SECREDAS

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

DELIVERABLE REPORT

Document Type	Deliverable
Document Title:	"Final reference set of scenarios & use cases"
Document Number	2018-wp1-D1.2
Primary Author(s)	Marianne Vandecasteele, Nicolas Moro (T1.1 leaders)
Document Date	21/12/2018
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
Marianne Vandecasteele	IMEC-NL	Luis Campos	PDMFC
Nicolas Moro	IMEC-NL	Juha Röning	OULU
Jana Viehbeck	Senetics	Karel Kalivoda	IMA
Alexandr Vasenev	TNO	Reinder Haakma	Philips
Joerg Kemmerich	ZF	Francesco Guaraldi	UNIMORE
Hayk Hamazaryan	ZF	Mirco Marchetti	UNIMORE
Radu Lupu	UPB	Clemens Viernickel	Merantix
Brenda Meza	FICOSA	Peter Tummeltshammer	Thales
Florian Stahl	AVL	Thorsten Krankozski	ZF
Iuliana Dragomir	TNO	Thanos Papaioannou	PDMFC
Luis Ribeiro	PDMFC	Aggeliki Tsohou	PDMFC

This lists shows the scenario owners and referral people for the security, safety and privacy analyses. A great many other staff from the participating partners in Task 1.1 contributed to the preparation of D1.2 as well.

FORMAL REVIEWERS

Name	Organization	Date
Task participants		19/12/2018
Roy Pennings (coordinator)	NXP-Semiconductors	28/12/2018
Work package leaders		28/12/2018

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
v0.1	25/10/2018	Marianne Vandecasteele	Draft version of document, including overview final reference set of use cases.
V0.2	20/12/2018	Nicolas Moro	Added new user scenarios and information about threat analysis
V1.0	21/12/2018	Nicolas Moro	Minor corrections after reviews from task partners Draft for review

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 1.2 (D1.2) is part of Task 1.1 and describes the final reference 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 final reference set of scenarios comprises 4 automotive scenarios, 1 health scenario and 1 rail scenario. For each scenario a detailed description is provided and the relevant threats/attacks are identified through an initial threat analysis.

Furthermore, the deliverable defines the scenario owner, the contributors and the way in which the scenario is linked to the WP9 demonstrator.

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 1.2

Deliverable 1.2 (D1.2) is part of Task 1.1 and describes the final reference set of user-scenarios and use cases compiled by the Work Package (WP) participants from partner organizations. This final set of 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 final reference set of scenarios listed in D1.2 comprises 4 automotive scenarios, 1 health scenario and 1 rail scenario. The scenarios that have been elaborated in this deliverable are:

1. road intersection;
2. vehicle with driver getting health problems;
3. keep car secure for the whole vehicle product life time;
4. advanced access to vehicle;
5. rail;
6. incident investigation.

For each scenario, a detailed description was provided by the scenario owner and contributing partners according to the use case description template and demonstrating the relevance of the specific scenario. The scenario description contains information on

- 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
- additional information such as link to demonstrator

Additionally, for each scenario a threat analysis is made to derive security implications and to define a set of attacks/threats relevant for these user scenarios. A methodology for security, safety and privacy threat analysis was suggested and applied to all scenarios across the different application domains. The relevant threats/attacks identified for the reference set of scenarios are summarized in this deliverable and are input to T1.2 ‘Impact of User Scenarios on the Components to be developed’.

2 Process of defining final reference set of scenarios and use cases

2.1 Final reference set of scenarios

At the start of the project, an inventory was made of new scenarios relevant to the SECREDAS project objectives. Based on a use case description template, all consortium partners were invited to provide new scenarios, complementary to the initial set of scenarios as was reported in D1.1.
This resulted in a new set of scenario descriptions, building on the initial set of scenarios and extended with new scenarios provided by 4 consortium partners. Detailed descriptions of all these scenarios were provided by the scenario owners, demonstrating the relevance of the scenario.

Via a process of classifying the new scenarios as addition, modification to an initial scenario or as new scenario, a final set of scenarios and sub-scenarios was defined. In particular TNO, UPB, PHILIPS, FICO-ADAS, OULU, AVL, IMA, IMEC-NL, Thales and ZF provided significant input to this process. Discussions related to this process took place through 2 tele-conferences 03/09/2018 and 12/09/2018, a 1-day WP1 F2F workshop 27/09/2018 at the IMEC-NL office in Eindhoven and numerous email exchanges between the partners. The workshop was attended in Eindhoven by 13 people from 10 consortium partners and 22 people from 17 consortium partners joined remotely via skype.

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 scenarios, 2 scenarios were extended with complementary sub-scenarios, 1 scenario was redefined to broaden its scope, 1 scenario was modified to include additional relevant threats and additionally 1 new scenario was added.

Annex 1 shows the product of deliverable D1.2, which are descriptions of the scenarios and sub-scenarios. From these descriptions, a matrix has been constructed, which gives a high level overview of the scenarios and sub-scenarios, including information on owner, contributor and link to demo. 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 automated vehicle that has no intention to stop.	**TNO / UNIMORE**	CRF, Prove & Run, NXP-NL, AVL, HELM	**Demo 1.1**	**TNO**	CRF, NXP-NL

		1.2 An automated vehicle approaches intersection which is equipped by a road-side system providing information about vulnerable road users.	**TNO / UNIMORE**	CRF, Prove & Run, NXP-NL, AVL, HELM	**Demo 1.2**	**TNO**	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 / UNIMORE**	TNO, AVL SF, HELM	**Demo 1.3**	**TNO**	TNO
		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	**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
		2.3 Driver Monitoring: Driver’s and vehicle’s status monitoring (incl. driver’s health and wellbeing)?	**OULU**	NOKIA-FI, SOLI, HALT	**Demo 2.3**	**OULU**	
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-AT / ZF**	AIT, AVL SF, IMEC-NL, IOTR, TNO	**Demo 3.2**		
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	**Demo 3.1**	**IMA**	BUT, Ubiqu, GTO, CISC
5	**Rail**	5.1 show the technical feasibility of a	**Thales**	Thales, AIT, TUKL			

		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 analyzed.	**ZF**				

2.2 Threat analysis on final reference set of scenarios

For each scenario an initial threat analysis is made to derive security implications and to define a set of attacks/threats relevant for these user scenarios. The identified threats/attacks are summarized in this deliverable and are a main input to T1.2 ‘Impact of User Scenarios on the Components to be developed’

First an approach for security, safety and privacy threat analysis was suggested, to be applied across the different application domains and in this way safeguard consistency across the domains. The proposed approach was validated by applying the method to one of the scenarios. In a final step, dedicated teams per scenario were identified to apply it to the specific scenario.

In particular AVL, SEN and PDMFC provided significant input to the process of defining the approach. The proposed methodology was discussed during the tele-conference on 12/09/2018 and during the WP1 F2F workshop on 27/07/2018. A dedicated Validation of the methodology by applying it to a selected scenario 4, was done by a dedicated team consisting of GTO, IMEC-NL, IMA, UBIQU, BUT and TNO. For this analysis 2 tele-conferences were held 12/10/2018 and 25/10/2018 combined with email exchanges between the partners.

Framework and tools used for the threat analysis

The partners agreed to use the following tools and frameworks for the threat analysis:

Data flow diagram	Microsoft Threat Modeling Tool 2016
Security	Threat Analysis and Risk Assessment (TARA) with the SAHARA risk assessment method
Safety	Failure Mode and Effects Analysis (FMEA)
Privacy	LINDDUN

A template was provided by AVL, with some additions from SEN (for safety) and IMEC-NL (for privacy).

