Management System is able to detect misalignment between the information transmitted by the hijacked vehicles and its current mobility status. The Roadside Surveillance/Monitoring System is able to send traffic video analysis information to the Traffic Management System for the traffic management system operator to take measures to clear/close the intersection and to force hacked vehicle to stop. The Roadside Surveillance/Monitoring System is able to share traffic video analysis information with connected vehicles through Traffic Management System and Roadside Units located near the intersection.
Compliance needs	C-ITS standards, TCP/IP protocols between Roadside Surveillance/Monitoring System and Traffic Management System.
Preferred method for Security/Privacy/Safety Analysis	

Relevant threats	Single or multiple attacks taking place in above scenario 1. One of the road users (that has been target of a cyber-attack aiming at hijacking an automated vehicle for criminal purposes) is ignoring the traffic light signals (and speed advice). This is detected thanks to the shared world model and mitigation measures are taken to control/stop the automated vehicle and/or traffic light and to alert other road users and authorities creating a safer situation and a more resilient system. 2. One of the road users (hacker) is spoofing the C-ITS system by injecting corrupted/tampered data (e.g. wrong location or speed) to the shared world model, but as SECREDAS system allows fast detection of such attack, all road participants at the intersection crossing are notified/warned of the cyberattack, the traffic lights controller is adjusted to mitigate the impact of the malicious data. 3. A hacker performs a DoS attack on the automated intersection crossing by means of overloading the V2X communication channel. This attack is detected by the SECREDAS system that will adjust the traffic lights controller to switch to conventional control mode (e.g. fixed durations of red-green periods). In case the road-side unit is hacked, it sends wrong/tampered information (e.g. GLOSA) to affect speed of vehicles present at intersection. The SECREDAS system also needs to detect this roadside unit attack and mitigate the impact on the intersection crossing. 4. Privacy attack: a hacker intercepts V2X messages in to track a given vehicle & re-identify the user.
Additional information	Linked to demo 1.1 The C-ITS intersection utilizes the enhanced Local Dynamic Map for traffic anomaly detection. The intersection with traffic lights is approached by a hijacked automated vehicle whose control has been taken over remotely by hacker with possibly theft objectives or worst, with terrorist purposes. Thanks to road-side video surveillance sourced information exchanged with the automated vehicles own sensing bringing more reliable traffic situation assessment, the SECREDAS system is able to detect that the vehicle has no intention to stop. The SECREDAS system reacts to the attack detection by initiating commands toward the traffic light controller, switching traffic lights in all other directions to red, in parallel the system automatically alerts first responders, police forces and city authorities, while the automated vehicle might be remotely forced to stop. Privacy preservation will also be ensured by integrating privacy preserving authentication schemes into the road safety and traffic monitoring communication protocol.

Scenario description 1.2

Scenario	
Context	Road intersection
Owner / Contact person	TNO, UNIMORE
Description of defining behaviour	An automated vehicle, that has been hijacked, approaches an intersection without traffic lights, which is equipped by a Roadside Surveillance/Monitoring System providing information about vulnerable road users. The vulnerable road users communicate their position and speed to Roadside Units close to the intersection and the Traffic Management System will use this information.
Actors / stakeholders	1. Automated vehicle (hacking target) and its driver; 2. Hacker; 3. Other vehicles and their drivers; 4. Vulnerable Road Users (VRUs)(e.g. pedestrians, cyclists, etc.); 5. Traffic Management System and its service operator; 6. Roadside Surveillance/Monitoring System and its service operator (ex: city police).
Infrastructure – system components and connections	1. Vehicles have capabilities to communicate with the roadside infrastructure (V2X); 2. Vulnerable Road Users have wearables with communication interfaces with infrastructure (V2P interface); 3. Traffic Management System has IP network interface with Roadside Surveillance/Monitoring System; 4. Roadside Surveillance/Monitoring System has IP network interface with Traffic Management System; 5. Roadside Unit has capabilities to communicate with vehicles (V2X) and with the wearables of the VRUs (V2P interfaces).
Step-by-step execution	Step I: The hijacked automated vehicle approaches the intersection. At the same time, other traffic including Vulnerable Road Users at the intersection start crossing the intersection. All vehicles and Vulnerable Road Users communicate their position, heading and speed via V2X to the Roadside Units. The Road-side Surveillance/Monitoring System monitors all road participants at the intersection all the time. Step II: The hijacked automated vehicle sends malicious information to the intersection (telling that it is slowing down) but continues driving at a high speed approaching the intersection. Step III: The Roadside Surveillance/Monitoring System transmits video analysis results information to the Traffic Management System such as (hijacked) vehicle actual speed, which differs from wrong speed information broadcast in V2X messages from the hijacked vehicle. Traffic Management System thanks to information received from Roadside Surveillance/Monitoring System, is able to detect a mismatch with hacked vehicle’s V2X messages. Traffic management system operator will identify an emergency situation and in turn, instructs intersection road users (including Vulnerable Road Users) to stop crossing the intersection and will initiate a request toward the traffic light controller to switch all lights to red. Step IV: All road users get a notification to clear the intersection. The hijacked automated vehicle might also be instructed to stop automatically.

