SECREDAS

Product **Se**curity for **Cr**oss Domain R**e**liable **D**ependable **A**utomated **S**ystems

DELIVERABLE REPORT

Document Type	Deliverable
Document Title:	"Initial set of scenarios & use cases"
Document Number	2018-wp1-D1.1
Primary Author(s)	Marianne Vandecasteele, WP1 leader
Document Date	08/10/2018
Document Version / Status	v1.0
Distribution Level	Confidential
Reference DoA	30 April 2018

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
Johan van der Kamp	TNO	Christoph Striecks	AIT
Patrick Pype	NXP Semiconductors	Eric Nassor	CRF
Reinder Haakma	Philips	Christophe Pagezy	Prove & Run
Brenda Meza	Ficosa	Cyrille Falcou	GTO
Florian Stahl	AVL	Filip Kitanoski	Roche
Karel Kalivoda	IMA	Mauro Gil Cabeza	Indra
Peter Tummeltshammer	Thales	Arturo Medela	TST
Jorge Villagra	CSIC	Guus Stigter	UBIQU
Tamara Goldsteen	HELM	Vaclav Kaczmarczyk	BUT
Ralph Weissnegger	CISC		

REVIEWERS

Name	Organization	Date
Patrick Pype	NXP-Semiconductors	07-10-2018
Roy Pennings (coordinator)	NXP-Semiconductors	07-10-2018

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
v0.1	06/09/2018	Marianne Vandecasteele	Draft MS excel scenario overview & draft deliverable text
v1.0	08/10/2018	Marianne Vandecasteele	Final version of initial list of use cases overview & updated deliverable text

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), for the development of next generation highly secured automotive, health, and rail technology, both hardware and software (input to WP3-8).

Deliverable 1.1 (D1.1) is part of Task 1.1 and describes the initial set of scenarios and use cases compiled by the work package participants, which are used throughout the project and this will feature in the WP9 demonstrator. The initial set of scenarios comprises 3 automotive scenarios, 1 health scenario and 1 rail scenario. For each scenario, the relevance has been described, and the threat/attack is defined.
Furthermore, the deliverable defines the scenario owner, the contributors, the technology involved and the way in which the scenario is linked to the WP9 demonstrator. The initial of scenarios shown in this deliverable will be extended into a final set of scenarios in deliverable 1.2 (D1.2).

At this time, the scenario validation methodology in a demonstrator-setting has not yet been defined, as this requires input from WP9, which has not yet started its activities.

Table of Contents

1 Background to deliverable 1.1

Deliverable 1.1 (D1.1) is part of Task 1.1 and describes the initial set of user-scenarios and use cases compiled by the Work Package (WP) participants from 20 partner organizations. The scenarios form the starting and reference point for hardware and software architecture design and development in subsequent work packages with regard to defining and implementing security, safety and privacy protection measures. These will result in common security & privacy protecting components to be used in the domain-specific (automotive, rail, health) solutions. The scenarios will allow the integration of different common and domain-specific components in dedicated subsystems. WP9 will test and validate the components against the user-scenarios and use cases.

The initial set of scenarios listed in D1.1.1 comprises 3 automotive scenarios, 1 health scenario and 1 rail scenario. The scenarios that have been elaborated in this deliverable are:

1. road intersection;
2. automated truck with driver getting health problems;
3. updating the vehicle;
4. advanced Access to Vehicle;
5. rail.

For each initial scenario, the relevance has been described, and the threat/attack is defined. As listed in the project's Description of Action (DoA), each scenario has been assessed for the following aspects:

- cyber-attacks: prevention – detection – mitigation;
- trusted V2X Communication (incl. Intelligent Speed Adaptation);
- secured Automated Driving;
- secure over-the-air updates of safety functions;
- anomaly & fault detection in an automated way;
- Remote monitoring of user/driver data (driver monitoring – e.g. driver falling asleep);
- trusted tamper-proof black box data collection;
- parameter tuning of safety-relevant functions (calibration, engine tuning, remote settings);
- breakdown of component when driving on the highway;
- swarm Learning;
- logging maintenance data;
- driver's authentication for accessing to e-Services proposed by the connected car (ex. Access to car maintenance data or airbag control).

Furthermore, the deliverable defines the scenario owner, the contributors, the technology involved and the way in which the scenario is linked to the WP9 demonstrator. The initial list of scenarios shown in this deliverable will be extended into a final set of scenarios in deliverable 1.2 (D1.2).