AVL, ZF and Magneti Marelli proposed to use another framework for the safety analysis. They think Hazard Analysis and Risk Assessment (HARA) would be more relevant for a detailed safety analysis for the automotive user scenarios. At the moment of this deliverable, only a high-level analysis using FMEA is available for Scenario 1 and its sub-scenarios. This issue was identified in a teleconference on 16/12/2018 and therefore this safety analysis can only be achieved for a later deliverable of WP1, most probably D1.7.

Way of working

A full example of a data flow diagram and threat analysis was collaboratively done for Scenario 4: Advanced access to Vehicle. This example was then provided to the different partners and in particular to the scenario owners.

The scenario owners were responsible for providing a data flow diagram to the teams in charge of the analysis for security, safety and privacy. Some scenario owners were not familiar with data flow diagrams or the tool which was chosen for that purpose and therefore received some support from other partners.

They had then the possibility, for each of the three types of analysis:

- to do it themselves (with or without the other contributors to the scenario definition)
- to delegate it to one of the support partners:
    - IMEC-NL for security
    - SEN for safety
    - PDMFC for privacy

The threat analysis' status was discussed at the Consortium Meeting in Leuven on 13/11/2018 and later in two teleconferences (on 28/11/2018 and 16/12/2018). The minutes for these meetings can be found on SharePoint.

Outcome

The threat analyses are available for most of the studied scenarios and are ongoing but not finalized for a few of them. The status per scenario can be found in Annex 1. The results of this analysis (data flow diagrams and list of threats for each scenario) have been stored on SharePoint in the folder dedicated to T1.1 (Root / WP_Progress / WP1 / T1.1 – Threat Analysis / Final Use Cases).

D3 Conclusions

D1.2 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 combination of an extended description, a data flow diagram and a threat analysis for security, safety and privacy will help the other tasks and work packages to get a very deep understanding of the challenges each scenario will have to address.

The following issues have been identified during the activities of this task:

- some partners had more expertise than others for the threat analysis
- some partners joined (or proposed to join) the task's activities very late
- some partners only provided their input very late, which had an impact on the following analysis
- it was difficult to align on the degree of detail and specificity of the different analyses
- the need for another method for the safety analysis of the automotive scenarios (HARA instead of FMEA) was identified very late
- in general, it was very difficult to efficiently share information with such a large group of partners

Annex 1

Scenario 1 detailed description

Scenario description 1.1

Scenario	
Context	Road intersection
Owner / Contact person	TNO / iuliana.dragomir@tno.nl – UNIMORE / francesco.guaraldi@unimore.it mirco.marchetti@unimore.it
Description of defining behavior	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. Road Side 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 Road Side 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 Road Side Units toward the Traffic Management System. Traffic Management System at intersection communicate GLOSA information to the vehicles through the Road Side 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 Road Side 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 / iuliana.dragomir@tno.nl – UNIMORE / francesco.guaraldi@unimore.it mirco.marchetti@unimore.it
Description of defining behavior	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 Road Side 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. Road Side 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 Road Side 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
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 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.

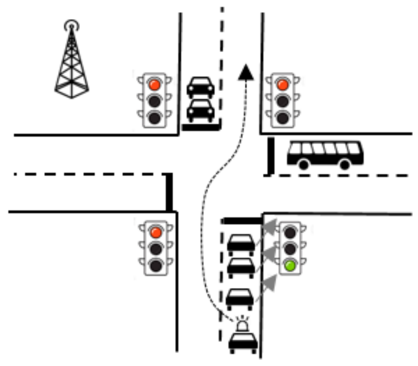
Scenario description 1.3

Scenario	
Context	Road intersection
Owner / Contact person	TNO / iuliana.dragomir@tno.nl – UNIMORE / francesco.guaraldi@unimore.it mirco.marchetti@unimore.it
Description of defining behavior	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. Road Side 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 Road Side 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 Road Side 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 Road Side 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 Road Side Units located near the intersection..
Compliance needs	C-ITS
Preferred method for Security/Privacy/Safety Analysis	
Relevant threats	Single or multiple attacks taking place in above scenario 1. One of the Road Side 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	Emergency vehicle approaches a crowded intersection
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 Road Side Unit.
Owner / Contact person	UPB / rlupu@elcom.pub.ro ; TNO / iuliana.dragomir@tno.nl ; UNIMORE / francesco.guaraldi@unimore.it mirco.marchetti@unimore.it

Description of defining behavior	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 Road Side 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 1(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 preemption 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
Additional information	

Scenario description 1.5

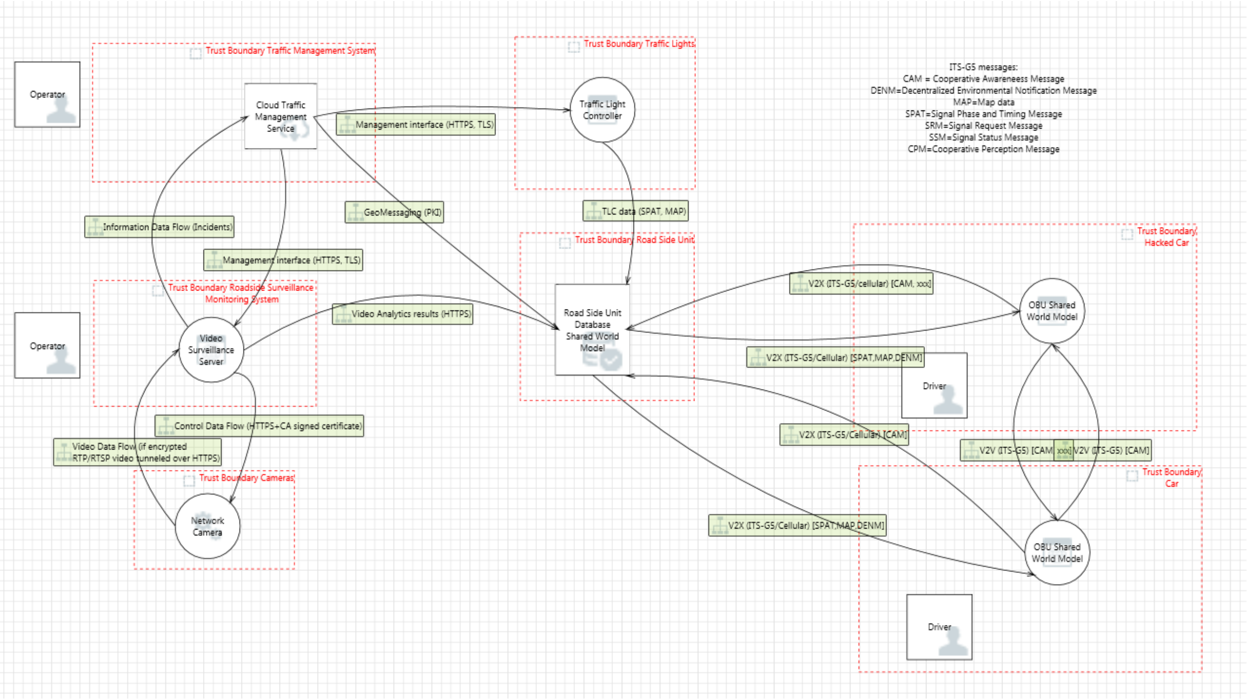
Scenario	
Context	Road intersection
Owner / Contact person	Merantix / clemens@merantix.com
Description of defining behavior	The intersection is populated with other vehicles and vulnerable users and is being approached by an automated vehicle. The perception system of the automated vehicle has been attacked 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	1. 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.
Compliance needs	None.
Preferred method for Security/Privacy/Safety Analysis	
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
Additional information	