Data flow	During all steps, all road users transmit their position, heading, and speed through V2X messages, to the infrastructure toward the Traffic Management System. Step III: Roadside Surveillance/Monitoring System transmits traffic video analysis information to Traffic Management System for the operator to initiate requests toward the intersection to force all vehicles to clear the intersection. The Traffic Management Systems sends warning information to all vehicles and Vulnerable Road Users. Step IV: The other road users reply to the request to clear the intersection. The Traffic Management System sends request to stop to the hijacked vehicle.
Assumptions	The Roadside Surveillance/Monitoring System is able to send traffic video analysis information to the Traffic Management System. The Vulnerable Road Users send their position to the Traffic Management System.
Compliance needs	C-ITS standards
Relevant threats	Single or multiple attacks taking place in above scenario 1. One of the road users (that has been target of a cyber-attack aiming at hijacking a vehicle for criminal purposes such as theft of goods or life-threatening action) is ignoring the slow down request from the surveillance system. This is detected thanks to the shared world model and mitigation measures are taken to control/stop the vehicle and to alert other road users and authorities creating a safer situation and a more resilient system. 2. One of the road users (hacker) is spoofing the C-ITS system by injecting corrupted/tampered data (e.g. wrong location or speed) to the shared world model, but as SECREDAS system allows fast detection of such attack, all other road users at the intersection are notified/warned of the cyberattack. 3. Detection of DoS attack on all V2X communication links by SECREDAS system will notify all road participants. 4. Privacy attack: a hacker intercepts V2X messages in to track a given vehicle & re-identify the user. 5. One of the road users (hacker) is sending out false identification, i.e. pretending being an emergency vehicle and therefore creating disturbance to normal traffic flows at possibly critical instant (example: actual police car sent to an emergency scene attempting to cross the intersection and blocked by the disturbance).
Additional information	Linked to demo 1.2 An automated vehicle approaches the C-ITS intersection while the enhanced Local Dynamic Map is providing information about Vulnerable Road Users. The Vulnerable Road Users communicate their position and speed via wearables to the vehicles and to the road-side system (optionally including the video surveillance system of previous scenario). The automated vehicle can cross the intersection without any safety risk for the vulnerable road users or need to adapt speed, hence preventing sudden stops.

Scenario description 1.3

Scenario	
Context	Road intersection
Owner / Contact person	TNO, UNIMORE

Description of defining behaviour	A vehicle approaches the intersection with current Operational C-ITS functions for green light for priority vehicles and GLOSA (Green Light Optimal Speed Advisor).
Actors / stakeholders	1. Automated vehicle and its driver; 2. Hacker; 3. Other (automated) vehicles and their drivers; 4. Traffic Management System and its service operator; 5. Roadside Surveillance/Monitoring System and its service operator (ex: city local police).
Infrastructure – system components and connections	1. Vehicles have capabilities to communicate with the roadside infrastructure (V2X); 2. Traffic Light Controller has communication interfaces with Traffic Management System; 3. Traffic Management System has IP network interface with Roadside Surveillance/Monitoring System, controls multiple traffic lights close to the intersection and V2X communication interfaces with road users; 4. Roadside Units have capabilities to communicate with vehicles (V2X); 5. Road-side Surveillance/Monitoring System is connected via IP network interface to the Traffic Management System.
Step-by-step execution	Step I: All vehicles approach the intersection and use the GLOSA information to stop for red light and continue driving for green light. Step II: The Roadside Unit is hacked and sends wrong/malicious information to the automated vehicles. The Traffic Management System will get informed by the Roadside Surveillance/Monitoring System or the Automated connected vehicle that notifies the situation. Traffic Management System will try to send notification/warning messages to the vehicles at the intersection and change the Traffic Lights to a fault mode to warn the drivers of the vehicles. Step III: The automated vehicles receive the warnings and react to that(e.g. give back control to driver). Step IV: The Roadside Surveillance/Monitoring System ensures that the traffic lights are switched to flashing yellow, informs the Traffic Management System to warn the drivers of the vehicles that the traffic light system is not working properly
Data flow	During all steps(I-IV) all road users communicate their position, heading and speed through V2X messages to the infrastructure toward the Traffic Management System. The Traffic Light Controller at intersection sends GLOSA information to the vehicles through the Roadside Unit. The Roadside Surveillance/Monitoring System monitors all traffic approaching and crossing the intersection. Traffic Light Controller at intersection communicates GLOSA information to the vehicles through the Roadside Unit. Step II: The Roadside Surveillance/Monitoring System sends warning information to the Traffic Management System. Step III: The Traffic Management System unit switches the traffics lights to flashing yellow and disables the GLOSA information.
Assumptions	The Roadside Surveillance/Monitoring system is able to send traffic video analysis information to the Traffic Management System to take measures to clear/close the intersection. The Roadside Surveillance/Monitoring System is able to share traffic video analysis information with connected vehicles through Traffic Management System and Roadside Units located near the intersection.

Compliance needs	C-ITS standards
Relevant threats	Single or multiple attacks taking place in above scenario 1. One of the Roadside Units has been hacked. 2. One of the road users (hacker) is spoofing the C-ITS system by injecting corrupted/tampered data (e.g. wrong location or speed) to the shared world model, but as SECREDAS system allows fast detection of such attack, all people at the intersection crossings are notified/warned of the cyberattack, the traffic lights controller is adjusted to mitigate the impact of the malicious data. 3. Detection of DoS attack on all V2X communication links by SECREDAS system will adjust the traffic lights controller to switch to conventional control (e.g. fixed durations of red-green periods). Roadside unit is hacked and sends wrong/tampered information (e.g. GLOSA) to affect speed of vehicles present at intersection. 4. Privacy attack: a hacker intercepts V2X messages in to track a given vehicle & re-identify the user.
Additional information	Linked to Demo 1.3 A vehicle approaches the intersection with current Operational C-ITS functions for green light for priority vehicles and GLOSA (Green Light Optimal Speed Advisor)

Scenario description 1.4

Scenario	
Context	At the headquarter of some city emergency service (e.g. ambulance, firefighters, police) the vehicle intervention has been initiated to address an emergency. The vehicle has to pass several crossroads with(out) (smart) traffic lights controllers. Obviously, reaching the destination with a minimum delay is crucial for the rescue effectiveness. The emergency vehicles have in-vehicle signage warning system that automatically switches on and warns the Traffic Management System via the Roadside Unit.
Owner / Contact person	UPB, TNO, UNIMORE
Description of defining behaviour	This scenario focuses on the moment when the emergency vehicle approaches an intersection including vulnerable road users besides other vehicles. Safely approaching the intersection with minimum delay requires from the part of emergency vehicle to demand priority over the other vehicles. This priority request could will be done directly via in-vehicle signage system installed on vehicles and traffic light control system, if in place.
Actors / stakeholders	1. Emergency Vehicle and its driver and (optional)emergency service client; 2. Vehicle and their drivers; 3. VRUs set (e.g. pedestrians, cyclists, etc.); 4. Traffic Management System and its service operator; 5. Roadside Surveillance/Monitoring System and its service operator; 6. In-vehicle signage system.

