



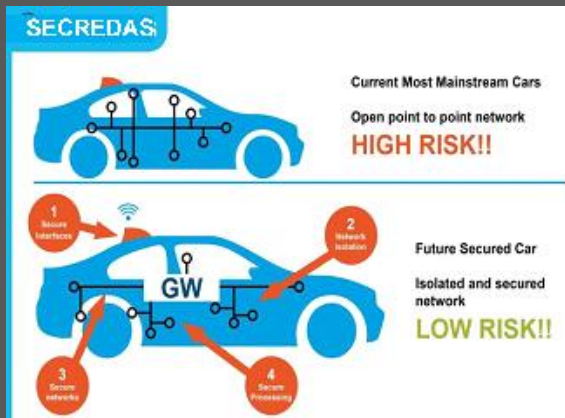
Project status overview at end of YR2

About

Secredas will increase consumer trust in connected and automated transportation and medical industries.

One in four potential buyers/users of autonomous vehicles in Europe do not trust them to be secure, safe or privacy compliant and are therefore reluctant to buy one. This lack of trust is an enormous challenge for European OEMs that aim to remain competitive and world leaders. More so, since newcomers such as Google and Apple have entered their market.

SECREDas focuses on taking a huge step on cybersecurity and safe technology for connected and automated vehicles. The technology SECREDas envisions, will be of use in the areas of automated systems within the automotive domain, but also in the domains of rail and health.



Typical potential driver risks when using today's connected cars and tomorrow's automated vehicles:

SECURITY:

back-end server attacks, V2X car attack, exploiting software updates, human error attacks, car interface attacks, in-vehicle attacks, security flaws exploit attacks, privacy attacks, physical manipulation, attacks on sensors.

SAFETY:

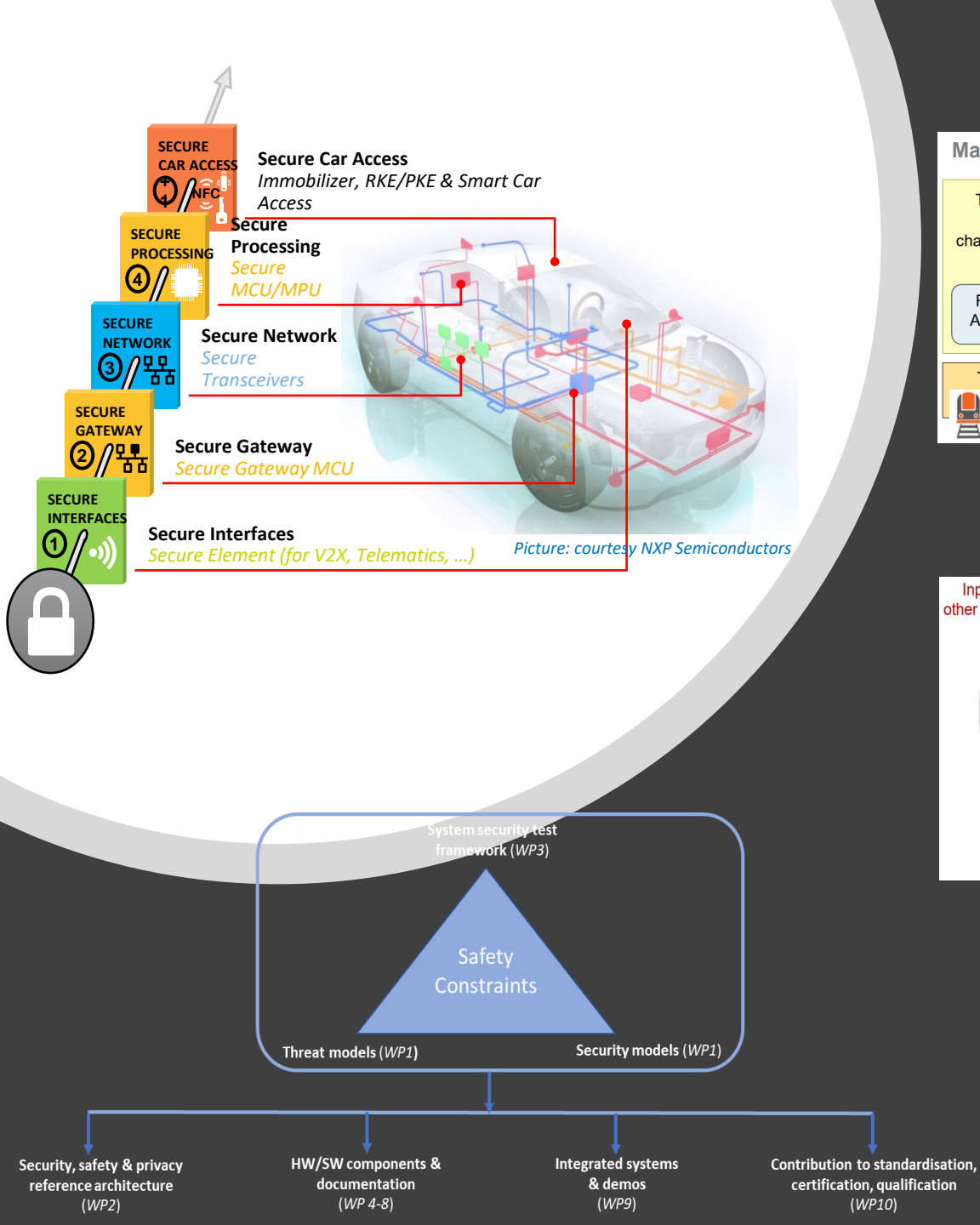
legitimate sender of information (remote or in-vehicle) has not been authenticated.

PRIVACY:

personal data exposure when interfacing with in-vehicle sensors/IoT and with external (cloud) applications.

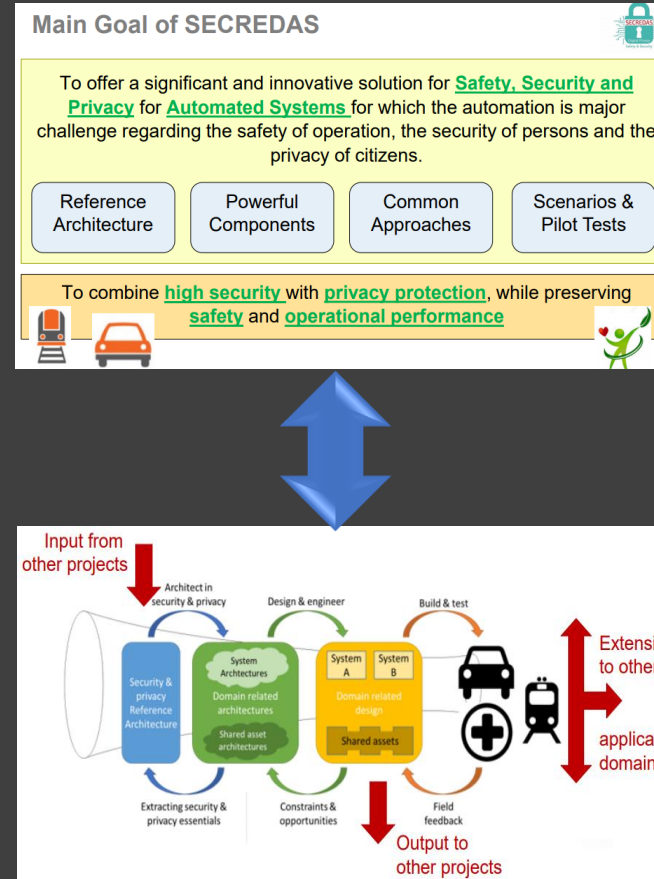


There is a need for secure, safe and privacy-conscious harmonised and interoperable solutions which effectively mitigate these risks and thus increase end-user trust. Hence... **SECREDas** !