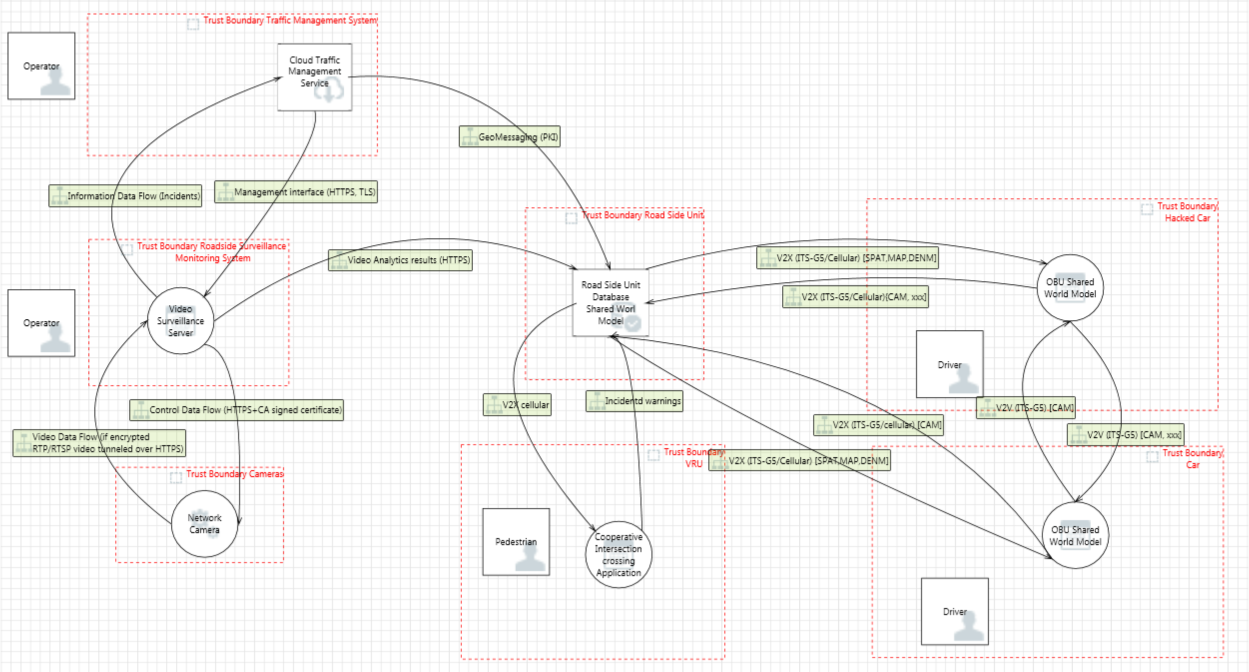
Scenario 1 threat analysis report

Scenario 1.1 report


Trust Boundary Traffic Management System
Operator
Cloud Traffic Management Service
Management interface (HTTPS, TLS)
Trust Boundary Traffic Lights
Traffic Light Controller
ITS-G5 messages:
CAM = Cooperative Awareneess Message
DENM=Decentralized Environmental Notification Message
MAP=Map data
SPAT=Signal Phase and Timing Message
SRM=Signal Request Message
SSM=Signal Status Message
CPM=Cooperative Perception Message
GeoMessaging (PKI)
TLC data (SPAT, MAP)
Information Data Flow (Incidents)
Management interface (HTTPS, TLS)
Trust Boundary Road Side Unit
Trust Boundary Hacked Car
Trust Boundary Roadside Surveillance Monitoring System
V2X (ITS-G5/cellular) [CAM, xxx]
Video Analytics results (HTTPS)
Road Side Unit Database Shared World Model
OBU Shared World Model
Operator
Video Surveillance Server
V2X (ITS-G5/Cellular) [SPAT,MAP,DENM]
Driver
Control Data Flow (HTTPS+CA signed certificate)
V2X (ITS-G5/Cellular) [CAM]
Video Data Flow (if encrypted RTP/RTSP video tunneled over HTTPS)
V2V (ITS-G5) [CAM, xxx]
V2V (ITS-G5) [CAM]
Trust Boundary Cameras
Trust Boundary Car
Network Camera
V2X (ITS-G5/Cellular) [SPAT,MAP,DENM]
OBU Shared World Model
Driver

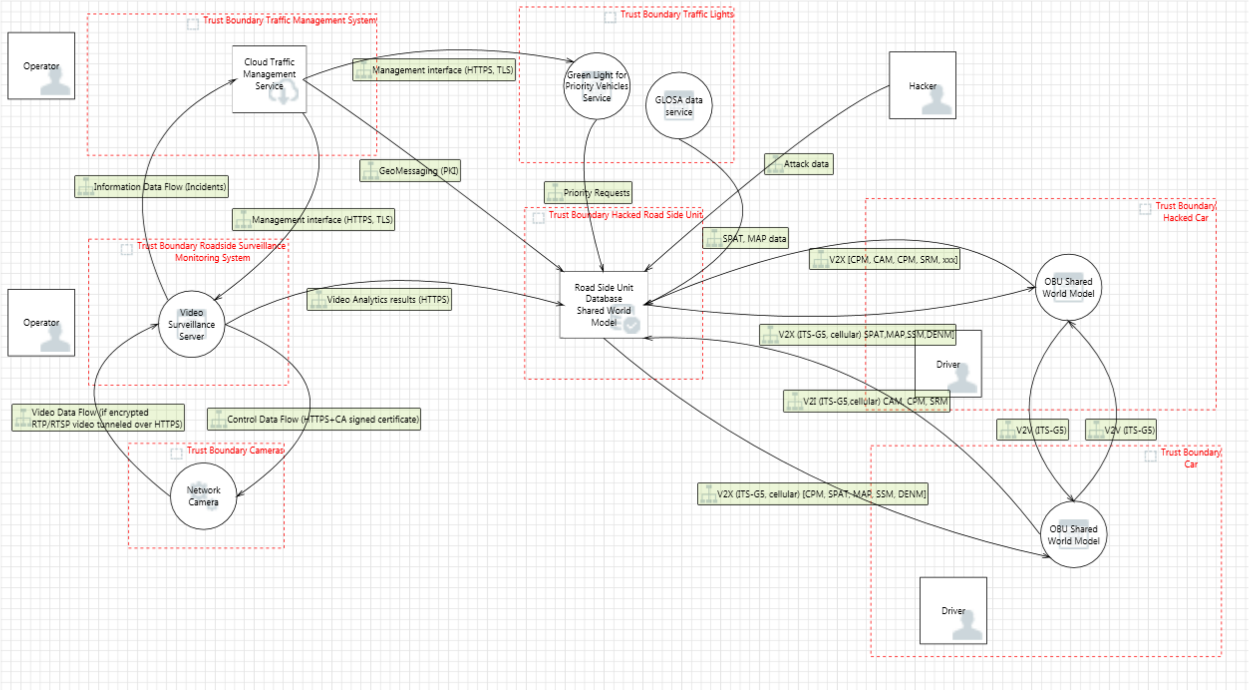
	Status	Partner
Data Flow Diagram:	Available on SharePoint	TNO
Security:	Available on SharePoint	UNIMORE
Safety:	Available on SharePoint (only high-level analysis so far)	NXP
Privacy:	Available on SharePoint	PDMFC