Infrastructure – system components and connections	1. Vehicles have communication interface with infrastructure (V2I, V2V, V2P interfaces); 2. In-vehicle signage system receives the communication from Roadside Units and/or the other vehicles; 3. Traffic Lights Controller has communication interfaces with intersection participants and (optionally) with emergency vehicle; 4. Traffic optimization service has communication interfaces with the intersection sensors and monitors and with emergency vehicle; 5. Vehicle and with city's Traffic Management Systems.
Step-by-step execution	Step 1(optional). On leaving emergency services headquarter for a new mission. Step 2(optional). The emergency assistance service might compute the optimal (minimum delay) path to the current intervention's place and shows the result and the city's map on display of the driver. Step 3. While the emergency vehicle approaches the intersection, the in-vehicle signage system initiates traffic lights command procedure. In the case of directly interaction the vehicle should a priori authenticate mutually with traffic lights control system. Step 4. Traffic lights control system investigates the how to switch regulate the intersection and switches on green lights on the optimal path of the emergency vehicle. Step 5. The appropriate vehicles and VRUs receive notification signal about the imminent presence of an emergency vehicle and consequently driving to the side of road. Step 6. The emergency vehicle crosses the intersection. Step 7. Continuation of the regular control scheme.
Data flow	All data are transferred over the interfaces securely and privacy protected, relying on legacy technologies. Interface I (emergency service client – emergency assistance service): authentication credentials, current position. Interface II (traffic lights control system – traffic management system): city's intersection profiles and real-time loading data, traffic control commands. Interface III (traffic management system – emergency vehicle): authentication credentials and authorization data, shuffles a given destination (location) data and the optimal path as a vector data (in return), traffic control commands. Interface IV (traffic lights control system – vehicles): notification data for in-vehicle signage. Interface V (vehicle -vehicle): notification data for in-vehicle signage.
Assumptions	• The actors are connected via at least one V2X technology (DSRC, 4G/5G, etc.); • Each VRU has a wearable for data communication; • All data communications are secured using legacy technologies (not tailored to vehicles domain); • All the actions should be achieved over a malicious environment. • The surveillance system can monitor the traffic in the intersection and all the communication with the infrastructure
Compliance needs	C-ITS standards

Preferred method for Security/Privacy/Safety Analysis	HEAVENS, NIST 800-30, NIST 800-37, NIST 800 –122, OCTAVE
Relevant threats	• Theft of intersection pre-emption service (road traffic priority) through traffic lights control system takeover by forging commands and/or spoofing emergency vehicle or emergency assistance service client; • Traffic disturbance/jamming by forging emergency warning messages; • Loss of privacy for intersection's traffic participants (e.g. driver tracking, location); • DoS attack on the intersection systems.

Scenario description 1.5

Scenario	
Context	Road intersection
Owner / Contact person	Merantix
Description of defining behaviour	The intersection is populated with other vehicles and vulnerable users and is being approached by an automated vehicle. The perception system of the automated vehicle has been attacked in such a manner that it would obtain false information about the traffic situation at the road intersection (e.g. disregard red traffic light, disregard oncoming traffic, disregard vulnerable road users) and hence perform driving actions which endanger other road users at the intersection. Despite the attempted attacks on the perception stack, the software of the automated vehicle is able to pre-emptively detect the attacks and can be shown to be robust against the attempted attack. The automated vehicle continues to behave in a safe manner at the intersection
Actors / stakeholders	1. Automated vehicle including parallel robust perception functions (hacking target) and its driver; 2. Hacker / Attacker; 3. Other vehicles and their drivers; 4. Vulnerable road users.
Infrastructure – system components and connections	Automated vehicle uses robust perception software as part of its automation functions.
Step-by-step execution	Step I: The attacked automated vehicle approaches the intersection with other vehicles and vulnerable road units, the traffic lights on the automated vehicle's lane are switched to red. At the same time other vehicles, from other direction starts crossing the intersection. Step II: The attacker has manipulated road signs and or traffic light appearance as well as directly attacked the perception function of the automated vehicle. As a result, the attacked automated vehicle would correctly recognize and locate other agents at the intersection not reduce its own speed approaching the intersection, maximizing probability of collision. Step III: The robust perception software running in the automated vehicle detects the attempted attack and demonstrates that it has not been affected by the adversarial attacks. The vehicle hence continues processes information which result in safe controls. Step IV: The automated vehicle stops at the red light of the intersection without endangering any other road users. The vehicle furthermore records the attempted attack.
Data flow	During all steps(I-IV), the automated vehicle only uses its internal, onboard perception system. Additional communication to other road users or infrastructure is not required.

Assumptions	The hacker is able to directly attack the sensors and software of the automated vehicle, as well as to manipulate traffic infrastructure such as road signs and/or traffic lights. The perception software is able to detect an attempted attack. The perception software is able to mitigate the attempted attack and pass on correct road information to the vehicle planning and control systems in real time.
Relevant threats	1. Automated vehicle does not recognize the attempted attack on time and hence does endangers other road users at the intersection through malicious controls; 2. Despite detecting an attempted attack/manipulation, the perception system of the automated vehicle is not able to process enough correct information about the situation at the intersection in order to produce safe planning and control outputs; 3. One of the road users behaves in a highly unpredictable way, which under normal circumstances would not have been a threat, but now in addition with the attempted attack causes the perception software of the automated vehicle to fail and process wrongful / incomplete information.