SECREDAS project structure:

- Identify typical end-user Use Cases for connected & automated vehicles.
- Define typical threat scenarios for connected & automated vehicles in real-life circumstances.
- Create a transposable security, safety & privacy design framework.
- Use Common Technology Elements to facilitate technical integration of HW/SW components & reduce cost.
- Use Design Patterns to reduce security, safety & privacy risks at design stage of HW/SW components.
- Develop HW/SW components based on design framework.
- Demonstrate integrated components to mitigate threats & increase end-user trust.
- Provide update commendations to various standardisation bodies.

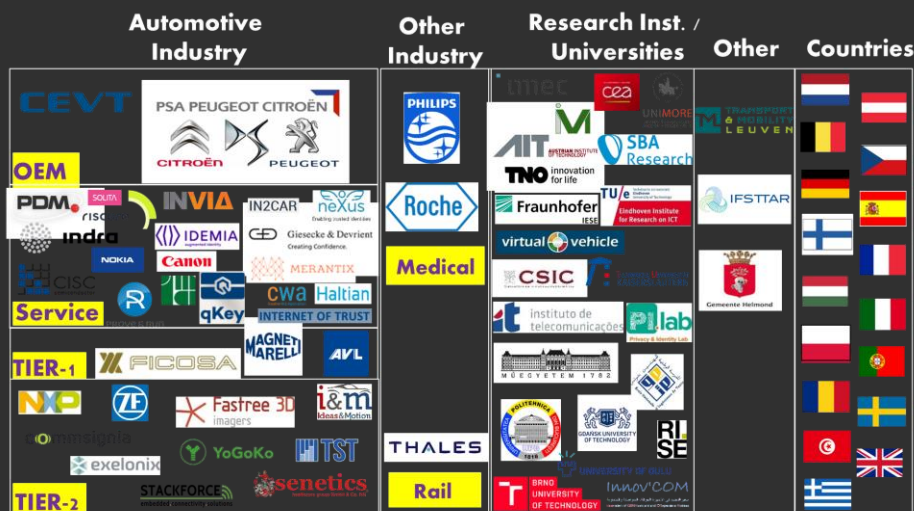


Common Technology Elements (CTEs) are domain independent technologies (implementations, mathematical models, specifications, processes, etc.) realized in existing systems (starting from TRL 7). Within SECREDAS, CTEs are related to safety, security, privacy protection. Examples are cryptographic libraries, hardware anchors for secure key storage, communication networks and protocols or existing security products like a firewall, trusted execution environments or blockchain.

CTEs are the starting point for the development of **Design Patterns (DPs)** in which design principles and best practices are combined and implementation recommendations for the correct use of CTEs. Design patterns are engineering domain independent and can include hardware and software designs as well as concepts on system level.

Summary of SECREDAS project collaboration:

- ✓ Funded by the EU ECSEL programme.
- ✓ 3-year project, started in May 2018.
- ✓ 73 partners involved.
- ✓ €51 Million total budget.



www.secredas-project.eu
info@secredas-project.eu

SECREDAS approach to risk mitigation:

- Use Cases (Road intersections, Driver Monitoring, Rail-Road interaction) and 6 scenarios for connected/automated vehicles have been defined, each with one or more risk scenarios involving one or more threats (total: 12 Use Case sub-scenarios; 10 threat scenarios).
 - Each threat scenario contains several sub-scenarios. Each sub-scenario comprises multiple sub-threats. (Examples: back-end server compromised, use of communication channels or update process to attack vehicle, system design exploits, data loss, attack on sensors etc.).
 - Each sub-threat is divided into sub-categories categories. (Examples: spoofing, message injection, data extraction etc.). Each threat category has been assigned specific 'control types' (examples: encryption, connectivity, logical access control etc.).
 - Each 'control type' comprises a set of technical mitigation options, meaning the development of HW/SW components which take into account security, safety and privacy principles (Examples: LIDAR, V2X, sensors, Secure CAN, ADAS, etc.).
 - Each component option is elaborated by the partners, using Common Technology Elements (CTEs) and Design Principles (DPs) to allow subsequent cost-effective integration of technologies into threat mitigation solutions.
- Full technical integration will be completed in YR3 (= final project year). Integrated threat mitigation solutions are demonstrated and validated in 3 separate DEMO cycles covering Autonomous driving, Driver Monitoring and Cybersecurity & Connectivity. A fourth DEMO using 'drones as vehicles' has been added for demonstration of non-integrated components (due to lower TRL-status).
- Project is largely on-schedule, but timely implementation of DEMO cycles is challenging due to planning uncertainty resulting from COVID19.

Summary of Use Cases and Threat scenarios:

Nr	Use Case Scenario	Sub-scenario	Use Case sub- scenarios
1	Road intersection	1.1	An intersection with traffic lights is approached by a hijacked automated vehicle that has no intention to stop.
		1.2	An automated vehicle approaches intersection which is equipped by a road-side system providing information about vulnerable road users.
		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).
		1.4	Emergency vehicle approaches a crowded intersection
		1.5	Resilience of the vehicle's perception systems against false information about the traffic situation
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
		2.2	Driver Monitoring: how human-in-the-loop automated and connected vehicles can be securely preserved from external threats?
		2.3	Vehicle and driver status monitoring (incl. driver's health and wellbeing)
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
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.
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.
6	Incident investigation	6.1	A critical situation is recognized, and it needs to be virtually reproduced and analysed.



SECREDAS main threat descriptions	
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.
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.
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 system4. In addition, CAN can be accessed physically through OBD port, charging station, or a mechanic's computer.
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.
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

Final set of Use Cases and Threat Scenarios defined for live DEMO cycles:

✓ 12 sub-scenarios specified, focused on Use Cases.

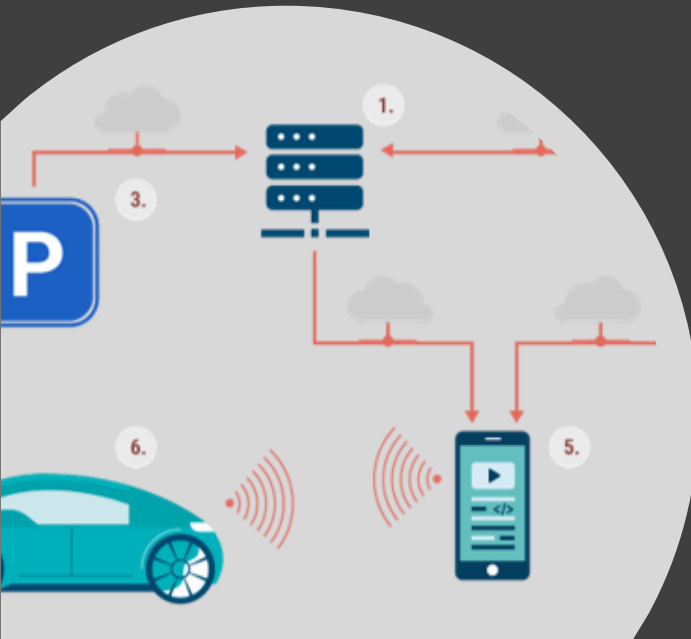
- approaching or navigating road intersections with/without road management infrastructure or obstacles.
- moving vehicles with drivers suffering sudden health problems.
- keeping the car secure during the full vehicle product life-time (incl. periodic update/upgrade cycles).
- advanced access (rights) to an automated vehicle.
- safety at rail-road crossings.
- incident investigation.