Scenario 1.2 report


Trust Boundary Traffic Management System
Operator
Cloud Traffic Management Service
GeoMessaging (PKI)
Information Data Flow (Incidents)
Management interface (HTTPS, TLS)
Trust Boundary Road Side Unit
Trust Boundary Hacked Car
Trust Boundary Roadside Surveillance Monitoring System
Video Analytics results (HTTPS)
V2X (ITS-G5/Cellular) [SPAT,MAP,DENM]
Road Side Unit Database Shared Worl Model
V2X (ITS-G5/Cellular)[CAM, xxx]
OBU Shared World Model
Operator
Video Surveillance Server
Driver
Control Data Flow (HTTPS+CA signed certificate)
V2X cellular
Incidentd warnings
V2V (ITS-G5) [CAM]
V2X (ITS-G5/cellular) [CAM]
V2V (ITS-G5) [CAM, xxx]
Video Data Flow (if encrypted RTP/RTSP video tunneled over HTTPS)
Trust Boundary VRU
V2X (ITS-G5/Cellular) [SPAT,MAP,DENM]
Trust Boundary Car
Trust Boundary Cameras
Network Camera
Pedestrian
Cooperative Intersection crossing Application
OBU Shared World Model
Driver

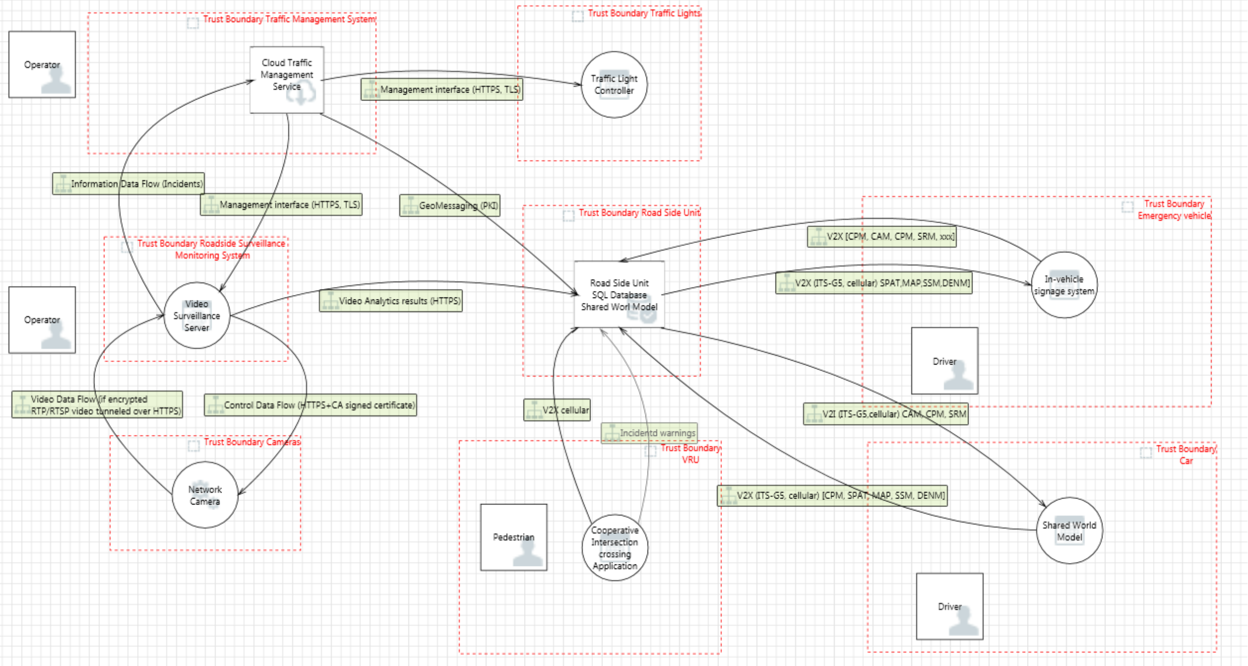
	Status	Partner
Data Flow Diagram:	Available on SharePoint	TNO
Security:	Available on SharePoint	UNIMORE
Safety:	Available on SharePoint (only high-level analysis so far)	NXP
Privacy:	Available on SharePoint	PDMFC

Scenario 1.3 report


Trust Boundary Traffic Management System
Operator
Cloud Traffic Management Service
Management interface (HTTPS, TLS)
Trust Boundary Traffic Lights
Green Light for Priority Vehicles Service
GLOSA data service
Hacker
Attack data
GeoMessaging (PKI)
Information Data Flow (Incidents)
Priority Requests
Management interface (HTTPS, TLS)
Trust Boundary Hacked Road Side Unit
SPAT, MAP data
Trust Boundary Hacked Car
Trust Boundary Roadside Surveillance Monitoring System
V2X [CPM, CAM, CPM, SRM, xxx]
Road Side Unit Database Shared World Model
OBU Shared World Model
Operator
Video Analytics results (HTTPS)
Video Surveillance Server
V2X (ITS-G5, cellular) SPAT,MAP,SSM,DENM]
Driver
V2I (ITS-G5,cellular) CAM, CPM, SRM
Video Data Flow (if encrypted RTP/RTSP video tunneled over HTTPS)
Control Data Flow (HTTPS+CA signed certificate)
V2V (ITS-G5)
V2V (ITS-G5)
Trust Boundary Cameras
Trust Boundary Car
Network Camera
V2X (ITS-G5, cellular) [CPM, SPAT, MAP, SSM, DENM]
OBU Shared World Model
Driver

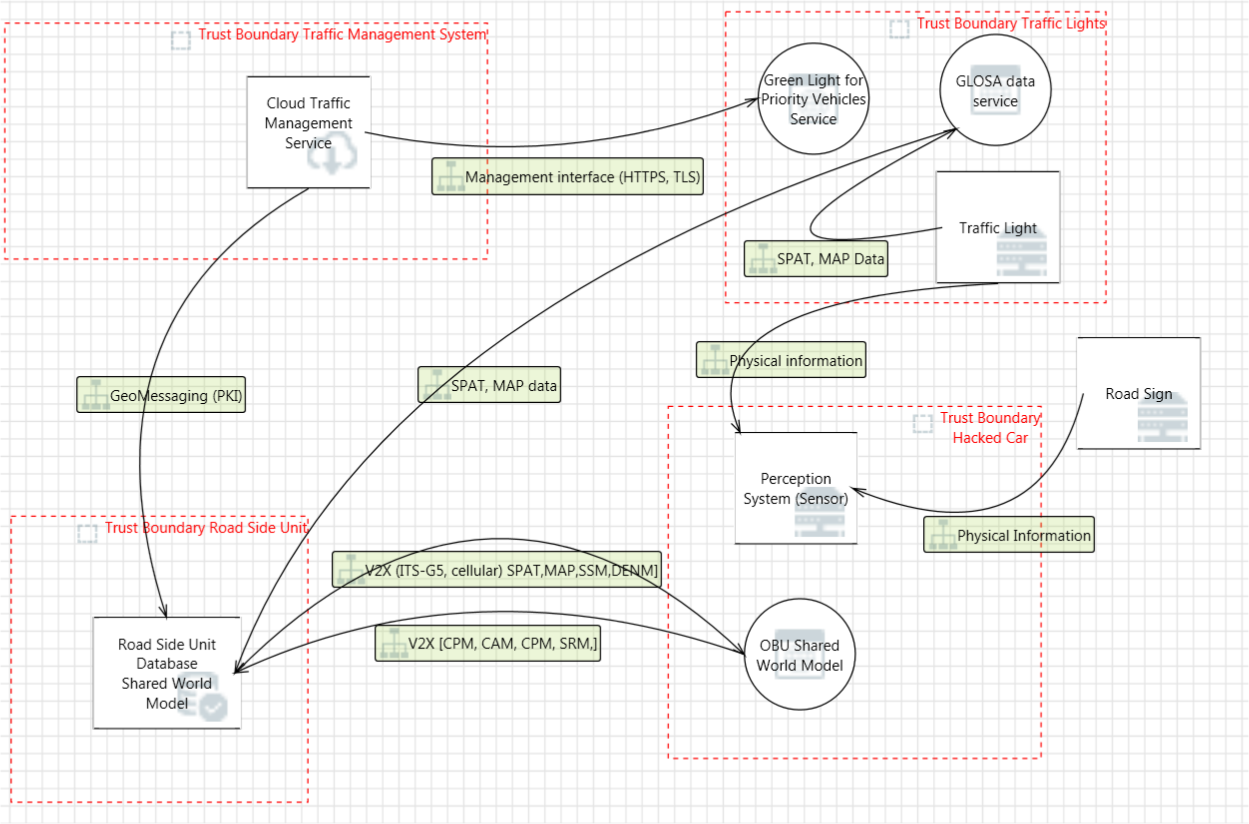
	Status	Partner
Data Flow Diagram:	Available on SharePoint	TNO
Security:	Available on SharePoint	UNIMORE
Safety:	Available on SharePoint (only high-level analysis so far)	NXP
Privacy:	Available on SharePoint	PDMFC