Scenario 2 detailed description

Scenario description 2.1

Scenario	
Context	Health status assessment of a person and how health status can influence the ability to safely drive an (automated) car.
Owner / Contact person	PHILIPS
Description of defining behaviour	Health status assessment • Unobtrusive monitoring of vital signs and other health parameters in daily life circumstances; • Prospective estimation of the ability of persons to drive a car safely from their health parameters, e.g. an appraisal when drivers are becoming sleepy or drowsy; • Safe and secure exploitation of this data in an in-car environment. An 'enhanced cruise control' could use this personal data e.g. to adapt distances to a preceding car to anticipated driver drowsiness level and/or to take measures to increase driver alertness.
Actors / stakeholders	Person owning a car; Wearables for unobtrusive vital signs monitoring; Communication infrastructure; Cloud; Vehicle.
Infrastructure – system components and connections	Wearables are worn by person owning a car; Wearables communicate directly or indirectly to the Cloud; Vehicles communicate to the Cloud; In-vehicle availability of health / driver aptness parameters.
Step-by-step execution	1. Person wears wearable on a daily basis; 2. Data from wearable is uploaded to cloud on a regular basis; 3. Person’s health is assessed from data collected from wearable; 4. Prospective assessment of aptness of the person to drive a car based on health assessment outcome; 5. Cloud makes fitness-to-drive data available to vehicle; 6. Vehicle downloads fitness-to-drive from cloud and makes it available to its sub-systems.
Data flow	See step-by-step execution.

Assumptions	Prospective assessment of aptness of the person to drive a car based on health assessment outcome is sufficiently accurate to be actionable by the vehicle.
Preferred method for Security/Privacy/Safety Analysis	ISO/SAE 21434
Relevant threats	Threat 2: Attacking the car using V2X communication channels, where attackers may spoof V2X messages, tamper with transmitted data or code, attack data integrity, exploit the trust relation, gain unauthorised access to data, jam the communication channel on the protocol or RF level, inject malware or malicious V2X messages. Threat 7: Attacks that exploit security flaws in the overall system design, breaking the encryption while transmitting personal and therefore sensitive information from/to the vehicle. Threat 8: Attacks on privacy or data lost and leakage in V2X communication, leading to data loose or leak. Indeed, Authentication measures should be perfect, so the driver does not get mixed up with someone else in the car.
Additional information	The use case is linked to Personal Health demonstrator of WP7 and to Demo IIb Health Status Assessment.

Scenario description 2.2

Scenario	
Context	Automated car with driver getting health problems / enhanced cruise control.
Owner / Contact person	FICOS-ADAS
Description of defining behaviour	Driver Monitoring: how human-in-the-loop automated and connected vehicles can be securely preserved from external threats? An automated vehicle is receiving relevant information from a control centre via I2V communication. In addition to that, the automated vehicle is equipped with systems to obtain physiologic signals from the driver.

Actors / stakeholders	Infrastructure;
	Cloud;
	Vehicle;
	Driver;
	Cyber threat.

Infrastructure – system components and connections	1. Unobtrusive systems to obtain physiological signals; 2. Connectivity to cloud-based control centre; 3. Secure communication with gateway.
Step-by-step execution	1. Information from the infrastructure arrives to the vehicle gateway; 2. If this package of information is trusted the information enters in the system; 3. If this package of information is not trusted, the system detects a cyber-threat and close all gateway; 4. Autonomous and semiautonomous systems need to stop working; 5. First the system checks the status of the driver; 6. If the driver is apt to drive, then the autonomous and semi-autonomous systems can stop working.

Data flow	1. Package of information goes from the infrastructure to the vehicle gateway; 2. The origin of the package is analysed; 3. If trusted the information goes thru the gate way; 4. If not, the information is blocked and cyber-threat protocol is activated. 5. Status of the driver is analysed in order to return him the control of the vehicle in a safe way; 6. The autonomous and semiautonomous systems are shut down for security reasons.
Assumptions	The cyber threat may give false information to the autonomous and semiautonomous systems in order to cause an accident.
Preferred method for Security/Privacy/Safety Analysis	ISO/SAE 21434
Relevant threats	Threat 2: Attacking the car using V2X communication channels, where attackers may spoof V2X messages, tamper with transmitted data or code, attack data integrity, exploit the trust relation, gain unauthorised access to data, jam the communication channel on the protocol or RF level, inject malware or malicious V2X messages. Threat 7: Attacks that exploit security flaws in the overall system design, breaking the encryption while transmitting personal and therefore sensitive information from/to the vehicle. Threat 8: Attacks on privacy or data lost and leakage in V2X communication, leading to data loose or leak. Indeed, Authentication measures should be perfect, so the driver does not get mixed up with someone else in the car.
Additional information	Linked to Demo 2.2 -an L3 automated vehicle will drive automatically following a route selected by the driver, simulating the circulation in a real urban environment. The vehicle (Citroën DS3, see Fig. 2) will receive relevant information from a control centre, which has a global view of the traffic and the environment conditions. This information will be sent via I2V communications, using the ETSI ITS-G5 / IEEE 802.11p communication standard to enable the deployment of Day 1 C-ITS services, namely hazardous location notifications (Road works warning) and signage applications (In-vehicle speed limits). While the speed limit will be integrated in the corresponding longitudinal control of the vehicle, the road works notification will make the automated system to notify the driver the need to take over control sufficiently in advance. These two services will be deployed physically in the testing facilities, both installing intelligent RSUs or IoT/M2M devices in sensitive places and developing the corresponding back-end infrastructure. A cloud-based control centre would generate the traffic incidents, integrating the information collected from the road sensors and/or simulating the events. In addition to that, the automated vehicle will be equipped with two systems to obtain physiologic signals that allows to detect drowsiness and stress: Camera-based pattern recognition and Depth Sensing with Kinect Sensor.

Scenario description 2.3

Scenario	
Context	Automated car with driver getting health problems / enhanced cruise control: Driver's and vehicle's status monitoring (incl. driver's health and wellbeing).
Owner / Contact person	NOKIA-FI, SOLI, HALT, OULU
Description of defining behaviour	Make effectively, safely and securely inference about the readiness of the driver and of the vehicle. Inference on the current well-being and health status of the driver, in order to assess their capability to safely perform their tasks. Trust in the sensors will also be assessed.

Actors / stakeholders	Driver;
	Vehicle;
	Cloud, service;
	Railway asset operator.