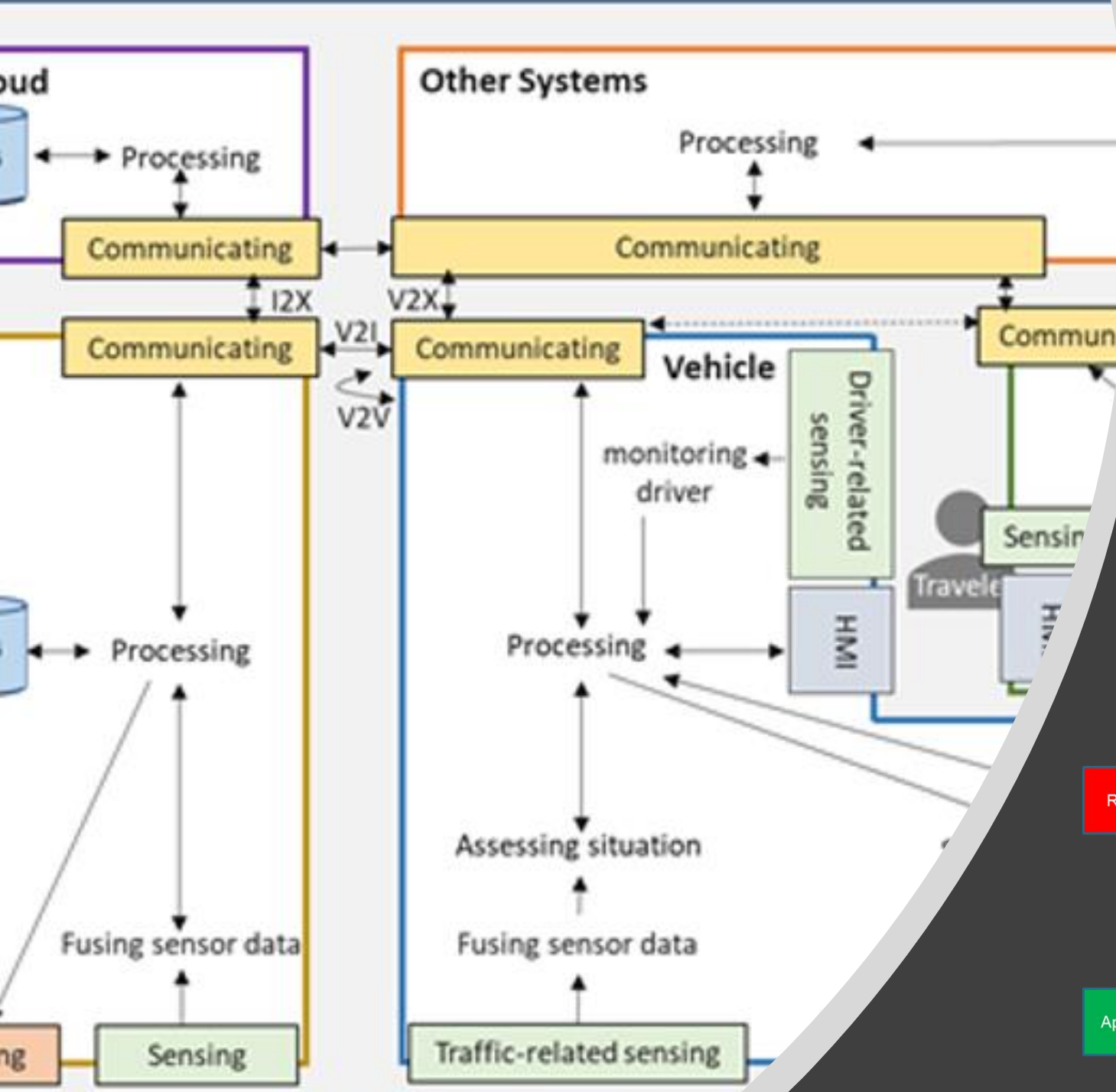
✓ Threat analysis for each sub-scenario completed.

- context, description of defining behavior.
- actors/stakeholders, infrastructure.
- system components and connections.
- step-by-step execution, data flow.
- assumptions, compliance needs.
- preferred method for analysis, relevant threats.

✓ Each (sub-)scenario was assessed for specific security, safety and privacy requirements/implications.

✓ Mapping to link Common Technology Elements (CTEs) & Design Patterns (DPs) to sub-scenarios completed.





SECREDAS reference architecture:

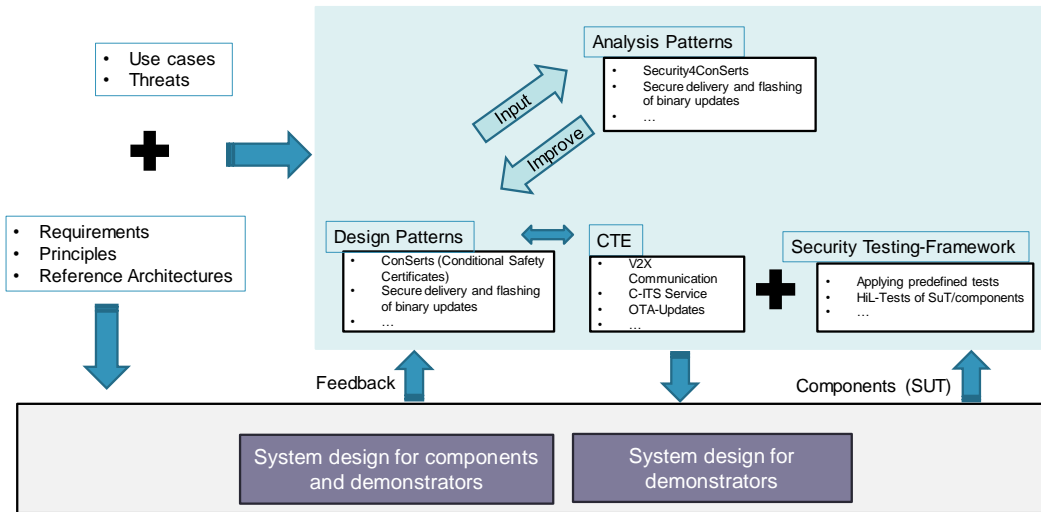
- ✓ Methodology developed for applying privacy and security aware design principles.
- ✓ Targeted at developers, analysts, testers.
- ✓ Applied to SECREDAS scope and Use Cases.
- ✓ Completion of Safety, Security & Privacy Evaluation framework.
- ✓ Completion of Privacy Implementation and Impact Reviews on Common Technology Elements (CTEs), Design Patterns (DPs), Safety Supervisor, HW/SW components.