Scenario 1.4 report


Trust Boundary Traffic Management System
Trust Boundary Traffic Lights
Operator
Cloud Traffic Management Service
Management interface (HTTPS, TLS)
Traffic Light Controller
Information Data Flow (Incidents)
Management interface (HTTPS, TLS)
GeoMessaging (PKI)
Trust Boundary Road Side Unit
Trust Boundary Emergency vehicle
V2X [CPM, CAM, CPM, SRM, xxx]
Trust Boundary Roadside Surveillance Monitoring System
Operator
Video Surveillance Server
Video Analytics results (HTTPS)
Road Side Unit SQL Database Shared Worl Model
V2X (ITS-G5, cellular) SPAT,MAP,SSM,DENM]
In-vehicle signage system
Driver
Video Data Flow (if encrypted RTP/RTSP video tunneled over HTTPS)
Control Data Flow (HTTPS+CA signed certificate)
V2X cellular
V2I (ITS-G5,cellular) CAM, CPM, SRM
Incidentd warnings
Trust Boundary Cameras
Trust Boundary VRU
Trust Boundary Car
Network Camera
V2X (ITS-G5, cellular) [CPM, SPAT, MAP, SSM, DENM]
Shared World Model
Pedestrian
Cooperative Intersection crossing Application
Driver

	Status	Partner
Data Flow Diagram:	Available on SharePoint	TNO
Security:	Available on SharePoint	UNIMORE, UPB
Safety:	Available on SharePoint (only high-level analysis so far)	NXP
Privacy:	Available on SharePoint	PDMFC, UPB

Scenario 1.5 report


Trust Boundary Traffic Management System
Cloud Traffic Management Service
Management interface (HTTPS, TLS)
Trust Boundary Traffic Lights
Green Light for Priority Vehicles Service
GLOSA data service
Traffic Light
SPAT, MAP Data
Physical information
Road Sign
GeoMessaging (PKI)
SPAT, MAP data
Trust Boundary Hacked Car
Perception System (Sensor)
Physical Information
Trust Boundary Road Side Unit
V2X (ITS-G5, cellular) SPAT,MAP,SSM,DENM]
Road Side Unit Database Shared World Model
V2X [CPM, CAM, CPM, SRM,]
OBU Shared World Model

	Status	Partner
Data Flow Diagram:	Available on SharePoint	MRTX
Security:	Available on SharePoint	MRTX
Safety:	Ongoing, not finalized yet	NXP
Privacy:	Available on SharePoint	PDMFC

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 / reinder.haakma@philips.com

Description of defining behavior	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.
Compliance needs	-
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	FICO-ADAS / brenda.meza@ficosa.com noelia.rodriguez@ficosa.com
Description of defining behavior	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 center via I2Vcommunication. 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 physiologocal signals 2. Connectivity to cloud based control center 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 dowm for security reasons
Assumptions	The cyber threat may give false information to the autonomous and semiautonomous systems in order to cause an accident.
Compliance needs	-
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 de 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.

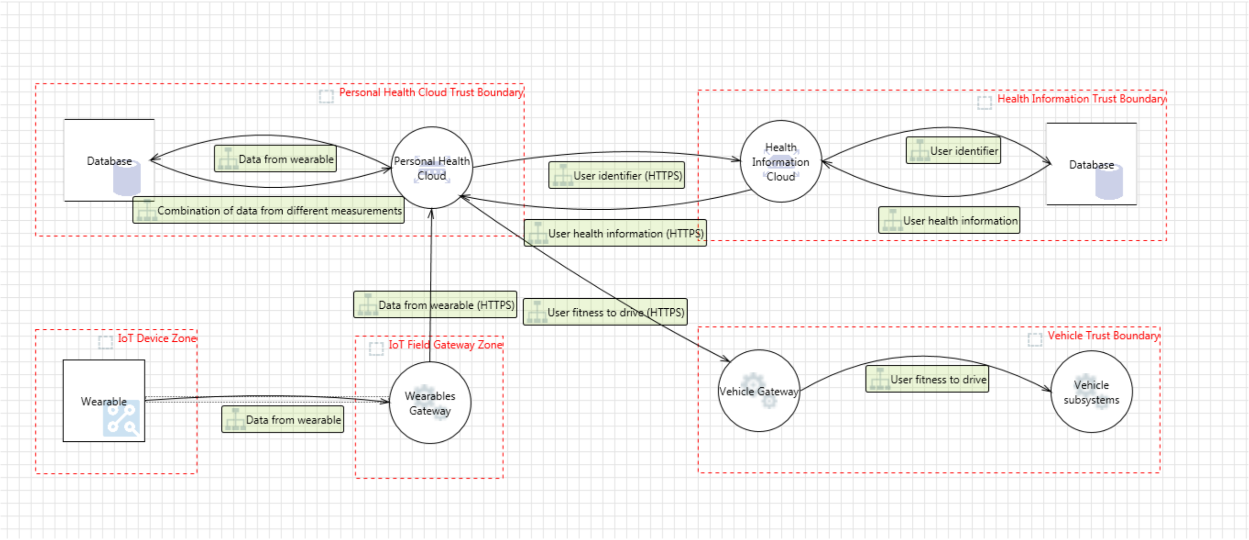
Scenario description 2.3

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 / juha.roning@oulu.fi
Description of defining behavior	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	1. 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).
Compliance needs	-

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 (Ficosa-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.