Infrastructure – system components and connections	A number of sensors, both unobtrusive wearables and in-vehicle, will be used as data source. Decisions (metrics) will be inferred based on those data. Remote monitoring will be provided to enable services (e.g. maintenance). The decision-making system could provide its output metrics, through additional system blocks, to the actuators envisaged in Scenario(s) 2, but this part will not be covered in this scenario.
Step-by-step execution	1. Physiological direct and inferred metrics (hearth rate, sleep quality, etc.) about the driver are collected before the driving task; 2. Passengers enter the vehicle; 3. Driver enters the vehicle and engages in driving tasks; 4. Systems collects off-line measurements and starts collecting on-line measurements (pulse rate profile, blood pressure, other physiological sensors; infrared sensors, temperature, carbon dioxide, other environmental sensors possibly including seat, toilet, etc. use; driving time); 5. System collects external information (open data, etc.); 6. Readiness of the driver is continuously evaluated and decision metrics are generated and properly routed; 7. Readiness of the vehicle is continuously evaluated and decision metrics are generated and properly routed; 8. Trust of the involved sensors and system interfaces is continuously assessed, and proper signals are generated and routed; 9. All above metrics are collected by the system and presented remotely on a dashboard.
Data flow	TBD
Assumptions	Sleep quality affects readiness on the following work period. Heart rate is related to attention. Environment quality (temperature, oxygen/carbon dioxide, etc.) affect both driver's readiness and passengers' comfort. Resource use affects the need of maintenance and more generally logistics. A longer route could be faster (e.g. in winter conditions a recently ploughed route could be faster and safer even if longer) (road case).
Preferred method for Security/Privacy/Safety Analysis	TBD
Relevant threats	Threat: Collecting physiological parameters from the driver (e.g. blood pressure, pulse rate profile) requires privacy protection.
Additional information	Whilst the rail case is used for the description, the taken approach is generic so to make the results applicable as much as possible to both road and rail cases. This use case scenario is linked to Scenarios 2.1 (PHILIPS) and 2.2 (FICOS-ADAS). Actually, these scenarios could be seen as complementary: they address the same problem with a slightly different approach and using different sensors. Merging them or at least their results will be investigated as those will become more mature. Because of the rail being used for description, the work done in rail Scenario 5 (Thales) will be tracked to emphasise and exploit possible complementarities. The present use case scenario is linked to Demo II (Driver monitoring system). The demo will be realised as simulations or off-line data processing as well as actual prototyping. Testing details are TBD. Testing in a rail environment is under evaluation whether it could be possible with the contribution of other consortium partners. Alternatively, testing in real rail vehicles or emulated conditions in private road area (OuluZone) will be considered. As a possible implementation of step 5, a drone, equipped with sensors, sending data to data platform and user interface will be considered.

Scenario 3 detailed description

Scenario description 3.1

Scenario	
Context	Keep car secure for the whole vehicle product lifetime (in operation and maintenance)
Owner / Contact person	AVL, ZF
Description of defining behaviour	Continuous improvement is required to keep a car secure for the whole product lifecycle. Vehicle updates are changes made to the hardware or software of a security, safety, or privacy relevant item that is deployed in the field. It is needed to define the update as addition/change/deletion of SW or the change of a security algorithm. In addition, SW downgrades and HW changes need to be considered. The backend system needs to be able to cope with down-level systems. The distribution process needs to be lean enough to handle high priority updates. This also includes secure OTA SW update technology to update software components for preventing potential attacks or exploitation of a known vulnerability.
Actors / stakeholders	OEM – is assumed to be responsible for hosting all new update in the vehicle. In case of software update, an OEM operates a software update server at the backend; Driver–who checks, decides, and accepts update for components in his/her car; Gateway-a SW and HW module in the vehicle that connects to the backend and manages the update process. It performs all necessary on-board security tasks and acts as an intermediate entity for software updates targeting ECUs, e.g. caching the software between the Internet and the CAN bus; ECU–connects to CAN bus and is assumed to be the endpoint where the software is installed; Maintenance personnel – is responsible for manual update in a repair shop.
Infrastructure – system components and connections	• HW/SW for security gateway; • Secure OTA update from back-end to on-board system; • Multi-concern safety & security verification & testing framework for security and safety assurance according to industrial standards.
Step-by-step execution	1. Cybersecurity critical bug detection; 2. Label management will be used to identify affected HW/SW components; 3. Case triage (Incident assessment, decision to start the bug fix procedure). For positive decision the process will be continued, otherwise the bug will be just documented; 4. The developed patch/(new HW) will be available and a bulletin will be broadcasted to necessary parties [As plan B for SW updates a possibility for manual upload has to be considered (not all updates are possible with SOTA)]; 5. Gateway checks OEM backend server regularly for new software/hardware updates (Gateway authentication needed). In case of HW update or a new SW that requires a manual update, the driver will be notified that a HW change or a manual SW update is available and required and he needs an appointment with a garage. Next steps 6-10 are only for SOTA. 6. If an update is available, check compatibility and legitimation; 7. If check is positive, Gateway notifies Driver a new update is available; 8. If Driver confirms update, Gateway downloads the update from OEM server, verifies its cryptographic signature; 9. Gateway initiates an ECU software update over the CAN bus; 10. If ECU update is successful, Gateway notifies Driver, Gateway also notifies the backend server that a new version of update is installed on the vehicle.

Data flow	1. A new software update is generated; 2. The software with its meta-data are compressed to a blob, encrypted and digitally signed. The software blob is stored on the backend server; 3. The software blob is downloaded over the Internet (including wireless link) to Gateway; 4. Gateway caches the software and updates the targeted ECU according to the description in the meta-data.
Assumptions	• OEM backend server is a trusted environment; • The link between OEM and Gateway is untrusted; • Gateway is secured against remote and local attacks.
Compliance needs	UNECE, "Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD".
Preferred method for Security/Privacy/Safety Analysis	Security Automotive Threat Analysis, Vulnerability Analysis, Risk Assessment (TAVARA) based on ISO/SAE 21434 working draft.
Relevant threats	Attack surface is the open ports/services and APIs of the on-board system and the backend system (attacks to bypass access control and authentication mechanisms), as well as the communication link that connects the backend system to the on-board telematics unit (MITM attacks). The attacker attacks weakest link in the OTA update process and injects malicious software into the update.