Launching a new processing:
Rely on processing of personal data ->
impact on users' privacy

Considering the processing:
Evaluation: Automated decision, sensitive
data, vulnerable data subject...

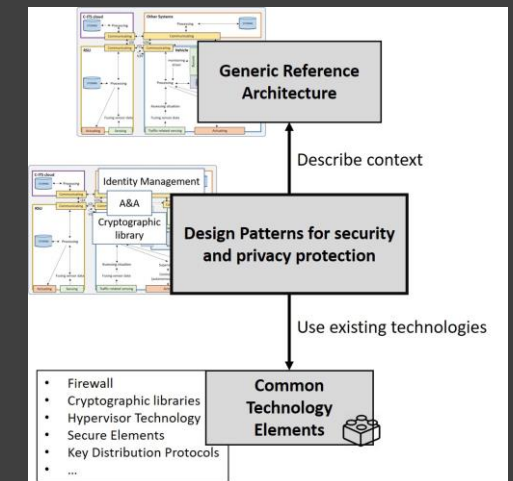
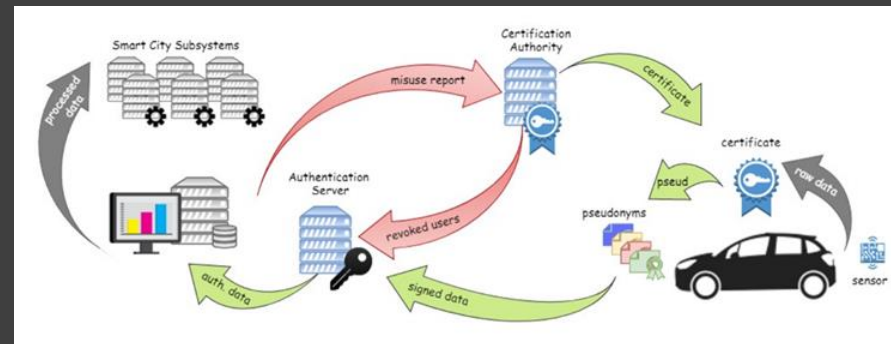
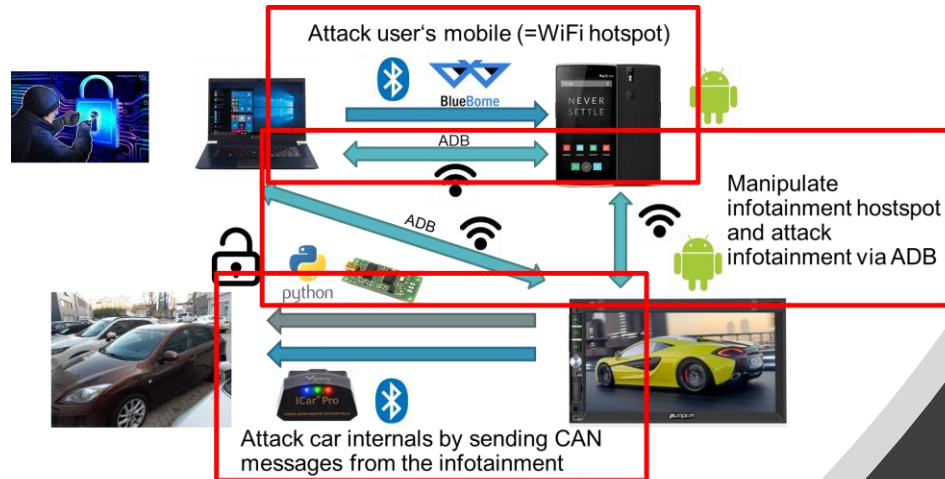
Addressing the risks:
Appropriate technical and organisational
measures, Residual Risks...

Evaluating the privacy risks:
Potential Impact, Risk sources, supporting
Assets...



CTE validation:

- ✓ Existing Common Technology Elements (CTEs) improved and validated for SECREDAS HW/SW development.
- ✓ 34 domain-independent Design Patterns (DPs) created.
- ✓ Completion of security & privacy testing framework & application to Use Cases.
- ✓ 18 analysis patterns created for analysing DPs.
- ✓ Domain independent tools for security testing developed, leading to verification cost reduction by 15%.



Sensor development:

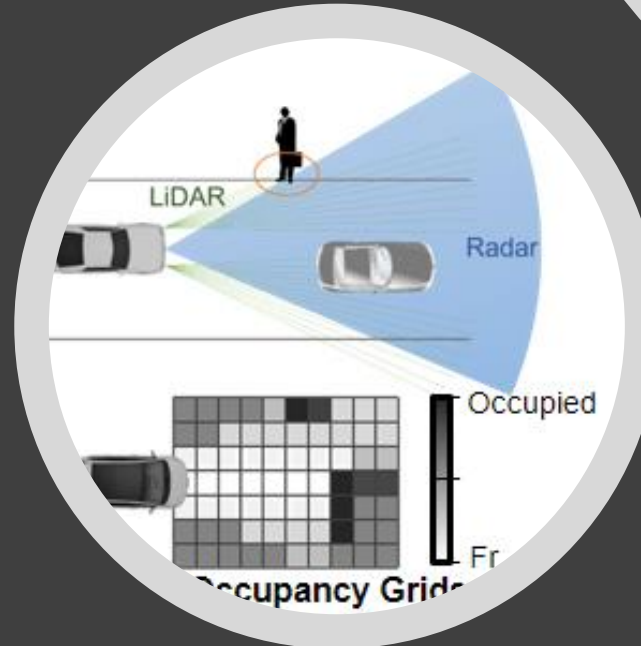
✓ Sensor components for sensor fusion selected & developed.

- LIDAR object recognition
 - Interference resilient; interference suppression.
 - Detection of direct attack on LiDAR “time of flight” distance measure.
 - Adaptive Tx/Rx integrated circuit (CMOS 180nm IC wafer).
 - World’s first implementation of a SPAD array Flash LiDAR.
 - LIDAR to sensor fusion adaptive interface.



✓ Sensor fusion algorithms developed and extended.

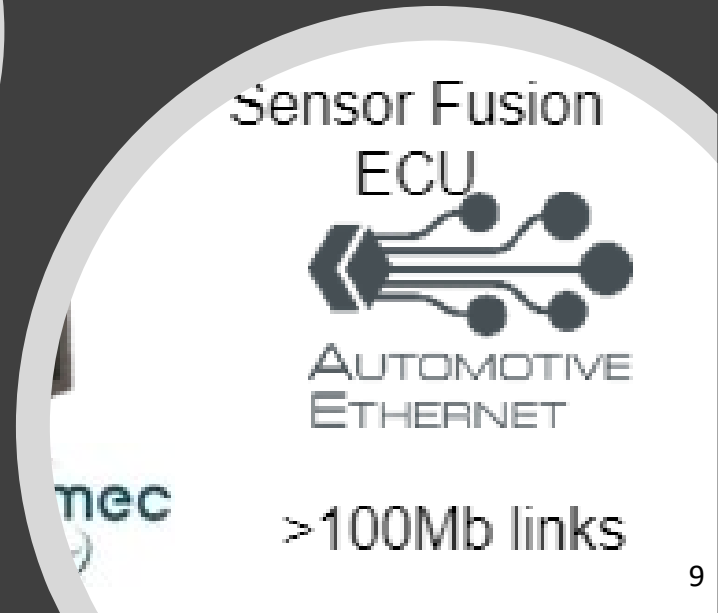
- Data processing & data fusion analysis
 - local sensor processing (attack detection) & fusion between local sensors + remote sensors (deep learning).
 - two methods for Occupancy Grid creation from Radar.
 - V2X messaging for transmitting remote sensor info.