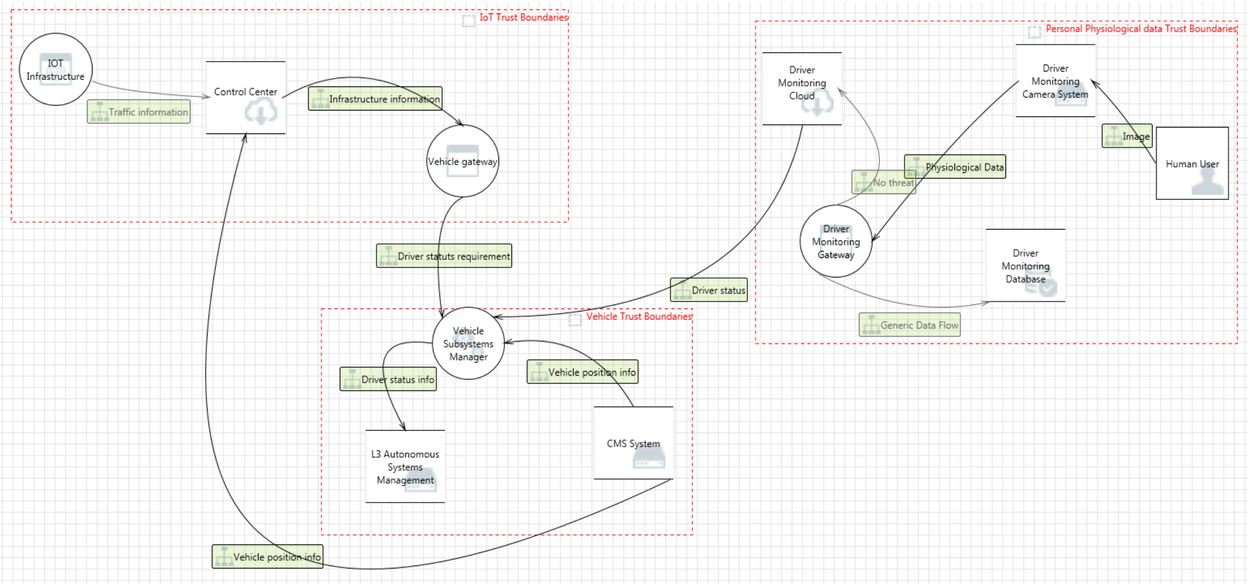
Scenario 2 threat analysis report

Scenario 2.1 report



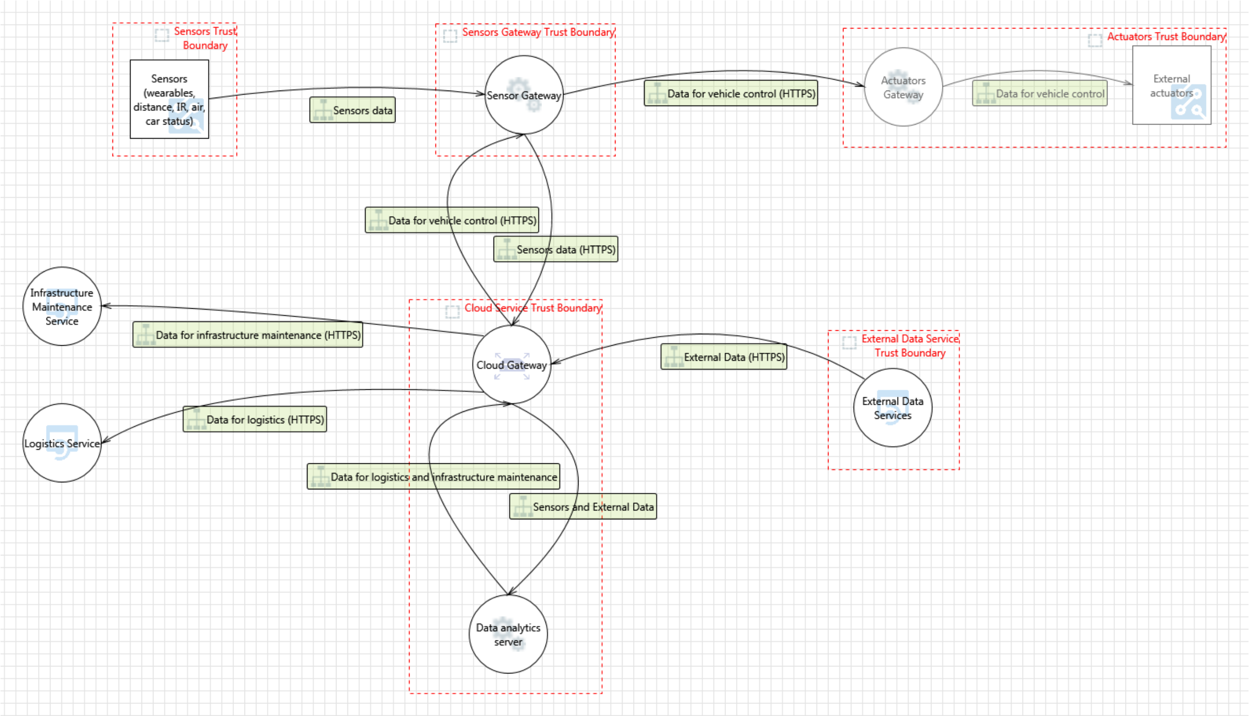
	Status	Partner
Data Flow Diagram:	Available on SharePoint	PHILIPS, IMEC-NL
Security:	Available on SharePoint	IMEC-NL
Safety:	Available on SharePoint	SENETICS
Privacy:	Available on SharePoint	PDMFC

Scenario 2.2 report



	Status	Partner
Data Flow Diagram:	Available on SharePoint	FICOSA
Security:	Ongoing, not finalized yet	IMEC-NL
Safety:	Available on SharePoint	SENETICS
Privacy:	Ongoing, not finalized yet	PDMFC

Scenario 2.3 report


Sensors Trust Boundary
Sensors (wearables, distance, IR, air, car status)
Sensors data
Sensors Gateway Trust Boundary
Sensor Gateway
Data for vehicle control (HTTPS)
Actuators Trust Boundary
Actuators Gateway
Data for vehicle control
External actuators
Data for vehicle control (HTTPS)
Sensors data (HTTPS)
Infrastructure Maintenance Service
Data for infrastructure maintenance (HTTPS)
Cloud Service Trust Boundary
Cloud Gateway
External Data (HTTPS)
External Data Service Trust Boundary
External Data Services
Logistics Service
Data for logistics (HTTPS)
Data for logistics and infrastructure maintenance
Sensors and External Data
Data analytics server

	Status	Partner
Data Flow Diagram:	Available on SharePoint	OULU
Security:	Ongoing, not finalized yet	IMEC-NL
Safety:	Available on SharePoint	SENETICS
Privacy:	Ongoing, not finalized yet	PDMFC