Scenario 4 detailed description

Scenario description 4.1

Scenario	
Context	Advanced access to Vehicle
Owner / Contact person	IMA
Description of defining behaviour	Scenario is reflecting the trend for property (vehicle) sharing. The traveller orders a car in the target destination via cloud-based service. Downloading the credentials to his/her mobile phone or smart personal identifier like GEMALTO eGo wristband, he will be navigated to find the vehicle and enabled to access it securely. User check in, check out so as the profile of service consummation will be smoothly registered. (in line with EU regulatory frame –eIDAS and GDPR).
Actors / stakeholders	OEM –responsible for operating the ID management server, mobile application and key distribution; Driver –user of the system, actively requests key and uses it for opening a car; Gateway –a module managing secure data communication between on-board access control unit (ACU) and remote ID management server. It is intended to manage also communication between ACU and CAN bus. Vehicle unlocking device; support for offline operation in case of lack of coverage for the gateway
Infrastructure – system components and connections	Driver/ Crew identification: variable RF contactless, RFID, NFC, BLE, eGo and wearable key devices; Car on board infrastructure: Body Board Control Unit (BBCU), CAN/FlexRay/Ethernet Gateway; Supportive technology: External Authentication Server; Vehicle identification: we aim to use bidirectional V2I built-in tools; In-vehicle Gateways.

Step-by-step execution	1. Driver registers to use a specific car at specific time using web interface; 2. OEM ID management server upload a time limited mobile key to Drivers mobile device and the access right for the gateway; 3. OEM pushes through car Gateway access rights update to the cars ACU, if online; 4. Driver interacts with the access reader in order to unlock the car; 5. ACU propagates unlock signal through onboard Gateway to the CAN bus.
Data flow	1. New mobile key and unique user identifier is created on the OEM server and user is requested to activate the key. 2. Access rights update is pushed from OEM server to ACU, as second channel the mobile phone itself is used in case the CU is offline. 3. After finishing the one-time key activation process, key is securely installed into user's device. 4. After interaction with access reader, key is sent to ACU over BLE/NFC/RFID5) ACU verifies access authorization and sends open command to onboard Gateway to unlock the vehicle. 5. In case of offline operation, the vehicle unlocking device after verification and validation sends open command to onboard Gateway to unlock the vehicle.
Assumptions	OEM backend server is a trusted environment. The link between OEM and Gateway and the link between key-bearing device and reader are untrusted. Gateway is secured against remote and local attacks. In-vehicle communication is a trusted environment.
Preferred method for Security/Privacy/Safety Analysis	Security: SO/SAE 21434 Safety: ISO 26262
Relevant threats	Threat 2: Non-secure communication protocol or improper server certificate check. Threat 5: (partially) No or weak encryption. Sensitive data related to users and manufactures must be properly protected. Threat 6: No or weak protection of in-vehicle network. Threat 7: User identification through V2X communication. Threat 8: Attacks on privacy or data lost and leakage. Privacy of the car user has to be guaranteed during the authentication process in order to prevent leakage of personal data. Threat 9: the vehicle is in a remote offline location.
Additional information	Linked to Demo 3.1 = robust dynamic car access system (CAS) based mixture of recent smart enablers. The innovative concept will be based on various identifiers both driver and car, access right cross-check, dynamic online authentication and profiling using BUT authentication server and BUT robust supplicant code.

Scenario 5 detailed description

Scenario description 5.1

Scenario	
Context	Rail
Owner / Contact person	Thales

Description of defining behaviour	Show the technical feasibility of a virtualization approach using hypervisor technology. This approach will separate different safety critical applications and manage redundancy. Secure communication will connect safety-critical applications. A key asset of this approach is the ability to run multiple safety-critical applications virtualized on one or more hardware machines. This scenario will be investigated with respect to virtualization's ability to meet real-time and safety as well as security requirements considering redundancy management from cluster as well as TAS Platform (safety critical railway platform) point of view. This environment will allow railway asset operators to run their railway operation (e.g. interlocking) in a cluster environment. These applications are connected to field elements and HMIs.
Actors / stakeholders	Railway asset operators; Cluster operator.
Infrastructure – system components and connections	Virtualization technology for ensuring a secure environment for the safety critical applications; Cloud/cluster-based technologies for secure staged deployment of safety critical applications; Secure communication ensuring the integrity and availability of the safety critical applications.
Step-by-step execution	Application deployment in cluster environment; Railway operation (e.g. interlocking); Application update and maintenance.
Data flow	HMI <-> application <-> field elements
Assumptions	Untrusted network on cluster boundary; Trusted virtualization environment.
Compliance needs	CENELEC railway safety standards IEC 62443 industrial network and system security
Preferred method for Security/Privacy/Safety Analysis	Risk assessment, threat analysis based on IEC 62443 3-2Security testing (penetration test, vulnerability analysis).
Relevant threats	Threats: • Use of open networks for communication -> attack via open ports/ unencrypted services; • Denial of service on publicly available cloud hosts; • Vulnerabilities in VM software due to needed compatibility to legacy systems; • 0-day exploits on server machines; • Trojan/Vulnerability in Virtualization software; • Sandbox escape; • Information leakage between virtual machines on same server; • Maliciously change (integrity) of cloud configuration; • Risk of virtualization sprawl (too any VM instances to be manageable).
Additional information	The TAS Platform is a technology platform for all types of safety-critical transport applications. It consists of a range of hardware and software components with associated methods and tools for creating safer and more reliable real-time embedded systems. The TAS Platform separates the railway-specific applications from the hardware and system software technology, and serves as a common base for these applications, providing fault tolerance services such as time synchronization, membership service, voting, and fault management. As such, the TAS Platform tries to use as many COTS/FLOSS components as possible to minimize development and life cycle costs (maintenance) as well as to provide long-term application support with minimal application porting efforts.