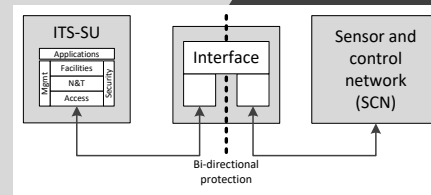
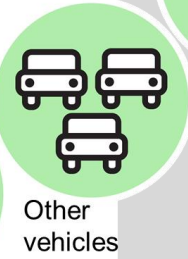
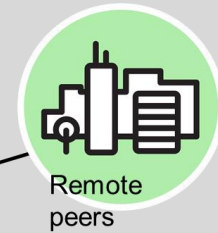
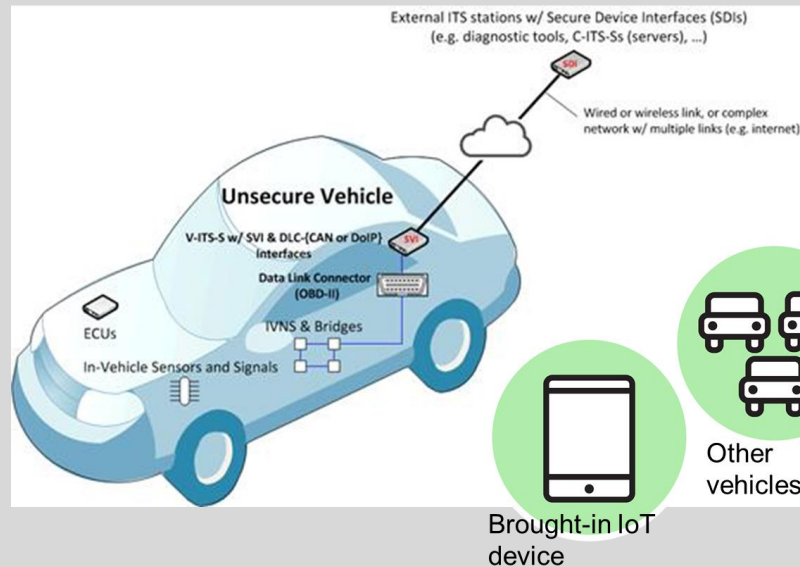
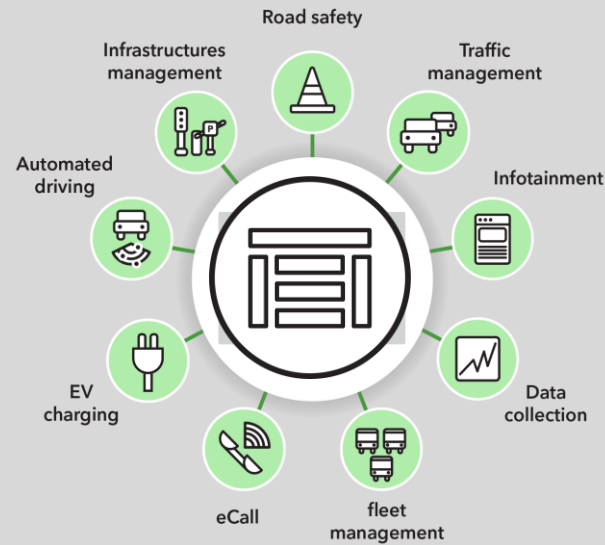
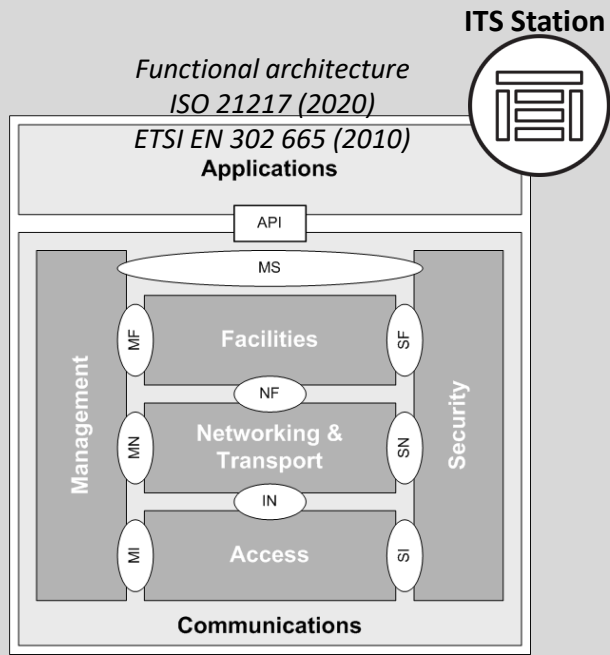


✓ Drone testbed for selected Use Case scenarios completed.

✓ All case scenarios can be demonstrated:

- Object identification.
- Collision avoidance.
- RSU information & sensor





Secure Gateway & secure sessions:

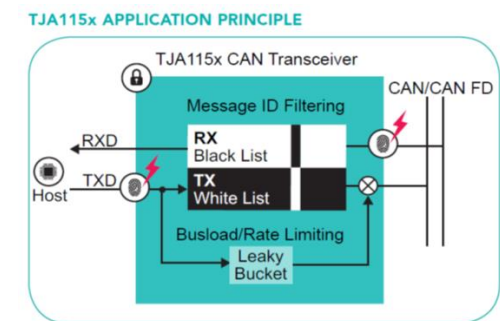
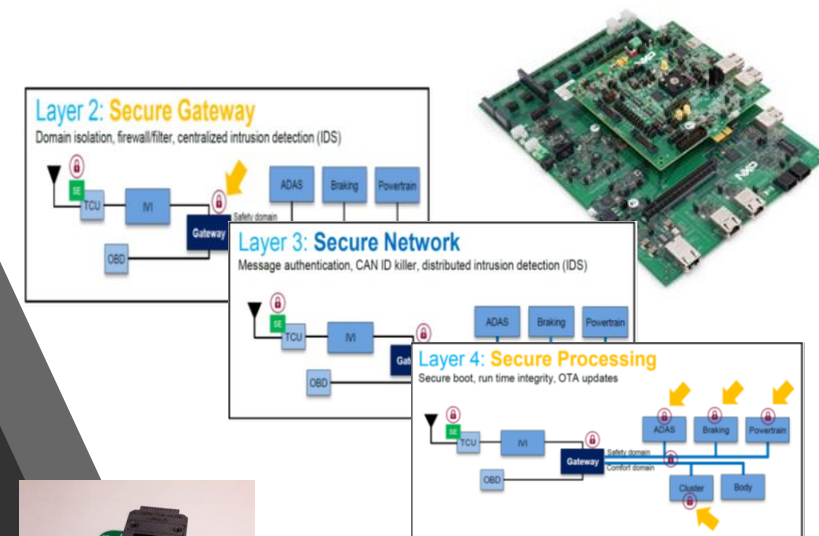
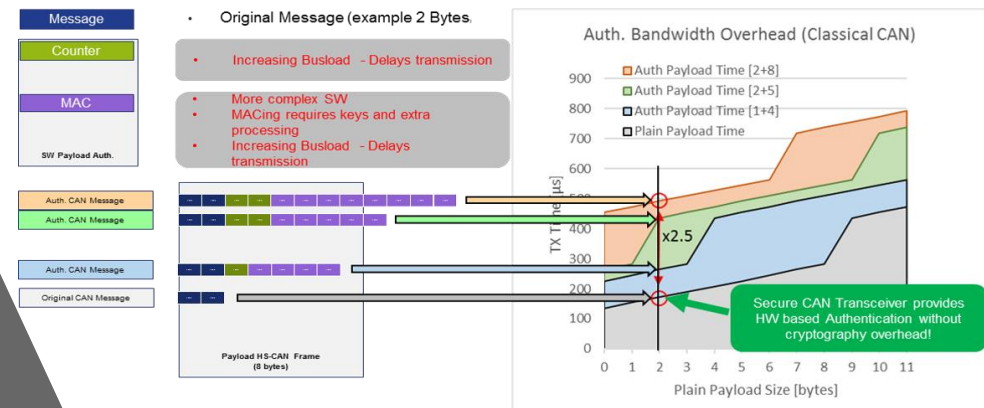
- ✓ **high level security features into ITS station architecture**
 - localised communications between vehicles & roadside infra.
 - Integration of IoT devices in ITS station architecture largely completed.
 - secure vehicle gateway validated.
- ✓ **Secure V2X communications**
 - all types of communication technologies & protocols covered.
 - integration of security components into existing platforms (supervisor architecture, HSM, key management) ongoing.
 - integration of new capabilities into the ITS station architecture: new ITS-G5 radio, new access technologies (Bluetooth/5G), new communication protocols (IoT / point-to-point localized communications, new C-ITS messages (CPM)).
- ✓ **Communication to/between secure IoT devices and sensors completed**
- ✓ **Secure radar/5G for V2X communication & sensing: proof-of-concept completed**
 - combining sensing (radar) and localized communications (V2X) in millimetric spectrum. HW design has been completed; technical specifications and physical layer are defined.
 - simulations & analytical studies + security at physical layer completed.
- ✓ **Secure testing & performance validation completed**
 - ongoing: complement existing test suite specifications from ETSI on C-ITS.



Next step: 1. achieving interoperability & compatibility with standards (C-ITS + automotive); 2. integration with communication stacks from partners.

In-vehicle networking & VCU:

- ✓ **Integrated Secure Element (ISE) based on CTEs to secure internal Infrastructure (V2X, in-vehicle network) of the car is 90% complete**
 - Trusted Execution Environment (TEE) available to provide a secure base to the gateways and VCUs.
 - Design and implement CAN data collector for analysis of vehicular networks (necessary for attack on in-vehicle network) is 70% complete.
 - Anomaly detection system (anomaly mining algorithms focusing on Long Short-Term Memory (LSTM) neural networks, signal extractor, use of ML, notification API etc.) has been tested.
 - Implementation of Secure On-board Communication (SecOC) to authenticate messages and protect the integrity of the communications on CAN bus and between gateways.
- ✓ **Secure CAN FD Transceiver concept and Secure CAN communication without crypto developed**
 - Intrusion detection & prevention (IDS / IPS) through on-the-fly CAN ID filtering and bus-guarding.
 - Flooding prevention (DoS).
 - Jailhouse Hypervisor with cache colouring.
 - Erika integration.
 - Simple CAN transceiver replacement (only HW!).
 - Secure CAN integration design completed.
- ✓ **Multi-core VCU component developed**
 - sample initial VCU silicon validated and available; documentation mature.
 - safety level up to ASILD; supports latest hardware security and network acceleration for traditional CAN, LIN and FlexRay and emerging automotive Ethernet.



Driver monitoring:

✓ Secure connections established

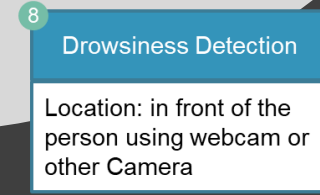
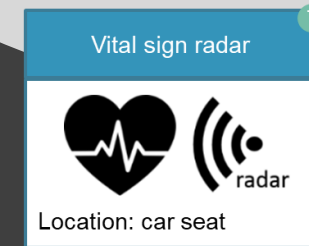
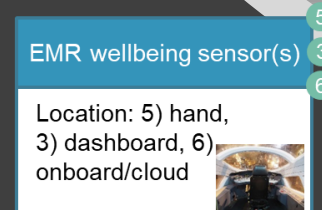
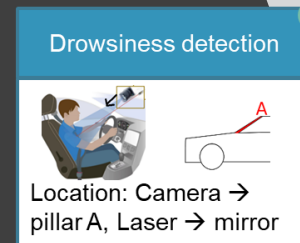
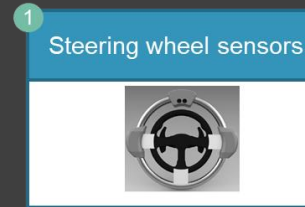
- Personal health and driver performance monitoring technologies and building blocks built.
- Description of health demonstrators available.
- Health demonstrator validation report available.

✓ Driver safety monitoring in place

- Behavior monitoring in simulated driving.
- Physiology (in particular: drowsiness monitoring) monitoring tested.

✓ Privacy assurance (GDPR compliance)

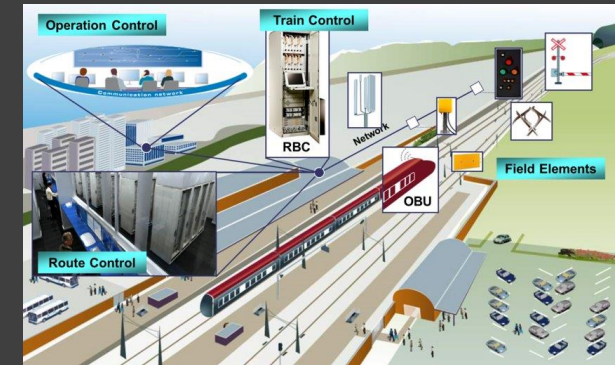
- Remote access to medical data validated.
- Acquisition and central storage of health data from wearables available.
- LPWA (Low Power Wide Area) air interface available.
- Data security validated.
- Driver authentication validated.
- Privacy preserving authentication validated.