Scenario 3 detailed description

Scenario description 3.1

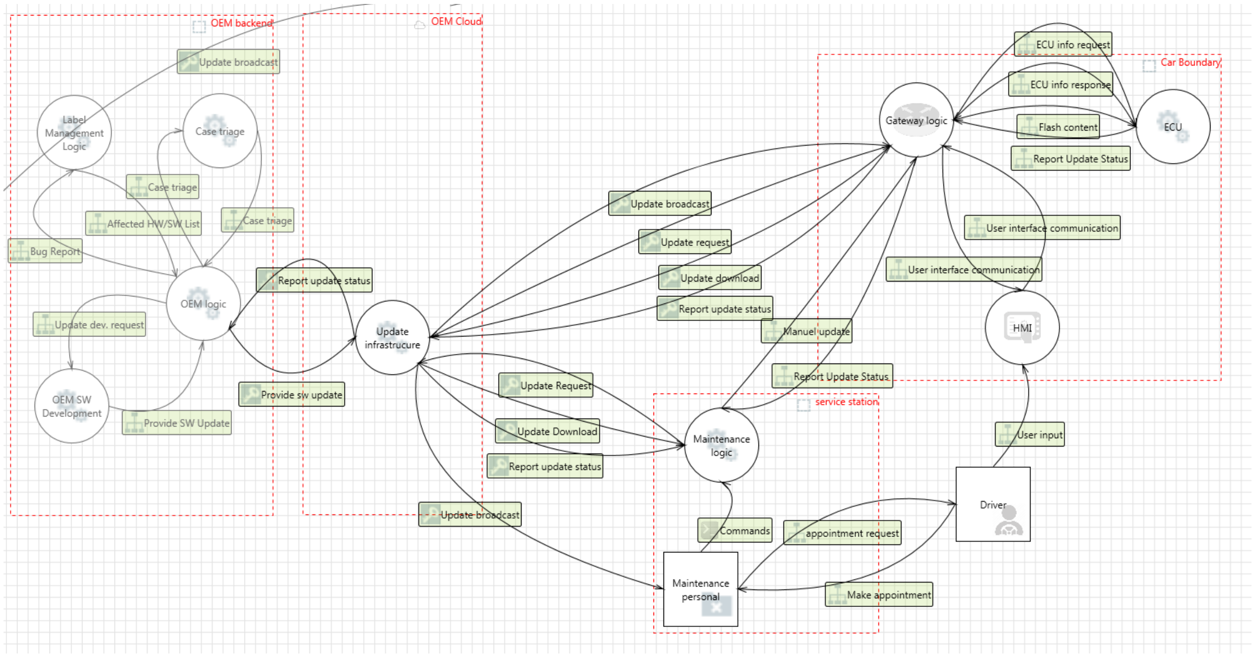
Scenario	
Context	Keep car secure for the whole vehicle product life time (in operation and maintenance)
Owner / Contact person	AVL / Zhendong.Ma@avl.com, AVL / Florian.Stahl@avl.com ZF / hayk.hamazaryan@zf.com, ZF / Joerg.kemmerich@zf.com
Description of defining behavior	Continuous improvement is required 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 and encrypted and digitally signed. The software blob is stored in 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
Additional information	

Scenario 3 threat analysis report

Scenario 3.1 report



	Status	Partner
Data Flow Diagram:	Available on SharePoint	AVL, ZF, IOTR, TNO
Security:	Available on SharePoint	AVL, ZF, IOTR, TNO
Safety:	Not available yet	
Privacy:	Available on SharePoint	AVL, ZF

Scenario 4 detailed description

Scenario description 4.1

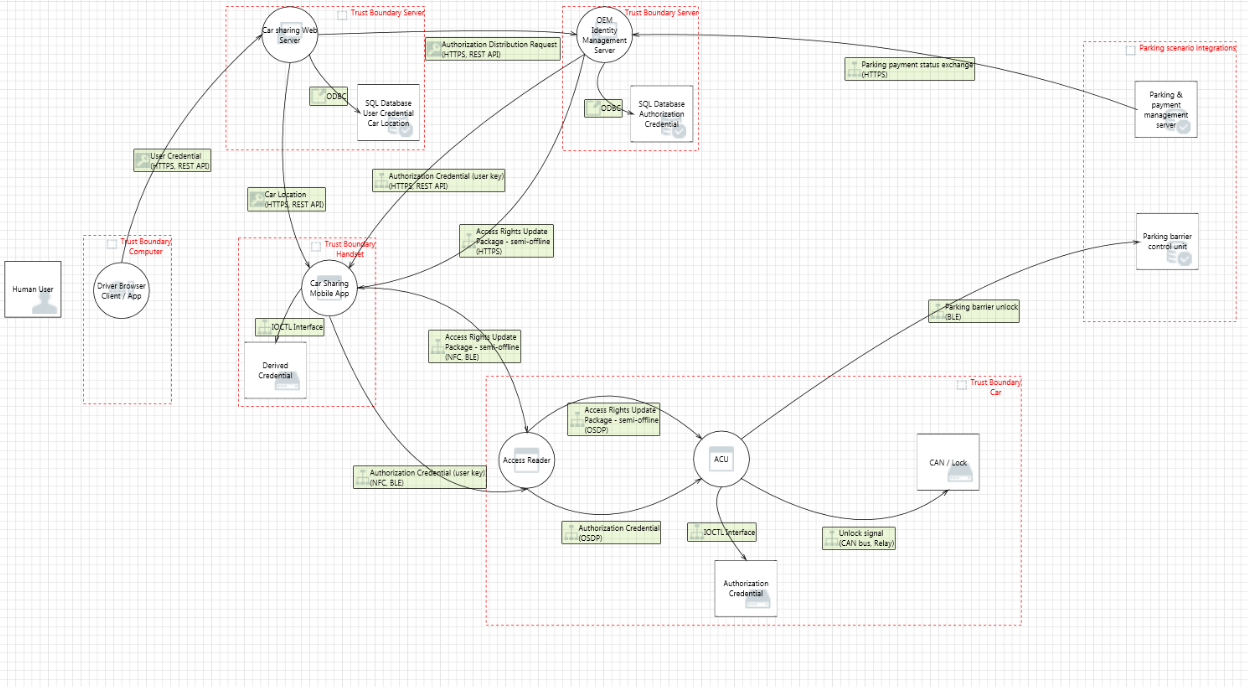
Scenario	
Context	Advanced access to Vehicle

Owner / Contact person	IMA / karel.kalivoda@ima.cz
Description of defining behavior	Scenario is reflecting the trend for property (vehicle) sharing. The traveler 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
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 it self is used in case the CU is offline 3) After finishing the one-time key activation process, key is securely installed into users device 4) After interaction with access reader, key is sent to ACU over BLE/NFC/RFID 5) ACU verifies access authorization and 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.
Compliance needs	
Preferred method for Security/Privacy/Safety Analysis	
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 vehcile is in a remote offline loccation

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 on line authentication and profiling using BUT authentication server and BUT robust supplicant code.

Scenario 4 threat analysis report

Scenario 4.1 report


Trust Boundary Server
Car sharing Web Server
ODBC
SQL Database User Credential Car Location
Authorization Distribution Request (HTTPS, REST API)
Trust Boundary Server
OEM Identity Management Server
ODBC
SQL Database Authorization Credential
Parking payment status exchange (HTTPS)
Parking scenario integrations
Parking & payment management server
User Credential (HTTPS, REST API)
Car Location (HTTPS, REST API)
Authorization Credential (user key) (HTTPS, REST API)
Access Rights Update Package - semi-offline (HTTPS)
Parking barrier control unit
Human User
Trust Boundary Computer
Driver Browser Client / App
Trust Boundary Handset
Car Sharing Mobile App
IOCTL Interface
Derived Credential
Access Rights Update Package - semi-offline (NFC, BLE)
Parking barrier unlock (BLE)
Trust Boundary Car
Access Rights Update Package - semi-offline (OSDP)
Access Reader
ACU
CAN / Lock
Authorization Credential (user key) (NFC, BLE)
Authorization Credential (OSDP)
IOCTL Interface
Unlock signal (CAN bus, Relay)
Authorization Credential

	Status	Partner
Data Flow Diagram:	Available on SharePoint	IMA, IMEC-NL, UBIQU, GTO, TNO, BUT, TST, CISC
Security:	Available on SharePoint	IMEC-NL, IMA
Safety:	No safety involved	
Privacy:	Available on SharePoint	IMEC-NL