Scenario 6 detailed description

Scenario description 6.1

Scenario	
Context	A critical situation is recognized, and it needs to be virtually reproduced and analysed. The aim is to improve the functionality of an automated system. For example: emergency braking because a person was detected in front of the car by the fall-back sensor and not recognized by the responsible component earlier.
Owner / Contact person	ZF
Description of defining behaviour	There was an incident in some point of time in the past, and it is needed to recover the whole situation with considering the data from different sources: Different clouds, external cameras, navigation data, data saved on incident participant's cars, incident investigation information and so on.
Actors / stakeholders	Clouds –store necessary information for the relevant period of time as an "Info-Freeze"; End User –no action because no accident situation; Roadside infrastructure–provide "Info-Freeze"; Onboard black box – continuously collect information of local systems like the GPS sensor and other sensors and save "Info-Freeze".
Infrastructure – system components and connections	Coordination between vehicle infrastructure, environment infrastructure, cloud.
Step-by-step execution	1. Recognition of critical situation; 2. Creation and protection from changes or deletion of "Info-Freeze" on different Clouds, roadside infrastructure and on-board black box; 3. Transfer of ”Info-Freeze"s into one external system; 4. Analysis of data within the external system and start development process; 5. As result: Rollout of SW update /functional feature or HW modification for automated system.
Data flow	Incident has been reported. Investigation and data collection have been started (needed information has been blocked for changes/deleting in different clouds, maintenance information of incident participants has been collected).
Assumptions	Cloud servers are a trusted environment. The link between Cloud and onboard black box is untrusted. Onboard black box is secured against remote and local attacks.
Preferred method for Security/Privacy/Safety Analysis	Security Automotive Threat Analysis, Vulnerability Analysis, Risk Assessment (TAVARA) based on ISO/SAE 21434 working draft.
Relevant threats	
Additional information	Attack surface is the open ports/services and APIs of the on-board system and the backend system (attacks to bypass access control and authentication mechanisms), as well as the communication link that connects the backend system to the on-board telematics unit (MITM attacks). The attacker threatens weakest link in the Incident Investigation process and injects manipulated data into the Info-Freeze. Privacy aspects of process needs to be prioritized.

ANNEX 2 – Components of demonstrator II

CSIC detailed description of action

CSIC automated vehicle features

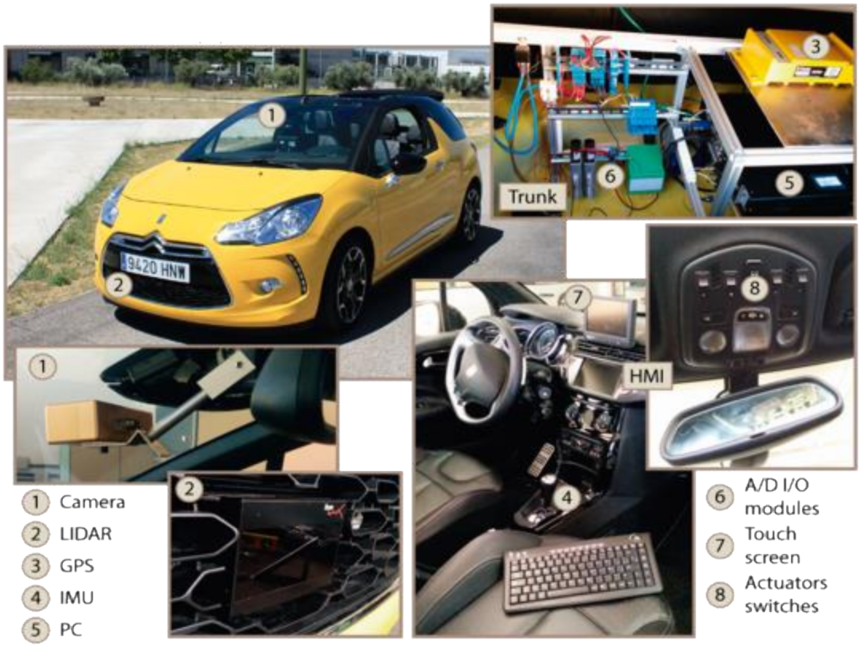
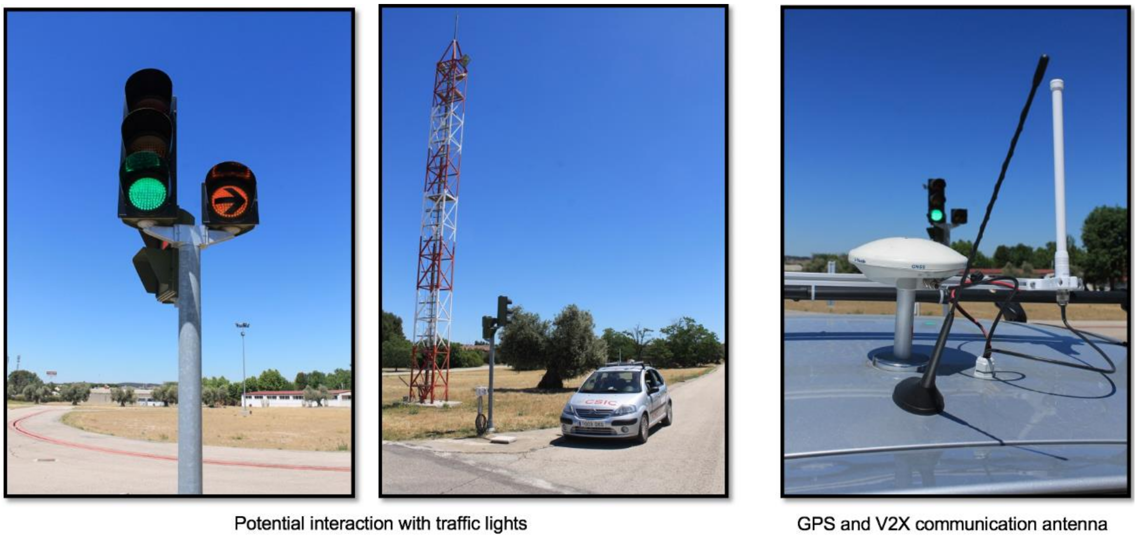


Figure 10 – CSIC's automated vehicle: Sensors and equipment.