2 Process of defining initial user-scenarios and use cases

During the preparation of the project proposal, partners already discussed the need and relevance of individual user-scenarios and use-cases. This involved all consortium partners, as (almost) each WP will be based or use one or more scenarios when developing software or hardware components. The final choice was made through a vote by all partners, in the understanding that at the start of the project implementation, further elaboration would take place. This could include adding, modifying or removing specific (sub-)scenarios. In particular TNO, IMEC-NL, AVL, YoGoKo, Prove&Run and Commsignia provided significant input during the project kick-off meeting on 16/05/2018. Philips provided specific input related to health/driver monitoring. Apart from the kick-off meeting (break-out session), further discussion took place through 2 tele-conferences 12/07/2018 and 23/08/2018and numerous email exchanges between the partners.

The main criterium used by WP1 partners during these meetings was the ability for WP9 to use the scenarios for testing and validating the effectiveness of new software and hardware components. The result is that from the original list of 5 user-scenarios, 2 have been modified.

Annex 1 shows the product of deliverable D1.1, which are print-screens of Microsoft Excel-sheets. The sheets provide the following agreed scenario information:

- the headline-scenario as defined in the DoA;
- different sub-scenarios and their respective owner;
- definition of the threat/attack per sub-scenario;
- technology and other input involved/provided by partners to strengthen each sub-scenario;
- a link to the type of demonstration in WP9.

From this overview, a matrix has been constructed, which will allow each scenario-owner to further refine scenarios together with identified partners. Please note that the scenario validation methodology in a demonstrator-setting has not yet been defined, as this requires input from WP9, which has not yet started its activities.

nr	**scenario**	sub-scenario's	**Scenario owner**	Partners contributing	**Link to Demo**	**Demo Owner**	Demo contributors
1	**road intersection**	1.1 - An intersection with traffic lights is approached by a hijacked truck that has no intention to stop.	**TNO**	CRF, Prove & Run, NXP-NL, AVL, HELM	**Demo 1.1**	**TNO**	CRF, NXP-NL
		1.2 - An automated car approaches intersection which is equipped by a road-side system providing information about vulnerable road users.	**TNO**	CRF, Prove & Run, NXP-NL, AVL, HELM	**Demo 1.2**		CRF, TNO, NXP-NL

		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).	**TNO**	TNO, AVL SF, HELM	**Demo 1.3**		TNO
2	**Health**	2.1 Health status Assessment: how personal health data can be safely and securely exploited in an in-car environment.	**PHILIPS**	PHILIPS, Roche	**Demo 2.1**	**PHILIPS**	SEN, IMEC, 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	**Demo 2.2**	**FICO-ADAS**	PHILIPS, SEN, IMEC, CSIC, INDRA, TST
3	**Update the vehicle**	3.1 secure OTA SW update technology to prevent potential attacks to ensure correct functioning of AD	**AVL-AT**	Prove & Run, AIT, AVL SF, IMEC-NL	**Demo 3.2**		
4	**Advanced access to Vehicle**	4.1 Demonstrator is reflecting the trend for property (vehicle) sharing. The traveler orders a car in the target destination via cloud-based service.	**IMA**	GTO, Ubiqu, BUT, TST, IMEC-NL, CISC	**Demo 3.1**	**IMA**	BUT, Ubiqu, GTO, CISC
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			

3 Conclusions

D1.1 is a first important step in the detailed definition of concrete user-scenarios and use cases that may occur in real-life circumstances and to which software and hardware must be developed to ensure that the security, safety and privacy protection integrity of a vehicle is maintained. The deliverable shows that the main scenarios defined in the DoA have been divided into sub-scenarios and that different combinations of partner-expertise are linked to each sub-scenario to further specify the threat(s) that each sub-scenario represents to the security and safety integrity of the vehicle. Where possible, potential commonalities and specific differences in scenarios have already been identified. This is important for subsequent work packages, who need to investigate not only technically optimal solutions, but also solutions which are cost-effective in tomorrow's vehicles.