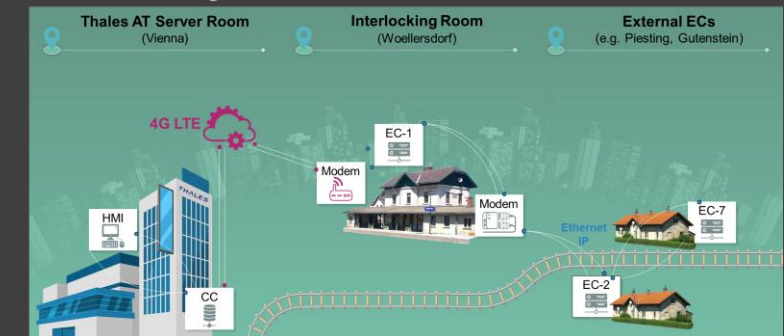
Rail User Scenario:

- ✓ Concept for secure IoT edge device incorporating virtualization, OTA updates, Trusted/Secure OS, COTS hardware

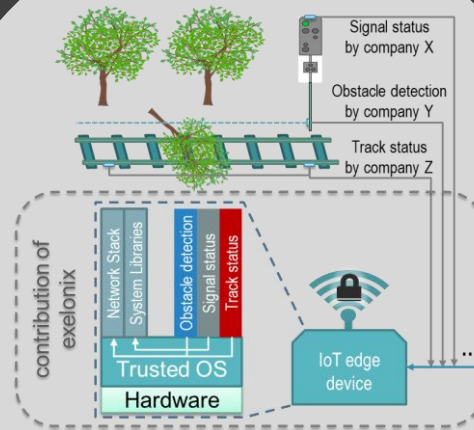
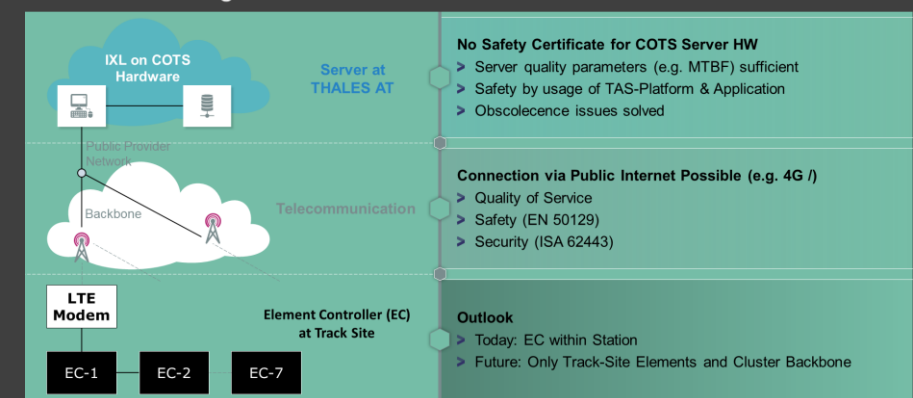
- HW prototype designed.
- integration of Secure OS/Hypervisor in progress.
- microcontroller-based Edge Device: 5G|SIP hardware platform and system concept developed.



Interlocking with Cloud Backend

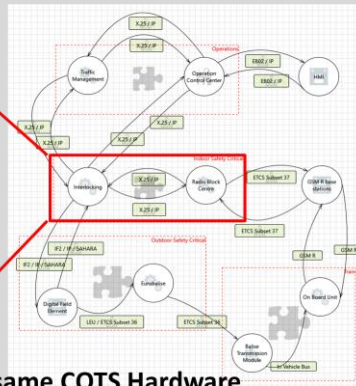
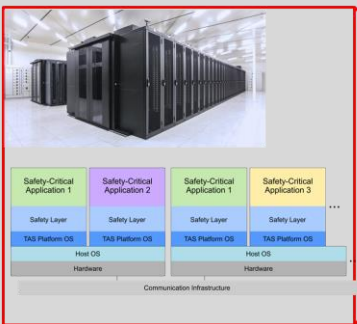


Interlocking CC on COTS Cluster

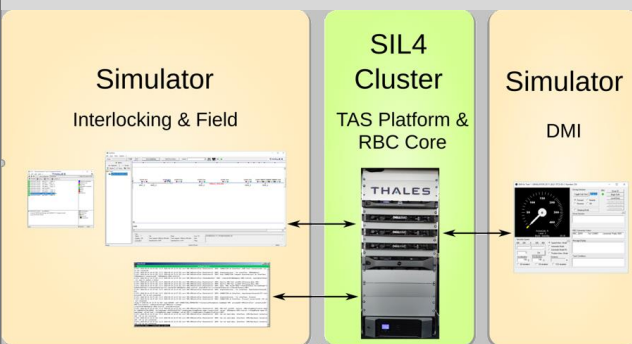


- ✓ Hypervisor technology for rail Use Case selected

- impacts of memory contention on Safety-critical tasks running in a Multicore node studied.
- study on memory contention regulation ongoing.



Goal: Multiple SIL4 Applications on same COTS Hardware

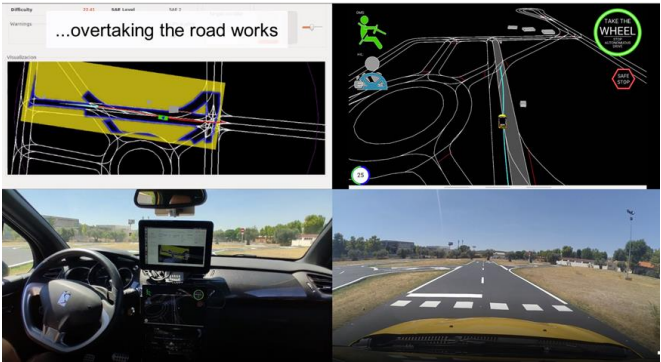
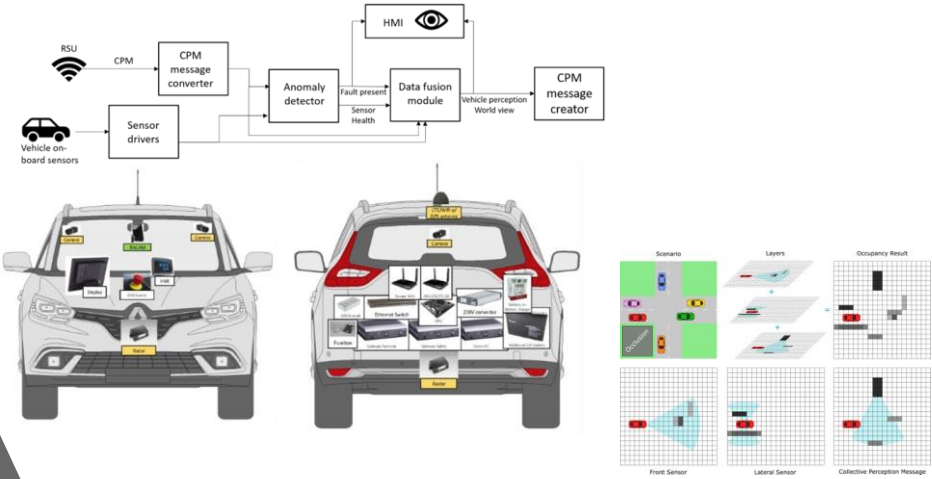


Common Demonstrator Cycles:

Current planning... (subject to COVID19 restrictions; updates ongoing)