On-board Sensors

- GNSS (10 – 20 Hz):
  - Trimble: receiver with access to GPS and GLONASS, able to use DGPS and RTK correction;
  - Position, speed and heading of the vehicle.
- IMU (100 Hz):
  - Crossbow: High precision angular rate and acceleration in 3 axis.
- CAN bus information (25 – 100 Hz):
  - Access to embedded sensors of the series production vehicle;
  - Speed, longitudinal and lateral acceleration, steering angle position, pedals positions, etc.
- LIDAR (12,5 Hz):
  - Front Ibeo Lux: 4 layers, 115º FOV, 150m range;
  - 2 Side Velodyne Puck: 16 layers, 360° FOV, 200 m.
- Camera (10 - 20 Hz):
  - Stereovision with Point Grey Bumblebee;
  - Obstacle detection, traffic signs and lights detection, lane detection.
- HMI:
  - Safety switches per actuator;
  - Android tablet with an OsmAnd-based routing interface;
  - Driver monitoring system based on cameras and infrared sensor.
- V2X:
  - RSU and OBU C-TS IEEE 802.11p;
  - On-board 3G/4G router.



Potential interaction with traffic lights

GPS and V2X communication antenna

Figure 11 – Photographs of the possible interactions between the car, traffic lights, GPS and V2X communication.

Software Architecture

Among the different existing technologies for inter-process communication, the adopted mechanism in the vehicle is the Lightweight Communications and Marshalling library (LCM). LCM is based on a publish-subscribe message passing model using UDP multicast as underlying transport layer. Under this model, processes publish data over a particular channel identified by a unique name and subscribe to those channels required to complete their tasks. Moreover, by using UDP multicast the system becomes highly scalable since the bandwidth required for the transmission of one message is independent of the number of subscribers. The use of the LCM library increases therefore the capability of the developers for debugging and detecting system failures. Furthermore, thanks to the time stamps, all the system data can be logged and replayed off-line as it was sent through the network.

Figure 122 shows how the different sensors, actuators, devices and SW modules operating in the vehicle are connected though a common API middleware (LCM).

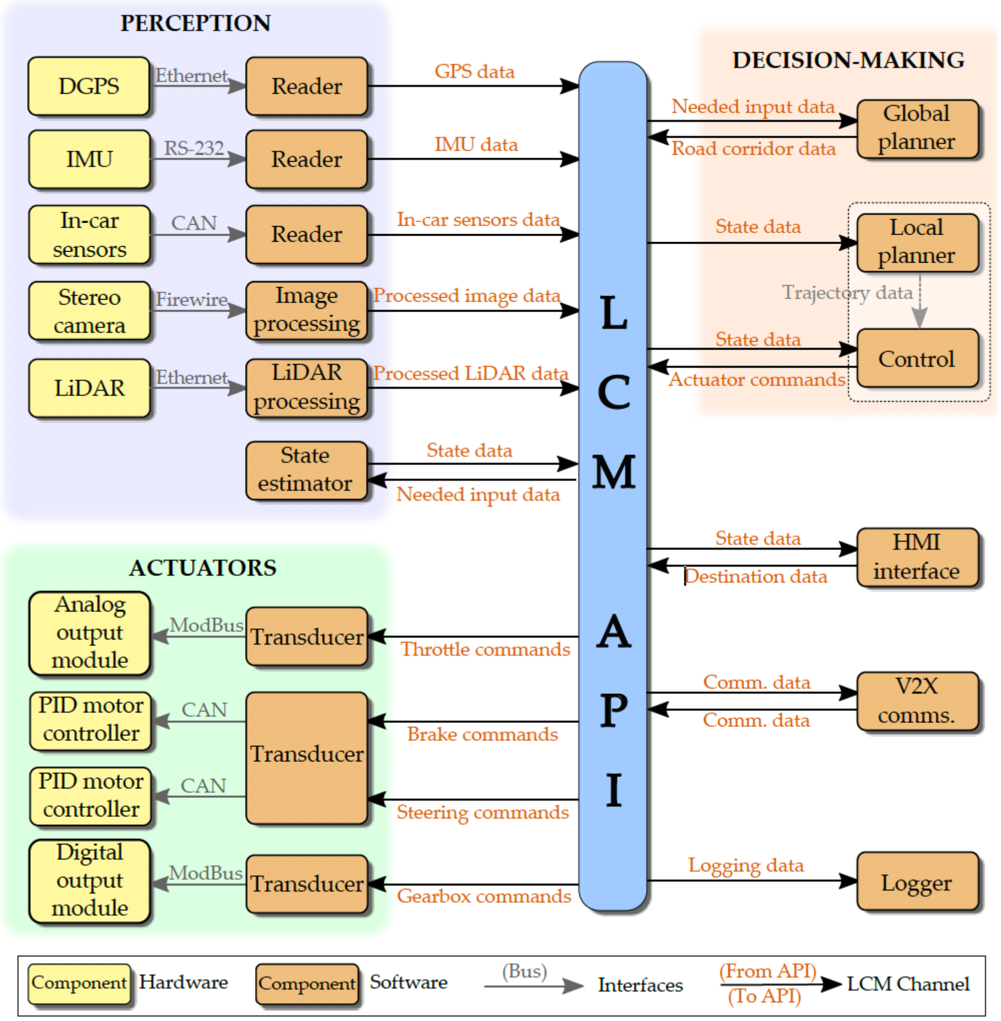


Figure 12 - Hardware and software components around LCM.

www.secredas.eu
mail@secredas.eu
Social media @secredas_eu

Horizon 2020
European Union funding
for Research & Innovation

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, The Netherlands, Poland, Romania, Sweden and Tunis