Scenario 5 detailed description

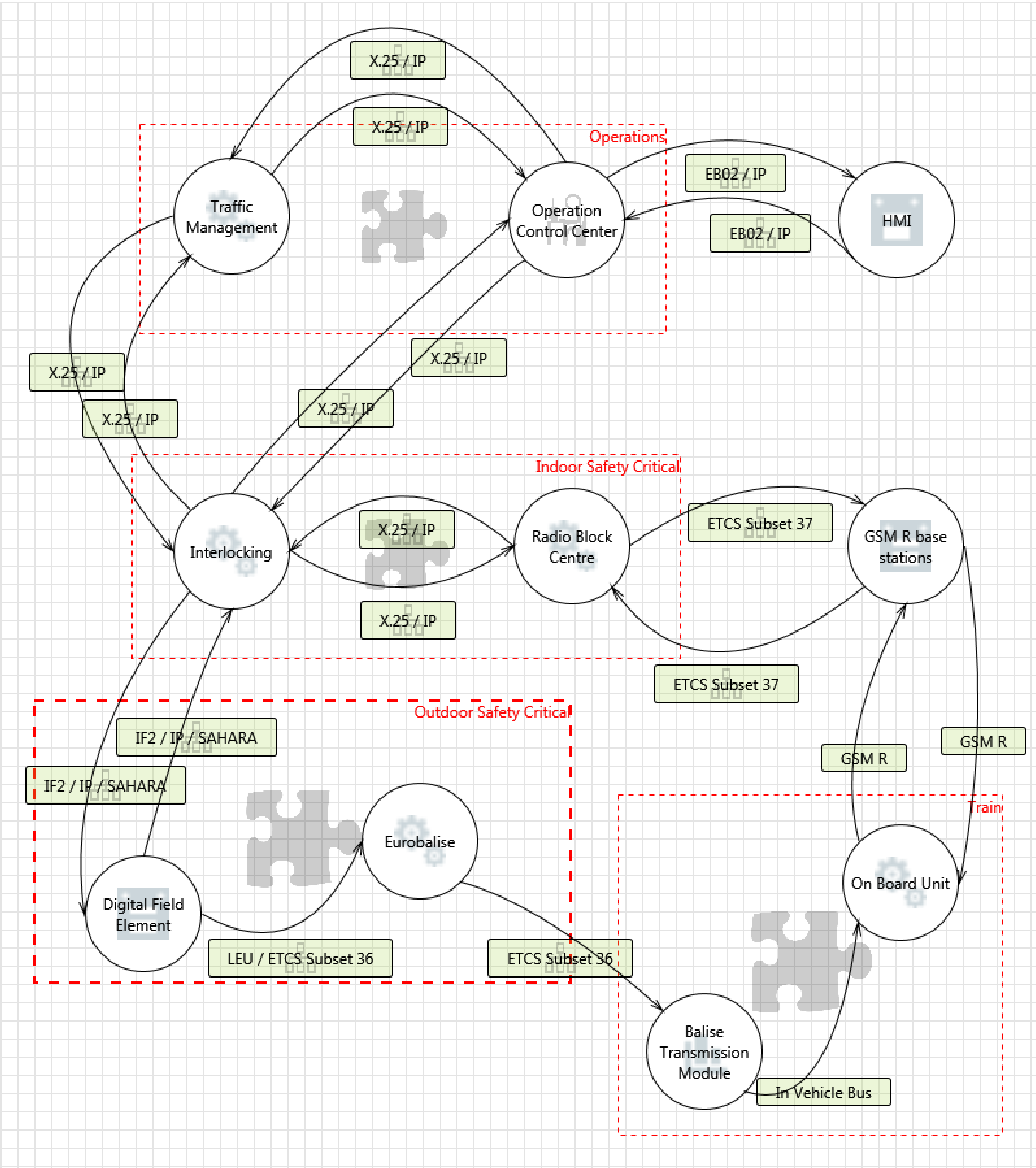
Scenario description 5.1

Scenario	
Context	Rail
Owner / Contact person	Thales / peter.tummeltshammer@thalesgroup.com

Description of defining behavior	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 3-2 Security 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 5 threat analysis report

Scenario 5.1 report



	Status	Partner
Data Flow Diagram:	Available on SharePoint	Thales
Security:	Ongoing, not finalized yet	Thales, AIT
Safety:	Ongoing, not finalized yet	Thales, AIT
Privacy:	Ongoing, not finalized yet	Thales, AIT, PDMFC

Scenario 6 detailed description

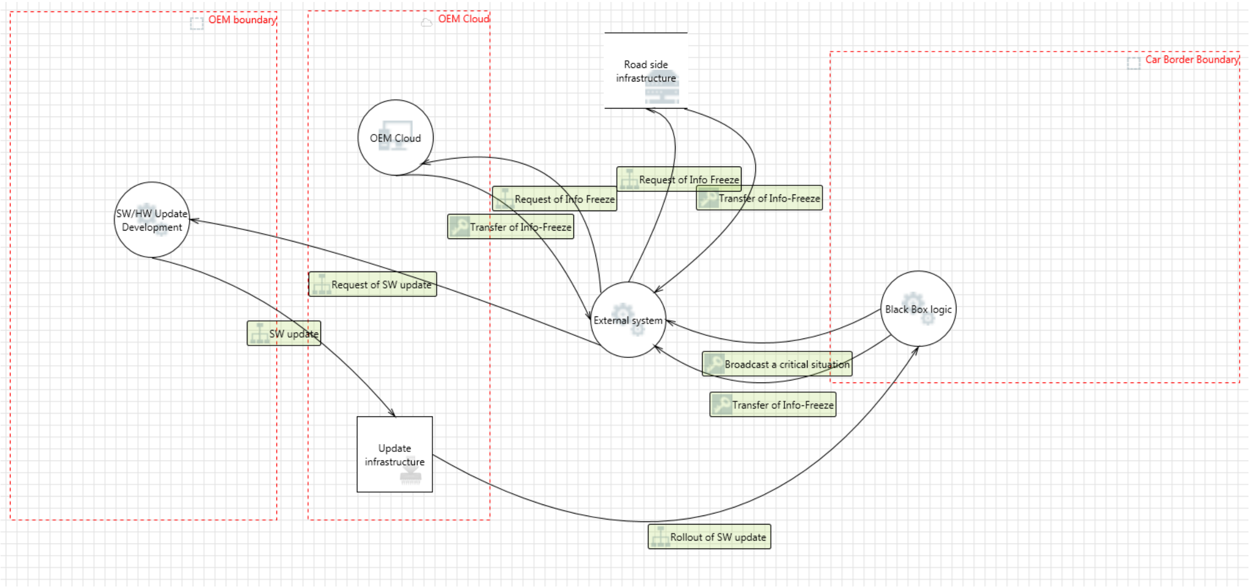
Scenario description 6.1

Scenario	**Incident Investigation**
Context	A critical situation is recognized and it needs to be virtually reproduced and analyzed. 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 / hayk.hamazaryan@zf.com, ZF / joerg.kemmerich@zf.com, ZF / thorsten.kranzkowski@zf.com
Description of defining behavior	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 Road side 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, road side 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 has been started (needed information has been blocked for changes/deleting in different clouds, maintenance information of incident participant's 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.
Compliance needs	
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 threatens weakest link in the Incident Investigation process and injects manipulated data into the Info-Freeze. Privacy aspects of process needs to be prioritized.

Additional information	

Scenario 6 threat analysis report

Scenario 6.1 report



	Status	Partner
Data Flow Diagram:	Available on SharePoint	ZF
Security:	Available on SharePoint	ZF
Safety:	Not available yet	
Privacy:	Available on SharePoint	ZF

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