Task	Description	Month
Planning	Deadline for accepting participants	M20 (Jan 2020)
	Fill in D9.5 together with partners	M21 (Feb. 2020)
	Partner list and contributions	M22 (Mar. 2020)
	Integration plan for WP9	M25 (Jun. 2020)
	Fill in D9.5 together with partners	M25 (Jun. 2020)
	Protocols for integration test	M26 (Jul. 2020)
Integration	Acceptance criteria integration	M26 (Jul. 2020)
	Components ready	M28 (Sep. 2020)
	Specify interfaces also in D9.5	M26 (Jul. 2020)
	Verify interfaces between components	M27 (Aug. 2020)
	Installation in Helmond	M29 (Oct. 2020)
	Integration of components	M28 (Sep. 2020)
	Integration at vehicle-side	M28 (Oct. 2020)
	Remote interface verification	M29 (Oct. 2020)
Validation	Remote functionality testing	M29 (Oct. 2020)
	Integration ready	M30 (Nov. 2020)
	Integration validation	M30 (Nov. 2020)
	Acceptance criteria for components in integrated setting	M30 (Nov. 2020)
	Data collection for component validation	M34 (Feb. 2021)
	Validation demo in operational condition	M35 (Mar. 2021)

- ✓ Integration is ongoing and, largely, on schedule. 30+ sub-systems in progress.
- ✓ Integrated solutions are being checked for suitability to mitigate defined Use Case Threat.
- ✓ Test protocols have been defined. Documentation in preparation.
- ✓ 9 scenarios validated for DEMO I, DEMO II and DEMO III. Additional demonstration platform (DEMO IV) using drones to simulate vehicles.
- ✓ Additional DEMO I and DEMO II location (Modena has been added to Helmond).
- ✓ All DEMO cycles will be recorded and published.

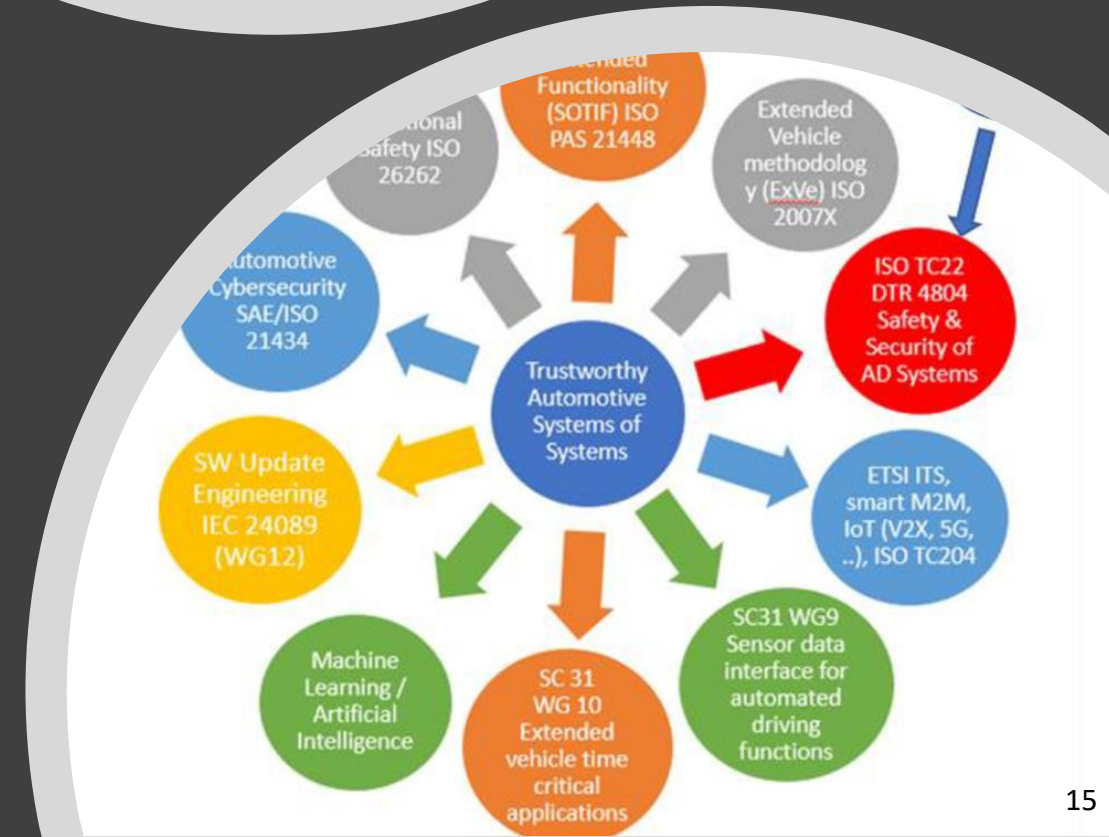
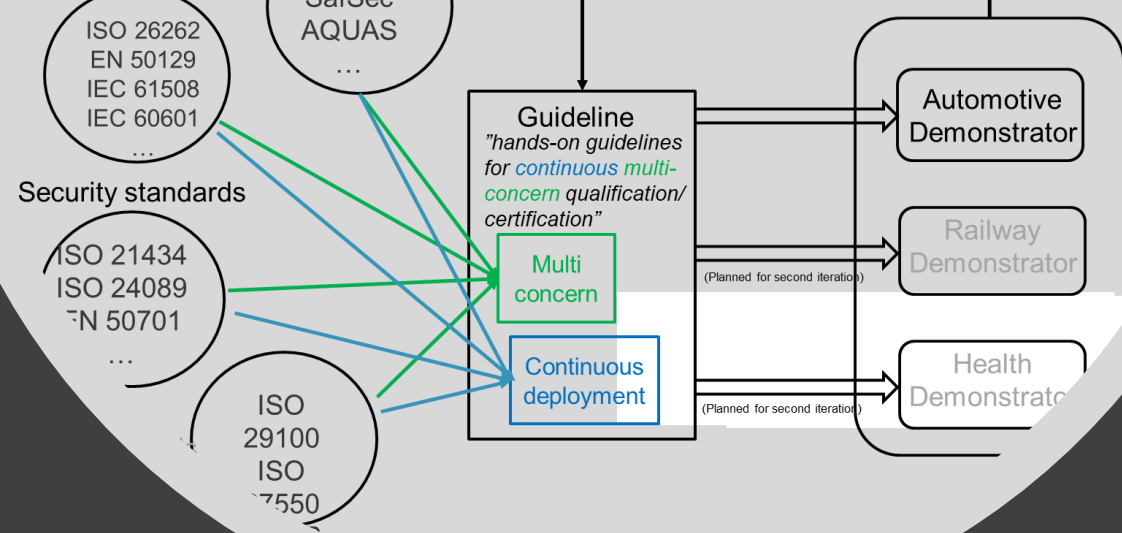


SECREDas efforts in standardization, qualification & certification:

Project aim: “SECREDas should take active role in international Standardisation”

- ✓ Analysis of existing partner involvement in standardization & current use of standards completed.
- ✓ Applicability of ITS standards to SECREDas checked.
- ✓ Ongoing support re. standards to partners during technical development.
- ✓ Ongoing dissemination of project findings to standardization committees (ISO, IEC, CEN/CENELEC, ETSI). Participation in working groups.
- ✓ Ongoing contribution to industrial associations (like ARTEMIS-IA, EPoSS).

➡ Expected outcome: supporting the evolution of a combined safety, security and privacy co-engineering culture !





End of presentation.
Please contact us !

About

Secredas will increase consumer trust in connected and automated transportation and medical industries.

www.secredas-project.eu
info@secredas-project.eu