D1.1 is a preparatory step toward the finalization of the user-scenarios and sub-scenarios that will be presented in D1.2 and which are currently under discussion by the WP1 partners.

nr	scenario	sub-scenario's	Scenario owner	Partners contributing	Technologies involved	Threats / Attacks [fault injection means considered]	Link to Demo	Demo Owner	Demo contributors
1	**road intersection**	1.1 - A cooperative intersection is equipped with road-side surveillance in order to detect traffic anomalies. An intersection with traffic lights is approached by a hijacked truck that has no intention to stop. Thanks to the road-side surveillance information, the Secredas system reacts to the situation and switches traffic lights in all directions to red, while the truck is remotely forced to stop.	**TNO**	CRF, Prove & Run, NXP-NL, AVL SF, HELM		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 traffic light signals (and speed advice). This is detected thanks to the shared world model and mitigation measures are taken to control/stop the vehicle and/or traffic light and to alert rescue and authorities creating a safer situation and a more resilient system.	**Demo 1.1**	**TNO**	CRF, NXP-NL
		1.2 - An automated car approaches an intersection without traffic lights which is equipped by a road-side system providing information about vulnerable road users. The vulnerable road users communicate their position and speed to the cars and the road-side system.	**TNO**	CRF, Prove & Run, NXP-NL, AVL SF, HELM	V2I, C-ITS, Local Dynamic Map, Shared World Model	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. "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."	**Demo 1.2**		CRF, TNO, NXP-NL
		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).	**TNO**	TNO, AVL SF, HELM	V2I, C-ITS, Local Dynamic Map, Shared World Mode	Privacy attack: a hacker intercepts V2X messages in to track a given vehicle & re-identify the user.	**Demo 1.3**		TNO
2	**Automated car with driver getting health problems / enhanced cruise control**	2.1 Health status Assessment: how personal health data can be safely and securely exploited in an in-car environment. 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.	**PHILIPS**	PHILIPS, Roche	Sensors and software to unobtrusively measure vital signs of the driver and derive its health status from the driver. Driver performance management. Enhanced cruise control software	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.	**Demo 2.1** -Different technologies to measure vital signs will be evaluated: Unobtrusive monitoring of heart rate, blood pressure, glucose levels and respiration rate 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 we have to assess 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.	**PHILIPS**	SEN, IMEC, ROCHE
		2.2 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 I2Vcommunication. In addition to that, the automated vehicle is equipped with systems to obtain physiologic signals from the driver.	**FICO-ADAS**	FICO-ADAS, CSIC, INDRA, PHILIPS, TST, Roche	Unobtrusive systems to obtain physiologocal signals Connectivity to cloud based control center Secure comunication with gateway	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.	**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 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.	**FICO-ADAS**	PHILIPS, SEN, IMEC, CSIC, INDRA, TST
3	**Update the vehicle**	3.1 secure OTA SW update technology to prevent potential attacks to ensure correct functioning of AD	**AVL-AT**	Prove & Run, AIT, AVL SF, IMEC-NL	main technologies: 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	Attack surface is the open ports/services and APIs of the on-board system and the backend system (attacks to bypass access control and authenticaiton mechanisms), as well as the communicaiton link that connects the backsystem 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	**Demo 3.2** - Lab demo of a complete ECU update procedure. Components: backend server3r, gateway (on-board telematic unit) and an ECU (in this case a HVCU) Communicaition channel between GW and backend is 3G/4G/5G, protected by TLS. Data packages are sent as authenticated-encrypted CMS packages		
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. Downloading the credentials to his/her mobile phone or smart advanced 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).	**IMA**	GTO, Ubiqu, BUT, TST, IMEC-NL, CISC	Driver/ Crew identification: variable RF contactless, RFID, NFC, BLE and eGo Car on board infrastructure: Body Board Control Unit (BBCU), CAN/FlexRay/Ethernet Gateway Supportive technology: External Authentication Server supporting RADIUS/DIAMETER protocols. Vehicle identification: we aim to use bidirectional V2I built-in tools In-vehicle Gateways	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	**Demo 3.1** IMA will create 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 on line authentication and profiling using BUT authentication server and BUT robust supplicant code.	**IMA**	BUT, Ubiqu, GTO, CISC
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. 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 point of view.	**Thales**	Thales, AIT, TUKL	Virtualization technology for ensuring a secure environment for the safety critical applications Cloud based technologies for secure staged deployment of safety critical applications Secure communication ensuring the integrity and availability of the safety critical applications	Threats: - Use of open networks for communication -> attack via open ports/ unencrypted services - Denial of service on publicly available cloud hosters - Vulnerabilities in VM software due to needed compatability to legacy systems - 0-day exploits on server machines - Trojan/Vulnerability in Virtualization software - Sandbox excape - Information leakage between virtual machines on same server - Maliciously change (integrity) of cloud configuration - Risk of virtualization sprawl (to many VM instances to be managable)			TUKL

www.secredas.eu

mail@secredas.eu

Social media @secredas_eu

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